Rapport

Melden van incidenten

Onderzoek bij beleggingsondernemingen en een beheerder van beleggingsinstellingen

Mei 2023

AFM

Inhoudsopgave

Inleiding 3

De deep dive incidenten 5

Bevindingen 5

Good practices 8

Conclusie en vervolgstappen 8

Inleiding

Sinds 2020 besteedt de Autoriteit Financiële Markten (AFM) extra aandacht aan incidenten bij beleggingsondernemingen[1] en bij beheerders van beleggingsinstellingen en/of icbe's (ondernemingen). Dit onderwerp kreeg de aandacht van de AFM doordat relatief weinig incidentmeldingen bij de AFM binnenkwamen, de AFM heeft hierom een project gestart.

Voor een goed werkende assetmanagementmarkt is het van groot belang dat ondernemingen incidenten tijdig bij de AFM melden. De AFM gebruikt incidentmeldingen om proactief te reageren op signalen en in te springen op ontwikkelingen in de sector. Incidenten stellen de AFM in staat een bijdrage te leveren aan het oplossen van problemen. Een gezonde en goed werkende sector is van belang voor ondernemingen en voor beleggers.

Ondanks de extra aandacht van de AFM is het aantal incidentmeldingen niet toegenomen. Het doel van dit project is het onderzoeken van de hieraan achterliggende oorzaken De AFM heeft een aantal acties ondernomen. Allereerst heeft de AFM een oproep[2] op haar website geplaatst en ondernemingen een brief over incidenten en de omgang met incidenten gestuurd. Daarnaast heeft de AFM gesprekken gevoerd met individuele ondernemingen en brancheverenigingen en hiervan een terugkoppelingsbrief per e-mail verstuurd die op haar website is gepubliceerd[3].

Tot slot heeft de AFM in het tweede kwartaal van 2022 een *deep dive* onderzoek uitgevoerd waarbij gekeken is naar de wijze waarop geselecteerde ondernemingen omgaan met incidenten en de incidentmeldingsplicht. Dit *deep dive* onderzoek kwam voort uit de constatering dat eerdere acties niet leidden tot een significante toename in het aantal incidenten dat werd gemeld. De ondernemingen hebben een individuele terugkoppeling ontvangen van de uitkomsten van de *deep dive*. Waar nodig heeft de AFM maatregelen genomen.

In dit rapport worden de belangrijkste bevindingen uit de *deep dive* en een aantal *good practices* beschreven. Deze zijn bedoeld om ondernemingen te stimuleren tot verbetering van de wijze waarop zij met incidenten omgaan.

Wettelijk kader

De aandacht van de AFM is gebaseerd op de bepalingen ten aanzien van de integere en beheerste bedrijfsvoering in de Wet op het Financieel Toezicht (Wft) en de uitwerking daarvan in het Besluit Gedragstoezicht financiële ondernemingen Wft (BGfo). Op grond van artikel 4:11, eerste en vierde lid, Wft dient er een adequaat beleid te worden gevoerd dat ervoor zorgt dat een integere uitoefening van het bedrijf wordt gewaarborgd. Op grond van artikel 4:14, eerste lid, Wft dient de bedrijfsvoering zodanig te worden ingericht dat deze een beheerste en integere uitoefening van zijn of haar bedrijf wordt gewaarborgd.

[1] Met uitzondering van beleggingsondernemingen die uitsluitend beleggingsactiviteiten verrichten.
[2] https://www.afm.nl/nl-nl/sector/actueel/2020/december/oproep-melden-incidenten
[3] https://www.afm.nl/nl-nl/sector/actueel/2021/september/onderzoek-meldplicht-incidenten-asset-managementsector

Op grond van artikel 24, eerste lid, BGfo dient een beleggingsonderneming te beschikken over procedures en maatregelen met betrekking tot de behandeling en administratieve vastlegging van incidenten. Verder moeten beleggingsondernemingen volgens artikel 24, tweede lid, BGfo maatregelen nemen om risico's te beheersen als incidenten zich voordoen en om herhaling te voorkomen. Op grond van artikel 24, derde lid, BGfo dient een beleggingsonderneming de AFM onverwijld over incidenten te informeren.

Een incident is gedefinieerd in artikel 1 BGfo:

> *"Een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van een financiële onderneming."*

In de brief van 23 december 2020[2] gaf de AFM een aantal voorbeelden van (mogelijke) incidenten. Deze voorbeelden zijn:

<u>Informatiebeveiliging</u>

- Diefstal of verlies van ICT-middelen met vertrouwelijke data van de onderneming
- Ongeautoriseerde toegang tot de ICT-infrastructuur van de onderneming, eventueel met ongeautoriseerde transacties tot gevolg.
- De installatie van malware op systemen van de onderneming.
- Een datalek, waarbij vertrouwelijke informatie terecht is gekomen in het publieke domein.
- DDoS aanvallen of de dreiging daarvan.

<u>Integriteitsincidenten</u>

- Een werknemer of beleidsbepaler wordt verdacht van en/of vervolgd voor een strafbaar (economisch) feit.
- Een beleidsbepaler die (in het verleden) een vergrijpboete opgelegd heeft gekregen voor het opzettelijk indienen van een onjuiste of onvolledige belastingaangifte.
- Een werknemer die een greep uit de kas doet.
- De financiële onderneming die een boete opgelegd krijgt van een andere (buitenlandse) toezichthouder dan de AFM.
- De financiële onderneming waarvan cliënten betrokken raken bij ernstige (economische) strafbare feiten.

Hierbij is van belang dat de onderneming beoordeelt in hoeverre het (mogelijke) incident een ernstig gevaar vormt voor de integere uitoefening van het bedrijf.

De deep dive incidenten

In de brief van 29 september 2021[4] heeft de AFM een *deep dive* onderzoek aangekondigd naar het melden van incidenten door ondernemingen. Gedurende mei en juni 2022 is bij vijf geselecteerde ondernemingen onderzoek gedaan naar de omgang met incidenten. De beheerder van beleggingsinstellingen en de beleggingsondernemingen (ondernemingen) zijn risicogestuurd geselecteerd. Met de *deep dive* heeft de AFM een onderzoek uitgevoerd naar de mogelijke oorzaken van het relatief lage aantal gemelde incidenten bij de AFM. In het onderzoek is gekeken naar de wijze waarop de geselecteerde ondernemingen een beleid en maatregelen ten aanzien van incidenten hebben geïmplementeerd en in hoeverre zij de incidentmeldingsplicht naleven.

Onderzoeksmethode

Het onderzoek baseerde zich op een documentenanalyse van het bestaande beleid en maatregelen rondom het melden van incidenten. Met behulp van een *walkthrough* sessie, waarbij de AFM in gesprek met de ondernemingen door hun beleid en de procedures rondom incidenten is gelopen, is per onderneming bepaald welke documentatie relevant is voor de *deep dive*. Omdat de wettelijke normen voor incidenten zogenaamde 'open normen' zijn en ondernemingen zodoende vrij zijn om een eigen invulling aan deze normen te geven, verschilden de documenten per onderneming.

Voorbeelden van bestudeerde documenten zijn het beleid rond incidenten, het compliance handboek en het incidentregister. Aan de hand van een beoordelingskader is de relevante documentatie geanalyseerd en zijn de ondernemingen met elkaar vergeleken. Het beoordelingskader bevat enerzijds *compliance*-aspecten (in hoeverre ondernemingen voldoen aan de wettelijke normen) en anderzijds is gekeken naar elementen van organisatiecultuur, bijvoorbeeld het durven uitspreken door medewerkers of voorbeeldgedrag vanuit leidinggevenden.

Bevindingen

Hieronder worden de belangrijkste observaties en bevindingen van het onderzoek onder de vijf ondernemingen besproken en *good practices* die in kaart zijn gebracht, gedeeld.

De definitie van incident wordt niet altijd uitgewerkt in het beleid

In het beleid van ondernemingen werd niet in alle gevallen een uitwerking gegeven van wat onder een (potentieel) incident verstaan wordt. Ook heeft de AFM grote verschillen geconstateerd in diepgang en reikwijdte van de definitie. Hierdoor kan het voor medewerkers, die op basis van dit beleid werken, onduidelijk zijn welke potentiële gebeurtenissen als incident kwalificeren. Dit brengt het risico dat de onderneming niet (tijdig) in staat is om aan de incidentmeldingsplicht te voldoen.

[4] https://www.afm.nl/~/profmedia/files/nieuws/2021/terugkoppelingsbrief_inventarisatie_incidenten.pdf

Het is derhalve belangrijk dat ondernemingen gebeurtenissen in de bedrijfsvoering toetsen aan de definitie van incident zoals weergegeven in artikel 1 BGfo.

Procedures en maatregelen niet in alle gevallen adequaat

De AFM is tijdens de *deep dive* een aantal voorbeelden tegengekomen van maatregelen en procedures die niet adequaat waren. Bij de ondernemingen waar dit het geval was, ontbrak het aan een beschrijving van rollen en verantwoordelijkheden of instructies hoe en waar medewerkers incidenten kunnen melden.

Ondernemingen moeten op grond van artikel 24 BGfo beschikken over procedures en maatregelen voor de omgang met incidenten. De AFM verwacht van ondernemingen dat de procedures en maatregelen als bedoeld in artikel 24 BGfo voldoende duidelijkheid bieden om gebeurtenissen in de bedrijfsvoering te kunnen evalueren tegen de norm voor (meldingsplichtige) incidenten. Hiervoor is het nodig dat rollen en verantwoordelijkheden zijn beschreven, dat duidelijk is wat de criteria zijn waarmee gebeurtenissen in de bedrijfsvoering worden geëvalueerd en dat het duidelijk is hoe en waar medewerkers (potentiële) incidenten kunnen melden.

De beoordeling van gebeurtenissen in de bedrijfsvoering niet altijd op basis van criteria

De AFM raadt ondernemingen aan om in hun beleid vast te leggen wat de criteria zijn waarmee gebeurtenissen in de bedrijfsvoering getoetst worden aan de wettelijke norm voor incidenten. Het kan per onderneming verschillen wat deze gedragingen of gebeurtenissen zijn en wanneer deze een ernstige bedreiging voor de integere bedrijfsvoering vormen. De AFM heeft daarom in de bovengenoemde “Terugkoppelingsbrief inventarisatie incidenten” van 29 september 2021 ondernemingen aangeraden om criteria vast te stellen als basis voor de evaluatie van gebeurtenissen in de bedrijfsvoering.

Hoewel meerdere manieren denkbaar zijn om gebeurtenissen in de bedrijfsvoering te toetsen aan de norm voor incidenten, vindt de AFM het belangrijk dat dit op een gestructureerde en consistente wijze plaatsvindt. Daarom raadt de AFM ondernemingen aan om deze wijze formeel vast te leggen in het beleid rondom de behandeling van incidenten.

Herleidbaarheid van besluitvorming kan worden verbeterd

Tijdens de *deep dive* is de AFM ondernemingen tegengekomen waarbij de herleidbaarheid van de besluitvorming, rondom gebeurtenissen die mogelijk als een incident kwalificeren, onvoldoende was. Het uiteindelijke besluit of een gebeurtenis als incident bij de AFM wordt gemeld, wordt veelal door de directie van de onderneming genomen.

De AFM raadt ondernemingen aan om (bestuurlijke) besluitvorming en de overwegingen die ten grondslag liggen aan het al dan niet melden van een gebeurtenis als incident, vast te leggen in bijvoorbeeld de notulen van een bestuursvergadering. Deze vastlegging faciliteert een adequate verantwoording aan onder meer toezichthouders en draagt bij aan consistentie in de besluitvorming.

Niet-operationele incidenten vereisen soms meer aandacht

Een aantal ondernemingen die zijn onderzocht, zijn sterk IT-gedreven. Het is de AFM opgevallen dat deze ondernemingen vaak uitgebreide procedures en maatregelen hebben om potentiële incidenten te detecteren, te evalueren en uiteindelijk te melden bij de AFM als dat nodig is. Ook wanneer deze ondernemingen (een deel van) hun IT hadden uitbesteed. In een aantal gevallen was het bij deze ondernemingen wel zo dat de procedures en maatregelen in het bijzonder gericht waren op incidenten van operationele aard. De AFM wijst erop dat deze procedures en maatregelen ook moeten worden toegepast op potentiële incidenten van niet-operationele aard. Denk hierbij bijvoorbeeld aan incidenten van sociale aard zoals ongewenst gedrag op de werkvloer.

Een aantal ondernemingen leunt relatief zwaar op het individuele oordeel van hun medewerkers.

Hoewel de AFM geen oordeel heeft over de professionaliteit van de medewerkers van de ondernemingen die onderzocht zijn, laat een aantal ondernemingen relatief veel verantwoordelijkheid aan de medewerkers om te beoordelen of een gebeurtenis een (potentieel) incident is. Het risico hiervan is dat de evaluatie van gebeurtenissen door ondernemingen ad hoc en niet consistent plaatsvindt. Ondernemingen gaven in een aantal gevallen aan dat medewerkers goed opgeleid zijn en zodoende weten wat er moet worden gemeld of wezen op de open cultuur binnen de organisatie die medewerkers moet faciliteren om incidenten te melden.

De AFM roept ondernemingen op om op basis van heldere procedures en maatregelen medewerkers actief en periodiek te informeren over wat er van hen verwacht wordt ten aanzien van het melden van gebeurtenissen in de bedrijfsvoering, ook bij wijzigingen in het beleid. Ook kunnen ondernemingen ervoor kiezen om in een medewerkersonderzoek aandacht te besteden aan incidenten en/of de open cultuur binnen de organisatie. Zodoende kunnen ondernemingen zicht krijgen op of sprake is van een open cultuur en de mate waarin medewerkers zich vrij voelen fouten te delen.

Het is voor ondernemingen niet altijd duidelijk welke informatie nodig is voor een incidentmelding bij de AFM.

Tijdens de *deep dive* is aan ondernemingen gevraagd in hoeverre er verbetermogelijkheden voor de AFM zijn ten aanzien van dit onderwerp. De beleving wat nodig is aan informatie en onderbouwing bij een melding verschilt tussen ondernemingen. Ook de wijze waarop incidentmeldingen worden gedaan verschilt. Bijvoorbeeld in gesprek met de toezichthouder, per e-mail of via een webformulier.

Ondernemingen noemen het gebrek aan terugkoppeling van de AFM na het doen van een melding. Hierdoor weten zij niet of een melding op een juiste wijze wordt verricht of dat aanvullende informatie nodig is. Voor ondernemingen is het niet altijd duidelijk wat er gebeurt met hun melding. Aan het einde van dit rapport staat onder ‘Vervolgstappen’ aangegeven wat de AFM met deze feedback doet.

Good practices

De AFM is naast de hierboven beschreven bevindingen een aantal voorbeelden tegengekomen van *good practices.* De *good practices* kunnen bijdragen aan een scherper geformuleerd beleid en de werking daarvan.

- *Het verlagen van de interne drempel om gebeurtenissen te melden en zodoende het melden door medewerkers te stimuleren*; bijvoorbeeld door naast potentiële incidenten ook fouten (events) of 'near misses' intern te laten melden.

- *Naast het 'Hoe' en 'Wat' in het beleid expliciteren 'Waarom' het belangrijk is om incidenten te melden*. Meer begrip achter het doel van het melden kan medewerkers stimuleren meldingen te doen. Ook helpt dit leidinggevenden de boodschap beter uit te dragen naar de organisatie.

- *Een toegankelijke manier van melden creëren door het inzetten van gebruiksvriendelijke tools*; bijvoorbeeld een formulier op intranet met heldere instructie en training hoe medewerkers deze formulieren kunnen invullen. En het hanteren van vaste informatiepunten die moeten worden ingevuld zodat meldingen op consistente wijze worden beoordeeld.

- *Informeren van de melder over de voortgang en uitkomst van de melding*; het expliciteren van de meerwaarde van een melding en duidelijkheid geven over het proces stimuleert medewerkers om (te blijven) melden.

Conclusie en vervolgstappen

De AFM besteedt extra aandacht aan incidenten om een antwoord te krijgen op de vraag waarom er minder incidentmeldingen bij de AFM binnenkomen dan verwacht. Er zijn meerdere oorzaken aan het licht gekomen die ervoor kunnen zorgen dat er minder incidenten bij de AFM worden gemeld dan verwacht. Uit de hierboven genoemde bevindingen blijkt dat er meerdere oorzaken zijn die ervoor kunnen zorgen dat er minder incidenten bij de AFM worden gemeld dan verwacht.

Hieronder staat weergegeven welke vervolgstappen de AFM zet naar aanleiding van dit onderzoek.

- Incidentmeldingen blijven vast onderdeel van doorlopend toezicht. Het onderwerp kan onderdeel (blijven) uitmaken van thematische of *deep dive* onderzoeken. De AFM verwacht dat instellingen aan de hand van dit rapport nagaan of en welke verbeteringen er nodig zijn en deze doorvoeren. De AFM verwacht dat ondernemingen alert zijn op het melden van incidenten.In december 2022 is de definitieve verordening Digital Operational Resilience Act

(DORA) gepubliceerd in het EU-staatsblad. Ondernemingen moeten vanaf 17 januari 2025 aan DORA voldoen. DORA bevat normen over beheer, classificatie en rapportage van ICT-incidenten. Deze normen zijn gedetailleerder dan de huidige normen in de Wft. De AFM roept ondernemingen op om zich te verdiepen in de normen in DORA en tijdig te beginnen met de voorbereidingen om hiermee in compliance te zijn.

- Ondernemingen hebben aangegeven dat het meldingsproces ingewikkeld is, de AFM zal met deze terugkoppeling aan de slag gaan. De AFM gaat na hoe de eenduidigheid van dit proces kan worden verbeterd. De AFM wil ondernemingen er op wijzen dat het vanwege haar risicogestuurd toezicht niet altijd mogelijk is om inhoudelijk op de melding in te gaan.

- De AFM wil ondernemingen onder haar toezicht helpen om het proces voor incidenten intern goed op orde te hebben. Verder is de AFM meerdere malen gevraagd om meer duidelijkheid te geven over incidentmeldingen. Met dit rapport komt de AFM hieraan tegemoet.

Autoriteit Financiële Markten
Postbus 11723 | 1001 GS Amsterdam

Telefoon
020 797 2000

www.afm.nl

Dataclassificatie
AFM - Publiek

Follow us: →

De AFM maakt zich sterk voor eerlijke en transparante financiële markten.

Als onafhankelijke gedragstoezichthouder dragen wij bij aan duurzaam financieel welzijn in Nederland.