Jaarlijkse informatie-beveiligingsmonitor

april 2020

DeNederlandscheBank

EUROSYSTEEM

Inleiding

DNB voert al een aantal jaren onderzoek uit bij banken, pensioenfondsen en verzekeraars naar informatiebeveiliging (IB). Dit doen we sinds 2010 op basis van onder andere periodieke self-assessments voor de onder ons toezicht staande instellingen. Als handvat voor het invullen van deze self assessments hebben we in 2019 de Good Practice[1] en bijbehorende Q&A Informatiebeveiliging geactualiseerd.

Basis voor de jaarlijkse IB-monitor zijn de IB-onderzoeken bij pensioenfondsen en verzekeraars. De IB-monitor is in 2019[2] voor het eerst uitgebracht. Uit de toezichtgesprekken met bancaire instellingen en andere onderzoeken, is naar voren gekomen dat de waarnemingen uit het IB-onderzoek 2019 relevant zijn voor de gehele Nederlandse financiële sector.

Verder zijn in deze IB-monitor, naast onderzoek vanuit Toezicht, te weten de in 2019 uitgevoerde onderzoeken, aangevuld met informatie vanuit standaard uitvragen[3] en doorlopend account toezicht, andere bronnen meegenomen. Zo ontvangt DNB meldingen van cyber-incidenten en zijn we via het TIBER-programma betrokken bij het testen van de weerbaarheid van een aantal instellingen op het gebied van cybersecurity. Daarnaast heeft DNB als (mede) voorzitter van werkgroepen binnen zowel EBA[4] en EIOPA[5] meegewerkt aan Europese Guidelines op het gebied van IT en Cybersecurity. De beelden die uit deze werkgroepen voortkomen zijn waar relevant verwerkt in dit document.

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.

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.

1 https://www.toezicht.dnb.nl/3/50-203304.jsp
2 https://www.toezicht.dnb.nl/binaries/50-237814.pdf
3 IT-SREP en SBA-NFR
4 European Banking Authority
5 European Insurance and Occupational Pension Pensions Authority

Inhoud

1 Waarnemingen IB-monitor

Cyberhygiëne en met name vulnerability management blijft cruciaal

Preventie alleen is niet genoeg, de focus verschuift naar samen-werking, detectie en response

Testen van maatregelen draagt bij aan continue verbeteren van Cyberweerbaarheid

Wees u bewust van de rol die u als bestuurder heeft bij Informatiebeveiliging

Geef met uitbesteden niet de verantwoordelijkheid uit handen, blijf zelf in control

Houd rekening met specifieke risico's die naar aanleiding van de pandemie COVID-19 naar voren komen

Cyberhygiëne blijft cruciaal

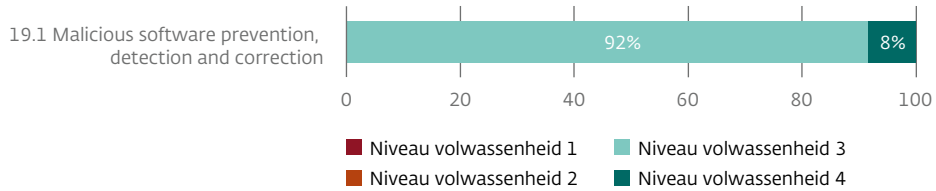
Om cyberdreigingen het hoofd te kunnen bieden is hygiëne op het gebied van cybersecurity essentieel. Cyberhygiëne omvat het definiëren, implementeren (toepassen) en onderhouden van cybersecurity standaarden (vereisten) en baselines (minimum vereisten). Deze standaarden en baselines hebben onder andere betrekking op maatregelen ten aanzien van het beperken van de impact van kwaadaardige software. De beheersingsmaatregelen #19.1 t/m #19.3 uit de Good Practice IB gaan in op cyberhygiëne en zijn in de IB-onderzoeken nader onderzocht.

De impact van cyberdreigingen in de vorm van bijvoorbeeld kwaadaardige software zoals malware en gijzelsoftware op de bedrijfsvoering van instellingen kan groot zijn. Nog maar korte tijd geleden hebben instellingen de impact ervaren van een kwetsbaarheid in de Citrix-infrastructuur, waardoor veel instellingen genoodzaakt waren deze infrastructuur voor het op afstand werken tijdelijk buiten gebruik te stellen. De impact hiervan zou nog groter zijn geweest als dit was samengevallen met de recente COVID-19 crisis.

De volgende mogelijke verbeterstap voor de instellingen ligt in een verdieping van preventieve technische maatregelen. Instellingen hebben over het algemeen de nodige voorzieningen (tools) in huis om malicious software af te weren (preventie) op te sporen (detectie) en onschadelijk te maken (correctie). Zie ook figuur 1 die is samengesteld uit de resultaten van de IB-onderzoeken uit 2019. DNB ziet dit als een goede stap vooruit. DNB constateert in haar onderzoek echter dat preventieve technische maatregelen als bijvoorbeeld netwerk segmentering en hardening[6] van systemen nog relatief beperkt worden toegepast. Hier ziet DNB een volgende mogelijke verbeterstap voor de instellingen in.

Figuur 1 Volwassenheid scores Manage malware attacks 2019

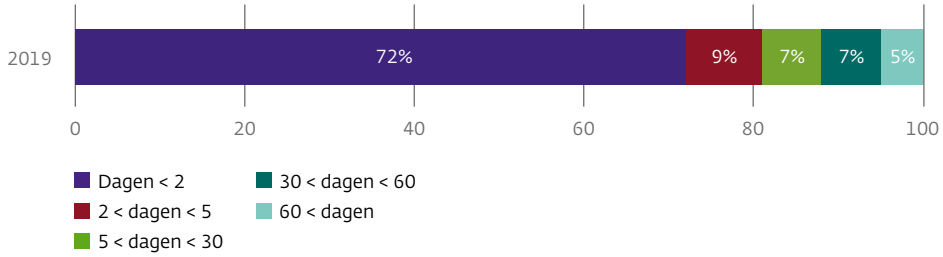
In procenten



DNB signaleert achterstanden bij het wegwerken van geconstateerde kwetsbaarheden binnen de IT-systemen van instellingen. Zie daartoe ook figuur 2 waar de doorlooptijd van het patchen van systemen bij de onderzochte instellingen is weergegeven. We zien in ons onderzoek dat 28% van kritische patches niet binnen 2 dagen is geïmplementeerd. DNB wijst instellingen op de risico's die voortvloeien uit het niet tijdig opsporen en mitigeren van kwetsbaarheden.

Figuur 2 Kritische systemen gepatcht voor kritische zwakheden

In procenten

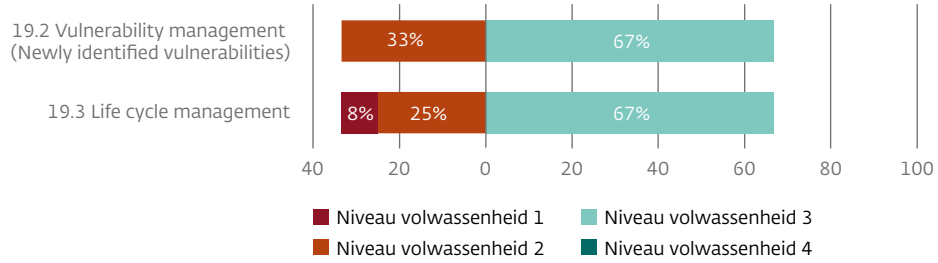


6 Het doel van systeem hardening is om zo veel mogelijk de risico's ten aanzien van informatiebeveiliging en cybersecurity te elimineren, door overbodige functies en/of software van het besturingssysteem uit te zetten of van het systeem te verwijderen.

Het gebruik van end-of-life systemen is nog te vaak gemeengoed en/of instellingen hebben simpelweg onvoldoende inzicht in de levenscyclus van de gebruikte applicaties. Met als gevolg dat applicaties worden gebruikt die niet meer zijn ondersteund door leveranciers. Daarmee zijn zij kwetsbaar voor cyber- en continuïteitsdreigingen. Dit heeft DNB in haar onderzoeken geconstateerd, zie figuur 3 over life cycle management. Naast het tijdig doorvoeren van patches om kwetsbaarheden te minimaliseren, is het uitfaseren van verouderde software en het doorvoeren van een goede scheiding in het netwerk (netwerk segmentatie) een goede maatregel om cyberrisico's verder te mitigeren. Dit is zeker niet alleen van toepassing op software in de IT-infrastructuur, maar geldt ook voor (business) applicaties. Daarnaast zijn ontwerpprincipes als 'security by design' bij oudere applicaties vaak niet gehanteerd, wat deze applicaties inherent kwetsbaarder maakt dan applicaties die wel volgens deze principes zijn ontworpen.

Figuur 3 Volwassenheid scores Vulnerability and Life cycle management

In procenten



DNB heeft verder het beeld dat instellingen tegenwoordig bij digitale aanvallen specifiek worden uitgezocht en zeer gericht op van te voren uitgezochte doelen binnen hun instelling worden aangevallen. DNB heeft het beeld dat het voorheen voldoende was om 'algemene' IB-maatregelen te nemen en daarmee in een analogie je huis met voldoende sloten beter beveiligd was dan dat van de buurman. Nu is het niet meer voldoende om betere sloten dan de buurman te hebben. Het is daarom belangrijk dat de instelling structureel en risico gebaseerd bepaalt wat de impact van de kwetsbaarheden is op de eigen specifieke IT-assets. In de Good Practice IB worden voorbeelden gegeven waarbij de instelling een eigen risk response bepaalt op basis van haar toleranties en de opvolging hiervan controleert. Het inschatten welke kwetsbaarheden het meest relevant zijn om op te reageren wordt door instellingen in praktijk nog als lastig ervaren. Samenwerking tussen instellingen en in de sector is hierbij evident en wordt nog te weinig gedaan.

Uit TIBER ziet DNB dat analyses van cybersecurity dreigingen ook bij Vulnerability management steeds relevanter zijn. Om te kunnen prioriteren op welke kwetsbaarheden gereageerd moet worden is het noodzakelijk om de volgende punten in kaart te brengen. In kaart kan worden gebracht welke dreigingen er zijn, over welke IT-assets de instelling beschikt die relevant zijn voor welk soort aanvallers en welke methoden worden gebruikt om die specifieke IT-assets te bereiken, te manipuleren en/of te beschadigen.

Voorbeelden genoemd in de Good Practice IB hierbij zijn:

- Een instelling implementeert tools voor de automatische detectie en blokkade van virussen, wormen, malware en spyware zoals moderne firewall technologie, virusscanners, Intrusion Detection Systems (IDS) en Intrusion Prevention Systems (IPS).
- Een instelling stuurt logfiles uit voornoemde systemen naar een Security Incident and Event Monitoring (SIEM)–systeem, ten behoeve van analyse en (re) actie.
- Een instelling heeft het netwerk gesegmenteerd, om de impact van een geslaagde malware aanval zo veel mogelijk te beperken.
- Een instelling bewaakt voortdurend in hoeverre Firewalls, virusscanners, IDS-en, IPS-en up to date zijn en rapporteert daar maandelijks over.
- In een configuratiemanagement database (CMDB) heeft een verzekeraar de vervangingstermijn opgenomen van applicaties en op basis hiervan plant zij vervanging.

Testen van maatregelen draagt bij aan continue verbeteren

Een zo realistisch mogelijk uitgevoerde test geeft een instelling inzicht in de genomen maatregelen en kan zich richten op verschillende aspecten van de bedrijfsvoering van de instelling. In onderzoek van DNB is specifiek aandacht besteed aan het testen van het gehele stelsel van genomen informatiebeveiliging en cybersecurity maatregelen, door middel van scenario testen. Zie daartoe ook figuur 4 met betrekking tot beheersingsmaatregel #22: Testing. Een scenario test kan bijvoorbeeld zijn gericht op zwakheden in de IT-infrastructuur of op menselijk gedrag en menselijk handelen, maar ook op het testen van continuïteitsmaatregelen van IT-systemen (Testing of the IT continuity plan). Effectief testen hangt nauw samen met het selecteren van de meest geschikte testmethode. DNB ziet testmethodes variëren van simpele desk-based oefeningen tot zo realistisch mogelijk gesimuleerde aanvallen. Een aantal instellingen heeft al een zo realistisch mogelijke test uitgevoerd, bijvoorbeeld door mitigerende maatregelen rondom DDoS aanvallen te simuleren. DNB onderschrijft het belang van testen om de werking van mitigerende maatregelen op gecontroleerde wijze vast te stellen.

Instellingen kunnen het structureel (laten) uitvoeren van testen in een terugkerende periodieke cyclus beter borgen, bijvoorbeeld als onderdeel van een groter testprogramma binnen de gehele keten. DNB ziet dat het structureel inbedden van informatiebeveiliging en cybersecurity testen binnen de (keten) organisatie van instellingen niet altijd optimaal wordt benut. DNB ziet veel ruimte voor verbetering om scenario testen effectiever (en in de gehele keten) uit te voeren om zo een meer realistische situatie na te bootsen.

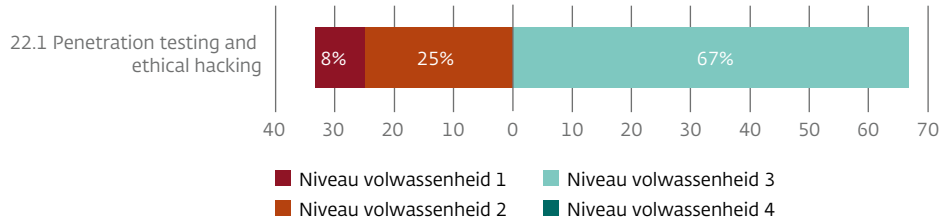
De integrale continuïteit van de bedrijfsvoering van instellingen is steeds vaker afhankelijk van een grote groep dienstverleners en onderaannemers. Instellingen kunnen hun ketenpartners meer betrekken bij de opzet en uitvoering van de eerder genoemde testen.

Uit DNB onderzoek komen naast het bovenstaande **twee andere risico's** naar voren:

- **De kwaliteit van uitgevoerde penetratietesten wisselt sterk** ten aanzien van onder andere de onderzoeksverantwoording, scope, diepgang en rapportage. DNB heeft het beeld dat in de markt van aanbieders van penetratietesten nog veel verschil in kwaliteit is en het voor de instellingen niet altijd eenvoudig is de markt voldoende te doorgronden. Het is belangrijk dat instellingen extra aandacht besteden aan de selectie van gekwalificeerde externe partijen indien zij deze wenst in te schakelen voor het uitvoeren van penetratietesten.
- **Business Continuity Management richt zich nog te veel op klassieke scenario's** zoals bijvoorbeeld gebouwencalamiteiten en brand. Het BCM beleid en diens tests zouden zich meer kunnen richten op locatie, mensen (key persons), ICT en uitbestedingspartijen. Waarbij men ook voorbereid is op andere eigentijdse dreigingen. Denk hierbij bijvoorbeeld aan de impact van malware, ransomware en ook een pandemie op de continuïteit van de bedrijfsvoering.

Figuur 4 Volwassenheid scores Testing 2019

In procenten



Een aantal instellingen communiceert haar concrete verwachtingen rondom het uitvoeren van penetratietesten (onderzoeksverantwoording, scope, diepgang, etc.) richting dienstverleners ter bevordering van de consistentie en kwaliteit van uitgevoerde beveiligingstesten. Kwalitatief goed uitgevoerde penetratietesten dragen in de praktijk sterk bij aan het verbeteren van (technische) maatregelen en het reduceren van informatiebeveiligings- en cybersecurityrisico's. Door heldere communicatie en verwachtingsmanagement richting dienstverleners wordt de uitvoering van penetratietesten op een consistente wijze geborgd en is de door instellingen gewenste kwaliteit van penetratietesten in lijn met de daadwerkelijke kwaliteit. Daar waar dienstverleners beschikken over beleid op het gebied van penetratietesten kan een vertaalslag plaatsvinden naar de verwachtingen van de instellingen zelf. Hierbij valt te denken aan: het vaststellen van kwaliteitscriteria voor de penetratietesten, vertaling van deze criteria naar afspraken met de dienstverleners en (mogelijk nog) aanvullende eigen testwerkzaamheden door instellingen.

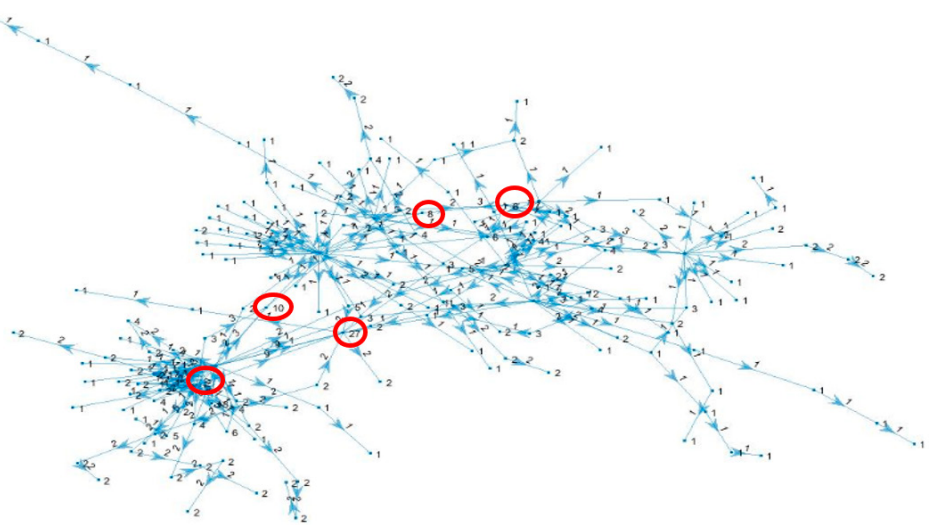
Geef met uitbesteden niet de verantwoordelijkheid uit handen, blijf zelf in control

DNB benadrukt dat de instelling eindverantwoordelijk blijft voor de door dienstverleners uitgevoerde activiteiten. Dit geldt zeker ook voor het borgen van de adequate werking van maatregelen ten aanzien van informatie-beveiliging en cybersecurity. De laatste jaren is ontegenzeggelijk de trend gaande dat uitbesteding van kritieke functies of activiteiten steeds verder toeneemt binnen de financiële sector. Daarmee wordt dus de afhankelijkheid van dienstverleners in de keten steeds groter en is de noodzaak voor samenwerking van dienstverleners en onderaannemers in de keten groter geworden.

DNB roept instellingen op zich bewust te zijn van mogelijke concentratierisico's. Dit kan onder andere door kritische vragen te stellen aan dienstverleners ten aanzien van bijvoorbeeld de impact van calamiteiten (Business Continuity Management) op de dienstverlening. Daarnaast ook door het ontwikkelen van initiatieven zoals een pooled audit (zie kader).

Tegelijkertijd brengt het gebruik maken van dezelfde dienstverlener door meerdere instellingen ook kansen met zich mee. Zo worden instellingen vanuit hun gezamenlijk belang in staat gesteld om de krachten te bundelen richting de dienstverlener. Bijvoorbeeld in de vorm van het uitvoeren van gezamenlijke beveiligingstests en -audits, alsook het afdwingen van de implementatie van 'sound industry practises' op het gebied van informatiebeveiliging en cybersecurity. Ook hier roept DNB op dat instellingen meer gezamenlijk optrekken om minimale verwachtingen ten aanzien van informatiebeveiligingsmaatregelen bij diestverleners (inclusief onderuitbestedingspartijen) overeen te komen.

Concentraties in de keten bij enkele grote aanbieders van IT infrastructuur, datacenter services, applicatiebeheer en core processen voortgekomen uit een uitvraag aan verzekeraars.

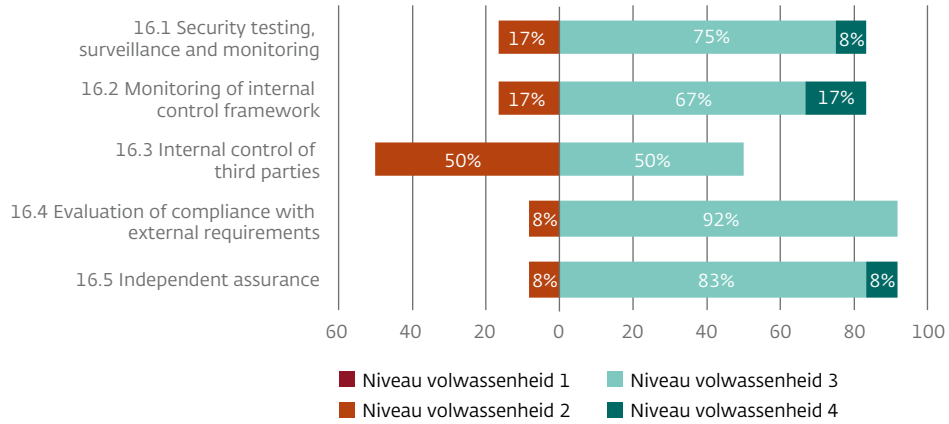


Uit DNB onderzoek komen naast bovenstaande de volgende **drie andere risico's** naar voren:

- **Niet alle instellingen hebben hun kritieke of belangrijke uitbestedingsketens voldoende in kaart gebracht.** DNB geeft in haar Good Practice IB aan dat DNB er op let dat de instelling een proces heeft ingericht dat ten minste het volgende waarborgt dat zij de IT-ketens rondom kritische processen scherp in beeld hebben, zicht hebben op relevante onder-uitbesteding en adequate contractuele afspraken maakt met haar dienstverleners.
- **Het risico bestaat dat instellingen ten onrechte zekerheid ontlenen aan assurance rapportages.** Het gebruik van assurance rapportages door instellingen is voor verbetering vatbaar. Uit de onderzoeken komt naar voren dat steeds meer dienstverleners assurance rapportages kunnen overleggen over de kwaliteit van hun dienstverlening en de eigen interne beheersing. Zie daartoe ook figuur 5 beheersingsmaatregel #16.5, monitoring. Het gebruik van deze rapporten is echter voor verbetering vatbaar. Het blijkt dat instellingen nog onvoldoende zelf vaststellen of het soort assurance dat wordt verleend, gepast is voor de uitbestede activiteiten (werking geeft meer zekerheid dan alleen opzet en bestaan). Ook blijkt dat de scope/beheersingsmaatregelen van de rapportage beter kunnen aansluiten bij de reikwijdte/maatregelen van de uitbestede dienstverlening. Daarnaast kunnen instellingen meer expliciet maken op welke wijze gebruikersoverwegingen uit de assurance rapportage in de eigen organisatie zijn ingebed en wat de impact is van eventuele bevindingen uit de assurance rapportage voor de eigen organisatie van de instelling.
- **Monitoring van informatiebeveiligingsmaatregelen op operationeel niveau bij ketenpartners is beperkt**. Zie daartoe ook figuur 5 en de beheersingsmaatregelen 16.1-16.5 uit de Good practice IB. Voorbeelden hierbij zijn dat gegevens van instellingen en haar klanten vaak niet meer opgeslagen staan op de eigen IT-infrastructuur, maar op de systemen van ketenpartners en cloudproviders. Duidelijke afspraken en accurate verantwoordingsinformatie zijn daarom randvoorwaardelijk voor instellingen om afdoende controle en monitoring op informatiebeveiligings- en cybersecurity-maatregelen bij dienstverleners uit te oefenen.

Figuur 5 Volwassenheid scores Monitoring 2019

In procenten



Voorbeeld van een Pooled Audit

Under regulation, EU financial institutions are required to ensure unrestricted audit rights and capability to perform audits in case they outsource material workloads to cloud service providers. As a result, Deutsche Börse initiated a collaborative cloud audit group (CCAG) in 2017 in order to comply with these regulatory requirements. The collaborative audit group performs such audits in a collective manner, significantly reducing the effort for both financial institutions and cloud service providers. This industry-wide initiative includes large EU financial institutions and insurance companies. The CCAG's first successful pooled audit on Microsoft Azure was completed in 2018.

Samenwerking, detectie en response wordt steeds belangrijker

Preventie alleen is heden ten dage niet meer genoeg, de nadruk komt meer te liggen op detectie en response. Zoals in waarneming 1 Cyberhygiene is aangegeven vormen preventieve maatregelen op het gebied van informatiebeveiliging en cybersecurity de basis die op orde moet zijn om gerelateerde dreigingen het hoofd te kunnen bieden. DNB ziet dat maatregelen op het gebied van detectie & monitoring steeds belangrijker worden. De vraag is namelijk niet meer of een instelling risico's loopt ten aanzien van informatiebeveiliging en cybersecurity, maar hoe deze ermee omgaat als de instelling daadwerkelijk is getroffen door een cyber-aanval of -incident.

Het wordt steeds belangrijker op welke wijze en hoe snel de instellingen en haar dienstverleners in staat zijn dreigingen en aanvallen te herkennen, het hoofd te bieden, danwel de impact hiervan te beperken. Uit DNB onderzoek komt naar voren dat kwaadwillenden die eenmaal binnen zijn bij een instelling, zich relatief (te) eenvoudig toegang kunnen verschaffen tot aanpalende onderdelen van de IT-infrastructuur van de instelling, of van haar dienstverleners. De recente ransomware aanvallen op verschillende bedrijven hebben laten zien dat de impact van een langdurige aanval omvangrijk kan zijn. Een steeds verdere integratie van systemen en netwerken kent daarmee een ongewenst neveneffect van toegenomen kwetsbaarheid op het gebied van informatiebeveiliging en cybersecurity.

De grote dienstverleners bieden al tools en werkwijzen aan voor detectie en monitoring. Het beeld van DNB is dat instellingen hier vooralsnog op zeer beperkte schaal gebruik van maken. Hierbij kan gedacht worden aan geavanceerde behavioural tools die bijvoorbeeld afwijkende gedragspatronen van medewerkers op het netwerk kunnen detecteren. Ook kan gedacht worden aan het aanstellen en professionaliseren van een Security en Operating Center (SOC).

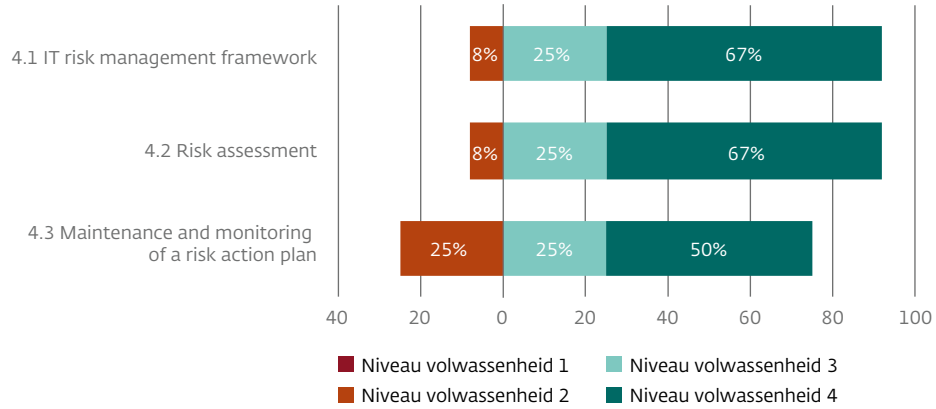
Een Security en Operating Center (SOC) kan bijdragen aan het versterken van de detectie & monitoringsmogelijkheden van de instelling. Vanwege de beperkte omvang van een instelling kan een dergelijk SOC echter een brug te ver zijn. Een aantal instellingen neemt derhalve SOC dienstverlening af van commerciële partijen. Daarnaast onderzoekt een aantal instellingen de mogelijkheid een gezamenlijk SOC in te richten.

Ook samenwerking met andere instellingen, al dan niet grensoverschrijdend wordt hierbij steeds meer van belang. Door informatie uit te wisselen over digitale aanvallen en manieren om deze aanvallen op te sporen en indien opgespoord te neutraliseren wordt de sector weerbaarder. Een instelling beschikt qua informatie vaak alleen over een stukje van de puzzel. Informatie-uitwisseling kan tot een meer volledig beeld leiden waardoor de eigen beheersmaatregelen kunnen worden aangescherpt.

Rol van het bestuur

Om de risico's van dreigingen op het gebied van informatiebeveiliging en cybersecurity goed te kunnen inschatten is bij het bestuur vaak diepgaande (technische) kennis benodigd. Uit de onderzoeken komt naar voren dat iets meer dan de helft van de instellingen over een voldoende volwassenheidsniveau beschikken ten aanzien van de beheersingsmaatregelen met betrekking tot de Risk Management Cycle. Zie daartoe ook figuur 6 en de beheersingsmaatregelen 4.1-4.3 uit de Good practice IB. DNB ziet verder dat instellingen risico's op het gebied van informatiebeveiliging en cybersecurity, nog beter en meer structureel in kaart kunnen brengen en kunnen bespreken op bestuursniveau. Heeft het bestuur een beeld wat de belangrijkste "kroonjuwelen" van hun organisatie zijn en met welk palet van maatregelen, preventief, defectief, responsief die het beste kunnen worden beschermd? Is zij in staat in dat palet keuzes te maken?

Figuur 6 Volwassenheid scores Assess and manage IT risks 2019
In procenten



Alhoewel het beter gaat constateert DNB nog steeds in haar gesprekken met instellingen dat het (beperkte) kennisniveau van besturen en directies over deze dreigingen een aandachtspunt is. Bij onvoldoende kennis bestaat het gevaar dat besturen en directies niet in staat zijn de risico overwegingen met betrekking tot cyberdreigingen en de daarmee samenhangende maatregelen goed te overzien. Dit kan er vervolgens toe leiden dat niet altijd de juiste en/of onvoldoende maatregelen worden genomen. Een adequaat kennisniveau draagt bij aan het voldoende prioriteit kunnen geven aan het doorvoeren van noodzakelijke maatregelen. De beheersingsmaatrelen uit de Good Practice IB kunnen helpen het fundament op te zetten, maar het is nooit af. Voor een specifiek gerichte aanval zoals in waarneming 1 Cyberhygiëne is besproken is continu verbeteren nodig. Informatiebeveiliging is het continu analyseren, testen, leren, verbeteren en prioriteren van middelen.

Het bestuur/de directie draagt zorg voor haar eigen deskundigheid op het gebied van informatiebeveiliging en cybersecurity, zodat het voldoende 'countervailing power' heeft ten opzichte van haar eigen organisatie en haar uitbestedingspartners. Een voorbeeld hierbij is dat het bestuur/de directie trainingen en opleidingen volgt om de belangrijkste IT-risico's en beheersings-maatregelen voor haar instelling te kunnen begrijpen en basiskennis van informatie-beveiliging en cybersecurity te borgen. Daar waar nodig en opportuun kan de instelling op onderdelen externe expertise inschakelen. Tot slot is het van belang dat het bestuur/de directie goed voorbeeldgedrag vertoont ten aanzien van bewustzijn voor risico's op het gebied van informatiebeveiliging en cybersecurity en het naleven van maatregelen (tone-at-the-top).

In de Good Practice IB zijn per onderdeel goede voorbeelden gegeven hoe besturen een goede invulling kunnen geven aan hun rol. Uit de onderzoeken kwam naar voren dat niet alle besturen die verwachtingen rondom hun rol voldoende op het netvlies hadden. Ook in toetsingsgesprekken zal DNB meer aandacht besteden aan het op orde zijn van het deskundigheidsniveau van bestuurders op dit onderwerp.

Houd rekening met specifieke risico's die naar aanleiding van de pandemie COVID-19 naar voren komen

DNB heeft recent (maart en april 2020) een inventarisatie uitgevoerd naar business continuïteit en cyberrisico's binnen de Nederlandse financiële sector (verzekeraars, pensioenfondsen, banken, betaalinstellingen) en belangrijke service providers. Directe aanleiding is de uitbraak van het COVID-19 (Corona) virus, wat bij de financiële instellingen heeft geleid tot het activeren van maatregelen (pandemie scenario's) en tot veranderende werkomstandigheden.

DNB heeft voor deze inventarisatie onder andere:

- extra contact opgenomen met de instellingen die vitaal zijn voor onze financiële stabiliteit, de grote Verzekeraars en Pensioenfondsen en Vermogensbeheerder over signalen en incidenten op het vlak van Business Continuiteit Management (BCM) en cyber-incidenten;
- een uitvraag gedaan bij de grootbanken (SSM) op basis van de 'ECB letter on Contingency preparedness in the context of Corona';
- specifieke signalen bij externe accountantorganisaties (en IT-auditors) opgehaald;
- een uitvraag gedaan onder grote third party service providers en bigtechs over de werking van hun BCM maatregelen, noodscenario's en over een eventuele toename van cyber-incidenten;
- zijn ten behoeve van het sector- dreigingsbeeld de CISO's van de grote instellingen specifiek benaderd.

Uit deze inventarisatie komen voor nu de volgende risico's en daarmee samenhangende aandachtspunten voor de financiële instellingen naar voren.
De aankomende tijd gaat DNB verder met de inventarisatie en blijft zij signalen uit de sector verzamelen en analyseren.

- **Verhoging risico dat de essentiële infrastructuur (tijdelijk) niet of vermindert toegankelijk is door toename DDoS aanvallen en pogingen tot hacken en afpersing.** De afhankelijkheid van internet voor thuiswerken maakt de dreiging van DDoS-aanvallen extra relevant. Daarnaast vergt thuiswerken veelal meer capaciteit voor het in de lucht houden van de netwerkapparatuur. De benodigde capaciteit om malafide activiteiten te kunnen signaleren en verwerken komt hierdoor onder druk te staan. Het blijft belangrijk om aandacht te houden voor monitoring en detectie van malafide activiteiten en het tijdig adresseren van kwetsbaarheden.

- **Verhoging risico's op digitale indringers door toename van pogingen tot phishing en (CEO-) fraude op zowel zakelijke als privé-omgevingen**. Aanvallers maken graag misbruik van actuele thema's, zeker bij social engineering aanvallen. Zo zijn er meerdere criminele groepen, zoals de Oost Europese groep TA505, die COVID-19 cq Corona als thema gebruiken voor hun phishing e-mails of inspelen op het (door ziekte) uitvallen van Key functionarissen bij CEO-fraudes. Instellingen kunnen inspelen op misbruik van actueel thema "COVID-19 / Corona" met extra aandacht voor awareness.

- **Verhoging risico op onterecht uitbetaalde facturen en andere geldbedragen.** Door het thuiswerken kunnen interne controles zoals het vier ogen principe onder druk staan en minder scherp worden uitgevoerd. Instellingen kunnen voorkomen dat gelden ten onrechte worden uitbetaald door extra aandacht te besteden aan Security awareness, alsmede extra (geautomatiseerde) controles op facturen en uitgaande geldstromen, bijvoorbeeld door het toepassen van data-analyse technieken.

- **Verhoging risico op digitale indringers door work-arounds.** Met thuiswerken vervaagt de grens tussen privé en werk; daarmee ontstaat er een verhoogd risico dat medewerkers zich niet aan het IB-beleid houden en leidt o.a. tot risico's op het gebied van data-lekken. Het sturen van gevoelige bedrijfsinformatie naar persoonlijke email of apparatuur is hierdoor nu een extra aandachtspunt voor instellingen.

- **Verhoging risico op operationele problemen in geval van grotere uitval van medewerkers waaronder IT Security personeel zoals medewerkers Security Operations Center (SOC).** Bijkomend risico voor de werking van het SOC is verder een combinatie van een hoge hoeveelheid externe verbindingen met het bedrijfsnetwerk, een lagere operationele bezetting en een toename in cyber-aanvallen. Dit terwijl de activiteiten binnen een SOC, waaronder het hebben van goede security logging & monitoring al een aandachtspunt vormen.

- **Verhoging risico dat kwetsbaarheden binnen de IT omgeving niet tijdig worden geadresseerd doordat verbeteringen en patches niet (of later dan gebruikelijk) uitgevoerd worden**. Door de werkdruk voortkomend uit de pandemie kan het voorkomen dat noodzakelijke upgrades en verbeteringen voor applicaties en IT infrastructuur worden uitgesteld. De activiteiten van het SOC kunnen dan ook als 'cruciaal' worden aangemerkt.

- **Verhoging risico dat het gebruikelijke kwaliteits- en/of security-niveau van service providers niet gegarandeerd kan worden door (langdurige) afwezigheid van personeel.** Hierbij kan ok gedacht worden aan de garandering van de toegankelijkheid van de VPN verbindingen die door de service providers worden verleend. Tevens spelen er concentratierisico's in de onder uitbesteding aangezien een probleem bij één (IT) Service Provider een breed effect kan hebben. Het kan voor instellingen belangrijk zijn aandacht te hebben voor de toenemende grotere verantwoordelijkheid door de grotere afhankelijkheid van externe service providers.

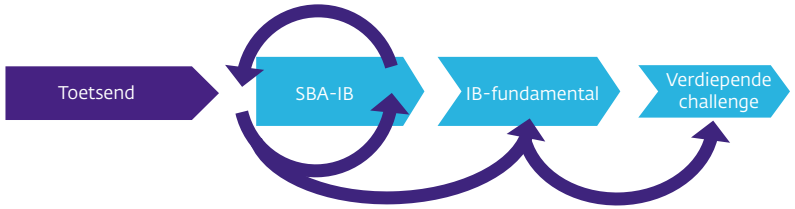
- **Verhoging van het risico dat falende beheersmaatregelen niet transparant worden of later dan gebruikelijk inzichtelijk.** Meerdere instellingen geven aan moeite te hebben met tijdige afronding van rapportages (bijv. controls testing, jaarwerk en FTK-staten). Door tijdsdruk of onvoldoende operationele bezetting (bijvoorbeeld door ziekte) kunnen reguliere beheersmaatregelen onder druk komen te staan of worden mitigerende maatregelen niet transparant genomen. Dit kan gedurende een langere periode een operationeel risico vormen. Het kan belangrijk zijn om aandacht te blijven besteden aan het uitvoeren van adequaat risicomanagement. Ook dient aandacht besteed te worden aan het vastleggen van adequate audit trails, zodat effectiviteit van interne controlemaatregelen (achteraf) kan worden aangetoond en werknemershandelingen traceerbaar blijven.

- **Belangrijk issue op monitoring van hoge autorisaties/rechten bij werknemers van instellingen.** Door uitval (ziekte, ontslag, niet vervangen van personeel, etc), ontvangen bestaande werknemers tijdelijk extra verantwoordelijkheden/ taken dan uit hoofde van hun huidige functie noodzakelijk danwel gewenst is. De tijdelijk extra verstrekte rechten dienen adequaat afgewogen te zijn (obv risico-analyse) alsmede adequaat te worden gemonitord. Dit is niet altijd het geval, waardoor je een securityrisico loopt. **Dit issue heeft ook impact op de werking van IT General Controls.**

DNB geeft verder op haar website https://www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-verzekeren/nieuwsbrief-verzekeren-maart-2020/index.jsp aan wat zij ten aanzien van het business continuity management verwacht van de onder haar toezicht staande instellingen.

2 Vooruitblik

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 inrichting van hun informatiebeveiliging. De komende jaren hanteert DNB verscheidene onderzoeksmethoden met betrekking tot het onderwerp informatiebeveiliging en cybersecurity binnen de sector. De onderzoeksmethoden vormen een samenhangend toetsingskader en hebben een onderling versterkend effect. De onderzoeksmethoden zijn hieronder beschreven.



2.1 Sectorbrede Analyse Informatiebeveiliging (SBA-IB)

De SBA-IB betreft een sectorbrede uitvraag op basis van de Good Practice Informatiebeveiliging waarbij instellingen de volwassenheidsniveaus van de 58 controls scoren en risico-indicatoren in kaart brengen aan de hand van een vragenlijst en een self-assessment. Instellingen leveren in principe in de SBA-IB geen ondersteunende documentatie aan.

2.2 IB-fundamental

Het IB/Cyber fundament onderzoek betreft het 'reguliere' IB onderzoek dat DNB sinds 2010 uitvoert bij een selectie van instellingen. Input op basis van het SBA-IB onderzoek draagt bij aan de selectie voor het IB/Cyber fundament onderzoek.

Dit onderzoek richt zich op het aanwezig zijn van een IB-fundament bij instellingen waarin ook uitbesteding fundamenteel wordt beheerst. Instellingen leveren een self-assessment aan, op basis van de Good Practice Informatiebeveiliging, met complete onderbouwing/dossiervorming, voorzien van een onafhankelijke validatie (door bijvoorbeeld een interne of externe auditor of sleutelfunctiehouder). DNB beoordeelt het self-assessment en de daarbij behorende onderbouwing en voert op locatie een 'challenge' uit t.a.v. de gerapporteerde volwassenheidsniveaus. Dit onderzoek leidt tot een rapport met bevindingen en een terugkoppeling van de door DNB verwerkte volwassenheidsniveaus.

2.3 IB/Cyber verdiepend

Het IB/Cyber verdiepend onderzoek wordt uitgevoerd bij een beperkt aantal instellingen en wordt op maat ingestoken op basis van de inzichten van het IB fundament. Hierbij vindt een verschuiving plaats van 'controls based' naar 'threat-based' onderzoek. Voor elk verdiepend onderzoek wordt vastgesteld welke onderdelen van het toetsingskader Informatiebeveiliging het meest effectief zijn om diepgaand on-site te challengen. Hierbij kan DNB gebruik maken van onderzoekstechnieken als data-analyse en process mining.

Naast deze onderzoeksmethoden zal DNB de komende periode ook nadrukkelijk aandacht besteden aan onderlinge samenwerking tussen de instellingen, hetgeen DNB als essentieel ziet voor de financiële sector om cyberdreigingen het hoofd te kunnen bieden.

Feedbackloop Good Practice IB

DNB wil rond deze Good Practice samen met de sectoren invulling gegeven aan een "feedback loop", waarbij instellingen input kunnen leveren om de voorbeelden actueel te houden.

DNB heeft daartoe een e-mail adres ECOPIT@DNB.NL beschikbaar gesteld. DNB verrijkt de Good Practice op grond van resultaten uit haar onderzoeken (geanonimiseerd) en verwacht dat instellingen zelf voorbeelden verzamelen en inbrengen bij ontmoetingen met DNB (seminars). Bij de mitigatie van cyber dreigingen is samenwerking tussen financiële instellingen essentieel. Indien u als instelling goede voorbeelden heeft van maatregelen waar de andere instellingen van kunnen leren, dan vernemen wij dat graag. In 2020 wordt de Good Practice IB geactualiseerd en nemen we uw nieuwe goede voorbeelden hierin mee.

3 Achtergrond bronnen IB-monitor

3.1 IB-onderzoeken DNB

Sinds een aantal jaren onderzoekt DNB de kwaliteit van informatiebeveiliging en cybersecurity binnen de 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[7] gepubliceerd.

DNB voert elk jaar IB-onderzoeken uit bij een selectie van Verzekeraars en Pensioenfondsen om het volwassenheidsniveau vast te stellen van de beheersing van Informatiebeveiliging bij die instellingen. De waarnemingen uit deze onderzoeken zijn de basis voor deze jaarlijkse IB-monitor.

In de Q&A Informatiebeveiliging wordt aangegeven dat conform art. 3.17 Wet Financieel Toezicht, juncto artikel 20 Besluit prudentiële regels en artikel 143 Pensioenwet juncto artikel 138 Wet verplichte beroepspensioenregeling, instellingen onder toezicht van DNB beschikken over adequate procedures en maatregelen ter beheersing van IT-risico's. Het gaat hierbij onder meer om het waarborgen van de integriteit, voortdurende beschikbaarheid en de beveiliging van geautomatiseerde gegevens. Adequaat betekent in dit verband dat de procedures en maatregelen zijn gebaseerd op de aard, omvang en complexiteit van de risico's van de activiteiten van de instelling en de complexiteit van haar organisatiestructuur.

Om aan deze bepaling te kunnen voldoen hebben instellingen op grond van een risicoanalyse beheersingsmaatregelen getroffen op het gebied van informatiebeveiliging. 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*).

Daarnaast evalueren de instellingen periodiek en aantoonbaar – als onderdeel van hun risicomanagement proces (Riskmanagement cycle) – in hoeverre de getroffen beheersingsmaatregelen in opzet, bestaan en werking effectief zijn om de voortdurend veranderende risico's op het gebied van informatiebeveiliging en cyberdreigingen het hoofd te bieden. Daar waar nodig worden beheersingsmaatregelen verbeterd of vervangen door betere maatregelen. De instellingen richten hun Governance en Organisation in om de aansturing hiervan te bewerkstelligen. Tevens zorgen instellingen ervoor dat zij 'in control' zijn op het gebied van informatiebeveiliging bij uitbesteding (Outsourcing) en Testen zij in hoeverre zij weerbaar zijn tegen cyberdreigingen.

De Good Practice IB geeft de instellingen handvatten, te weten beheersingsmaatregelen en voorbeelden, waarmee zij kunnen voldoen aan de wettelijke bepalingen om de integriteit, voortdurende beschikbaarheid en beveiliging van de geautomatiseerde gegevensverwerking te waarborgen.

7 https://www.toezicht.dnb.nl/3/50-203304.jsp

In de onderzoeken van 2019 is met name aandacht geweest voor de handvaten ten aanzien van de 'rol van het bestuur' en vier nieuwe beheersingsmaatregelen die in 2019 in de Good Practice IB zijn geïntroduceerd. Dit zijn:

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, opdat het gewenste informatiebeveiligingsniveau niet in gevaar komt.
4. Penetration testing and ethical hacking: Testen van de weerbaarheid van de instelling tegen cyberdreigingen.

Deze focus op vulnerability management, testen van de weerbaarheid en de rol van het bestuur is terug te zien in de belangrijkste waarnemingen in deze IB-monitor.

De beheersmaatregel *empolyee awareness* wordt over het algemeen door de financële instellingen voldoende ingevuld en komt daardoor niet terug in de belangrijkste waarnemingen van DNB. Wel vormt zij een extra aandachtspunt in de huidige Corona Pandemie. Zie daartoe de waarneming die aanvullende aandachtspunten geeft ten aanzien van de Corona Pandemie.

3.2 TIBER en Incident meldingen

Sinds juni 2016 is DNB vanuit haar centralebankfunctie samen met de sector bezig met TIBER-NL, een programma om financiële instellingen weerbaarder te maken tegen cyberaanvallen. Relevante ervaringen en beelden opgedaan uit dit programma zijn ook meegenomen in deze IB-monitor.

Uitgedacht in 2016, is in 2017 de eerste versie van het Threat Intelligence Based Ethical Red Teaming framework voor Nederland uitgebracht (TIBER-NL). Belangrijk onderdeel zijn hacktests op productiesystemen, op basis van actuele dreigingsinformatie. Het framework beschrijft hoe Nederlands belangrijkste financiële instellingen zich vrijwillig kunnen laten testen tegen actuele en zeer geavanceerde cyberaanvallen. De testen worden onder coördinatie van DNB uitgevoerd. De ontwikkeling van de documentatie binnen het framework gebeurt in nauwe samenwerking met zowel de partijen uit de financiële sector als partijen uit de security sector. Doel is om zo de cyber weerbaarheid van de belangrijkste financiële instellingen in Nederland te vergroten.

TIBER-NL is gericht op instellingen uit de financiële kerninfrastructuur. In eerste instantie waren dat alleen banken, en sinds 2018 ook verzekeraars en pensioenfondsen. Het project is samen met de sector opgezet en wordt ook mede gefinancierd door de sector.

In de afgelopen drie jaar is het framework succesvol gebruikt in een twintigtal testen in Nederland. In 2018 is het framework door de ECB overgenomen en wordt in een aantal Europese landen geïmplementeerd. Met de implementatie van TIBER in de andere Europese landen zijn nu internationale grensoverschrijdende testen mogelijk geworden.

Recent is een nieuwe versie van het TIBER framework gepubliceerd.[8] De belangrijkste aanpassingen in het raamwerk betreft de aansluiting van de intelligence over de instelling (waar zou de aanvaller gebruik van kunnen maken?) en het testscenario dat gespeeld wordt. Ook is er meer nadruk gelegd op het na afloop van de test leren van de ervaringen. Zo weet de instelling na afloop van de test nog beter waar het de verdediging tegen cyberdreigingen kan versterken.

8 https://www.dnb.nl/binaries/TIBER%20NL%20Guide_tcm46-387212.pdf

Naast de beelden en ervaringen uit TIBER zijn in deze IB-monitor ook ervaringen met gemelde incidenten meegenomen. Voor deze IB-monitor is daarbij breder gekeken dan de incidenten die DNB ontvangt. Als bron voor deze IB-monitor is met name gebruik gemaakt van een overzicht van incidentmeldingen en dreigingsbeelden van het OSINT dashboard van EUROPOL en de Dutch FI ISAC.

3.3 EBA en EIOPA

Cyber risk is de afgelopen jaren een belangrijk onderwerp voor internationale standard-setting bodies geworden. Denk aan de G7 (the Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector en Fundamental Elements for Threat-led Penetration Testing), the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (rapport van IOSCO Cyber Task Force), the Financial Stability Institute (Cyber lexicon), BCBS (Cyber-resilience rapport: Range of practices) en IAIS (Application Paper on Supervision of Insurer Cybersecurity).

Daarnaast hebben in opdracht van de Europese Commissie ook de European Supervisory Authorities (ESA's) het onderwerp Cyber nadrukkelijker geadresseerd in guidelines. In 2019 heeft de European Banking Authority (EBA) Guidelines on ICT and security risk management gepubliceerd. De European Insurance and Occupational Pensions Authority (EIOPA) heeft recent voor consultatie de draft Guidelines on information and communication technology (ICT) security gepubliceerd. Beide Guidelines geven richtlijnen voor de sector hoe zij hun Informatiebeveiliging moeten inrichten. De beide guidelines zijn waar mogelijk op elkaar afgestemd.

De Good practice IB van DNB past in de lijn van de beide guidelines van EBA en EIOPA.

DNB heeft de afgelopen jaren een actieve rol in de werkgroepen die de guidelines hebben opgesteld en zich ook breder bezighouden met IT en Cyber binnen zowel EBA als EIOPA. De beelden en ervaringen die opgedaan zijn in deze en andere (internationale) werkgroepen zijn waar relevant meegenomen in deze IB-monitor.

Bijlage Dreigingsbeeld 2020

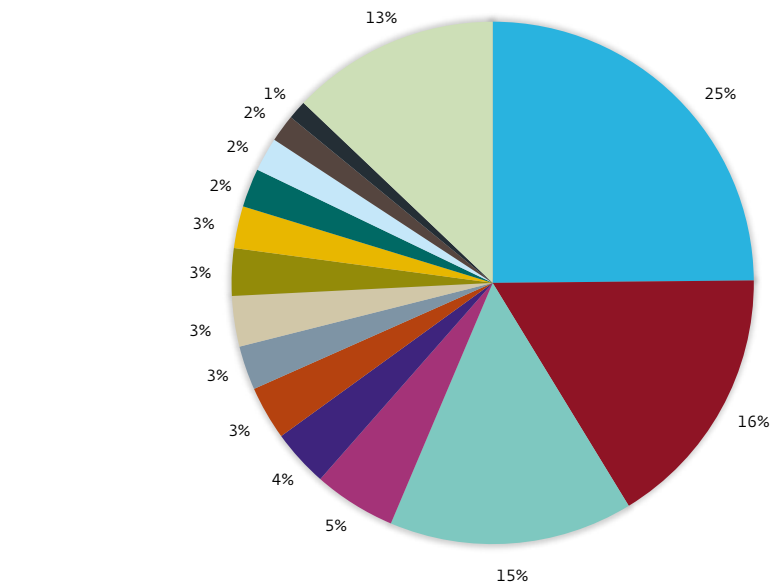
Dreigingen in het kader van cybersecurity zijn talrijk. Te talrijk om hier allemaal op te sommen. Op basis van de verschillende beelden en ervaringen opgedaan uit de genoemde bronnen die voor deze IB-monitor zijn gebruikt, beschouwt DNB voor 2020 met name de volgende dreigingen als vaak voorkomend, kansrijk en van potentieel grote impact op de financiële sector.

Het EC3 – onderdeel van het European Cybercrime Centre van EUROPOL – geeft wekelijks op Open Source gebaseerde en geautomatiseerde (OSINT) dashboards uit met algemene aanvalstechnieken die in verschillende sectoren zijn gebruikt. Uit deze verschillende dashboards over het afgelopen jaar (2019/2020) komt naar voren dat phishing een aanvalstechniek is die het meest voorkomt bij IB-incidenten. Phishing komt voor in twee vormen: gericht op een grote groep (phishing) en specifiek gericht op bepaalde personen binnen een organisatie (Spear Phishing). DNB herkent deze beide aanvalstechnieken ook als veel voorkomend bij de financiële instellingen. Bij met name Spear Phishing stellen wij vast dat steeds veelvuldiger gebruik wordt gemaakt van de verkoop van persoonlijke data, soms gelekt, vaak gewoon online beschikbaar, uit onder andere databases van bedrijven, sociale netwerken en websites. Deze informatie wordt gebruikt in combinatie met 'social engineering': de werkwijze om mensen te manipuleren om persoonlijke en gevoelige informatie over hun werkgever af te staan.

Naast de aanvalstechnieken uit de dashboards van OSINT ziet DNB zelf dat financiële instellingen kwetsbaar zijn via partijen waaraan werkzaamheden zijn uitbesteed (dienstverleners) en die toegang hebben tot of die behoren tot hun (kern) infrastructuur. Hierbij kan worden gedacht aan dienstverleners als cloud-, Infrastructuur- en datacenteropslag, call centers, betalingssystemen en werkplekfaciliteiten. De financiële instelling kan daarbij via de dienstverlener zelf

Figuur 7 Aanvalstechnieken OSINT afgelopen jaar

In procenten



Bron: verschillende dashboards door het afgelopen jaar (2019/2020) heen van OSINT EUROPOL. De dashboards zijn opgesteld uit verschillende bronnen over de genoemde topics in een bepaalde tijdsspanne.

het doel van een digitale aanval zijn of geraakt worden door een digtale aanval gericht op de dienstverlener waarvan de financiële instelling onbedoeld ook het slachtoffer wordt.

Ten aanzien van bepaalde dienstverleners komen concentratierisico's voor. Een klein aantal dienstverleners werkt namelijk voor een groot aantal financiële instellingen. Met name deze partijen zijn een aanlokkelijk doel voor aanvallers. De aanvallers kunnen door deze geconcentreerde dienstverleners aan de ene kant bij meerdere financiële instellingen binnen komen. Aan de andere kant kunnen aanvallers door één geconcentreerde dienstverlener plat te leggen, een groot deel van de financiële sector raken. De beheersing door de financiële instellingen van hun uitbestedingen blijft ook in dit opzicht van groot belang.

Verder vraagt DNB naast externe dreigingen ook aandacht voor relevante interne dreigingen vanuit medewerkers in de eigen organisatie. Dat kan op drie manieren.

1. Interne medewerkers kunnen opzettelijk (on)geautoriseerde toegang krijgen tot relevante interne systemen en daaruit data stelen, manipuleren of afluisteren. Denk hierbij aan medewerkers die uit zijn op persoonlijk gewin of medewerkers die bijvoorbeeld door een reorganisatie ontevreden zijn. Ook zijn gevallen bekend van medewerkers die infiltreren in een financiële instelling vanuit een criminele organisatie.
2. Het komt steeds vaker voor dat goedwillende medewerkers worden gemanipuleerd door criminele partijen, die zich bijvoorbeeld voordoen als collega's of leidinggevenden, om ongewild data te verstrekken of toegang te geven tot systemen. CEO fraude is hier een voorbeeld van.
3. Een toenemende interne dreiging is dat risico's op potentieel kwetsbare VPN verbindingen, laptops en mobiele telefoons toenemen doordat medewerkers steeds vaker thuis werken. Medewerkers werken daarbij vaak mobieler, niet alleen thuis maar ook in de trein, op openbare locaties en bij klanten. Hierdoor neemt ook het risico van verlies, diefstal van de devices toe, waardoor kwetsbare VPN verbindingen toegankelijker worden.

Voor de goedwillende (mobiele) medewerkers kunnen awarenessprogramma's helpen die mensen scherper te maken op het oplettend omgaan met devices en gevoelige informatie. Voor de kwaadwillende medewerker zal verder moeten worden gekeken naar bijvoorbeeld specifieke tooling die afwijkende gedragspatronen van medewerkers op het netwerk kunnen detecteren.

Eenmaal binnen, bijvoorbeeld via één van de eerder genoemde andere methoden, ziet DNB dat naast het stelen en manipuleren van data ook het afpersen voor financieel gewin, 'ransomware' is toegenomen. Verder is zichtbaar dat door geavanceerde aanvallende partijen langdurige infiltraties van onder andere (bank-) systemen plaats vinden. De aanvallende partijen gebruiken deze tijd om de instelling beter in kaart te krijgen en via steppingstones bij hun beoogde doel te komen.

Welke dreigingen voor individuele instellingen relevant zijn, hangt af van de specifieke omgeving waarin een instelling opereert. Iedere instelling heeft zijn eigen interne (systeem-)landschap en diensten die het levert. Voor het goed onderkennen van de specifieke dreigingen waarmee een instelling te maken heeft, is het relevant de relevante dreigingen in kaart te brengen. Onder het kopje "Cyberhygiëne blijft cruciaal" wordt hier verder op ingegaan.

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) 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 haar oordeel een goede toepassing inhouden van de regels waarop deze good practice betrekking heeft.

Met een good practice beoogt de Nederlandsche bank N.V. 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 DNB 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.