Datum	29 september 2021
Ons kenmerk	
Pagina	1 van 5
E-mail	Ondernemersloket@afm.nl
Betreft	Terugkoppelingsbrief inventarisatie incidenten

Geachte heer, mevrouw,

Op 23 december 2020 deed de Autoriteit Financiële Markten ("AFM**"**) een oproep om incidenten te melden. Naast deze oproep heeft de AFM de betreffende beleggingsondernemingen[1] en beheerders van beleggingsinstellingen en/of icbe's ("ondernemingen") een brief ("de brief") gestuurd.

De aandacht voor het onderwerp heeft niet geleid tot een significante toename van het aantal incidentmeldingen bij de AFM. Daarom heeft de AFM de afgelopen periode een inventarisatie gedaan naar hoe ondernemingen omgaan met het melden van incidenten en de incidentmeldingsplicht. Hierbij heeft de AFM gesproken met een aantal ondernemingen en brancheverenigingen.

In dit document worden de bevindingen beschreven die tijdens de inventarisatie naar voren kwamen. Het doel van dit document is drieledig. Ten eerste wil de AFM nogmaals aandacht vragen voor de incidentmeldingsplicht. Daarnaast wil de AFM een aantal aspecten van de incidentmeldingsplicht verder verduidelijken. Tot slot kondigt de AFM een *deep dive* onderzoek naar de omgang met incidenten door ondernemingen aan.

Wanneer is een incident een incident?

Op grond van artikel 1 van het Besluit Gedragstoezicht financiële ondernemingen Wft (**BGfo**) is een incident "*een gedraging of een gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van een financiële onderneming*". Uit de gesprekken die de AFM met de ondernemingen heeft gevoerd, komt naar voren dat het in beginsel duidelijk is wat er met deze definitie wordt bedoeld en hoe de definitie moet worden bezien in de context van de onderneming.

In het BGfo is opgenomen dat ondernemingen de AFM onverwijld informeren over incidenten. Uit de gesprekken met de ondernemingen die de AFM heeft gesproken komt naar voren dat de

[1] Met uitzondering van beleggingsondernemingen die uitsluitend beleggingsactiviteiten verrichten

incidentmeldingsplicht bekend is bij deze ondernemingen. Het is verder duidelijk voor de ondernemingen dat incidenten onverwijld moeten worden gemeld.

In de brief heeft de AFM een aantal voorbeelden genoemd van gedragingen of gebeurtenissen die mogelijk kwalificeren als incident op grond van het BGfo en daarmee meldingsplichtig zijn. De ondernemingen vinden deze voorbeelden duidelijk en onderkennen dat deze voorbeelden kunnen kwalificeren als incident.

Wanneer de AFM het in het vervolg van deze brief heeft over incidenten, heeft zij het, tenzij uitdrukkelijk anders aangegeven, over incidenten in de brede zin van het woord; dus niet alleen de incidenten die onder de hiervoor opgenomen BGfo-definitie vallen. In deze brief ziet de AFM IT-incidenten als de gebeurtenissen in de IT-huishouding van ondernemingen die, afhankelijk van de ernst, een meldingsplichtig incident kunnen vormen in de zin van het BGfo. Het is aan de ondernemingen om de gebeurtenissen in hun IT-huishouding te toetsen aan de BGfo-definitie.

IT-incidenten in relatie tot de meldingsplicht voor incidenten

Tijdens de gesprekken viel het de AFM op dat er bij sommige ondernemingen nog enige onduidelijkheid is over IT-incidenten in relatie tot de meldingsplicht voor incidenten. IT is voor veel financiële ondernemingen een belangrijk onderdeel van hun bedrijfsvoering. Voor veel ondernemingen in de financiële sector is de afhankelijkheid van IT inmiddels zo groot dat zonder IT-voorzieningen de bedrijfsvoering onmogelijk zou zijn.

De AFM begrijpt van een aantal ondernemingen dat IT-incidenten veel impact kunnen hebben en in sommige gevallen de dienstverlening van ondernemingen ook gedurende lange tijd kunnen verstoren. Als gevolg daarvan kan het vertrouwen in de onderneming worden geschaad. In dergelijke situaties kan een IT-incident een bedreiging voor de integere bedrijfsvoering (en dus een ernstig gevaar in de zin van artikel 1 van het BGfo) vormen en moet als gevolg daarvan bij de AFM gemeld worden.

Beleid en maatregelen

De ondernemingen geven aan beleid en procedures te hebben die zien op de omgang met en vastlegging van incidenten. Voor meerdere ondernemingen was de brief aanleiding om het interne beleid en interne procedures en maatregelen tegen het licht te houden en in het geval van uitbesteding van diensten en activiteiten ook in contact te treden met serviceproviders. In een aantal gevallen heeft dit geleid tot aanscherping van bestaand beleid en procedures. Ook vormde de brief bij een aantal ondernemingen aanleiding om onder medewerkers (extra) aandacht te vragen voor risico’s op het gebied van informatiebeveiliging en het melden van incidenten.

Onderdeel van de definitie van incident in artikel 1 van het BGfo is de norm ‘ernstig gevaar’. De AFM verwacht van ondernemingen dat beleid en procedures van een onderneming antwoord geven op de vraag wanneer een gedraging of gebeurtenis een ernstig gevaar voor de integere bedrijfsvoering vormt. Uit de inventarisatie is gebleken dat een aantal ondernemingen hier concreet invulling aan geeft door het

opnemen van zowel kwantitatieve als kwalitatieve criteria waar de individuele incidenten aan worden getoetst.

Ook kwam de AFM tijdens de inventarisatie voorbeelden tegen van ondernemingen die voor de classificering van incidenten gebruik maken van matrices waarin incidenten op basis van *thresholds* worden geplot. Vervolgens wordt daarbij op basis van de classificering het incident op het bijbehorende niveau van de escalatieladder belegd.

Een aantal ondernemingen geeft aan dat het gevaar bestaat dat het beleid rond incidenten door het gebruik van matrices een *afvinklijst* wordt. Daarom hanteren deze ondernemingen (ook) 'open normen' die besproken worden op het moment dat de gebeurtenis of gedraging (het incident) zich voordoet. Tijdens de inventarisatie kwam naar voren dat alle bestuurders bij de invulling van 'ernstig gevaar' de koppeling maken met de reputatie van en het vertrouwen in de onderneming en de sector als geheel.

De AFM ziet het gebruik van matrices met voldoende oog voor 'open normen' als een in opzet goede uitwerking van beleid voor het classificeren van incidenten.

De AFM komt in de praktijk regelmatig ondernemingen tegen die IT-incidenten in een aparte registratie bijhouden. Hierbij is de IT-incidentenregistratie in beheer van bijvoorbeeld een servicedeskfunctie. De AFM wil ondernemingen echter graag meegeven dat ook incidenten in het IT-incidentenregister moeten worden getoetst aan de norm die is opgenomen in het BGfo voor de meldingsplicht voor incidenten.

Een open cultuur biedt kansen om te leren van incidenten

De bestuurders van een aantal ondernemingen herkennen dat sinds de uitbraak van het coronavirus incidenten extra aandacht vragen omdat de aard van de incidenten veranderd is. De ondernemingen geven aan dat door thuiswerken er meer bedreigingen voor de beveiliging van informatie zijn ontstaan. Dit heeft in een aantal gevallen tot incidenten geleid. Dit is in lijn met de uitkomsten van een eerder onderzoek van de AFM naar de risico's van thuiswerken. Een aantal ondernemingen heeft naar aanleiding van het thuiswerken extra onlinetrainingen op het gebied van compliance awareness aangeboden aan medewerkers.

Ondernemingen geven aan dat bij het vaststellen en melden van incidenten zowel de compliance afdeling als de verantwoordelijke bestuurders betrokken zijn. In een aantal organisaties is er een commissie waarin (mogelijke) incidenten besproken en beoordeeld worden.

Een aantal bestuurders van ondernemingen benoemt tijdens de inventarisatie ook de cultuur binnen de onderneming. Deze bestuurders geven aan dat zij zich inspannen om een open cultuur te creëren waarbinnen medewerkers zich niet bezwaard voelen om incidenten intern te melden. Hierbij gaf een aantal bestuurders ook aan dat zij incidenten ook zien als een kans om te leren, zowel voor de medewerker als voor de onderneming. De AFM vindt een open cultuur een belangrijke randvoorwaarde voor een effectieve invulling van de verantwoordelijkheden die ondernemingen hebben ten aanzien van incidenten. De AFM vindt het positief om te zien dat bestuurders van ondernemingen zich voor een open cultuur inspannen.

Een drempel om incidenten te melden

Een beperkt aantal ondernemingen benoemt een drempel om incidenten bij de AFM te melden omdat onduidelijk is waar een dergelijke melding binnen de AFM terecht gaat komen en welke actie de AFM naar aanleiding van de melding onderneemt. De AFM benadrukt dat het een misverstand is dat incidentmeldingen altijd tot handhaving zoals een boete leiden. Het is voor een goed werkende asset managementmarkt namelijk van groot belang dat ondernemingen incidenten tijdig bij de AFM melden.

Het is voor de AFM vooral belangrijk om in het geval van een incident inzichtelijk te krijgen wat de oorzaak van een incident is, hoe een onderneming met een incident omgaat en hoe herhaling in de toekomst wordt voorkomen. De AFM gebruikt incidentmeldingen om proactief op signalen uit de sector te reageren. De AFM kan op basis van incidentmeldingen inspringen op ontwikkelingen in de sector en bijdragen aan het adequate functioneren van zowel de markt als individuele ondernemingen.

Incidenten bij serviceproviders

In 2020 heeft de AFM een informatieverzoek naar beheerders en beleggingsondernemingen verstuurd over uitbesteding. In de beantwoording van deze uitvraag ziet de AFM dat er regelmatig incidenten bij serviceproviders plaatsvinden. De AFM heeft op dit moment geen onderzoek gedaan naar de individuele incidenten, maar de AFM wil graag benadrukken dat ook incidenten bij serviceproviders van ondernemingen onder de meldingsplicht voor incidenten kunnen vallen. Het is hierom van belang om duidelijke afspraken te maken met serviceproviders over het melden van incidenten door serviceproviders zodat de financiële onderneming haar meldingsplicht bij de AFM adequaat kan invullen.

Externe dreigingen in de risicoanalyse

Tijdens de gesprekken die de AFM in het kader van de inventarisatie voerde, is het de AFM opgevallen dat bij veel ondernemingen in het risicoanalyseproces aandacht is voor interne beheersing en voor reputatierisico's. In het bijzonder hebben ondernemingen daarbij veel aandacht voor fraude en datalekken.

Veel ondernemingen hebben aangegeven dat zij dreigingen die uitgaan van externe partijen vaak niet meenemen in hun overwegingen. Hierbij geven zij bijvoorbeeld aan dat zij te klein zijn voor cybercriminelen of dat ze denken dat cybercriminelen alleen geïnteresseerd zijn in grote banken of verzekeraars.

De AFM maakt zich echter grote zorgen over de toenemende dreiging van hackers en andere kwaadwillende actoren die het gemunt hebben op klantgegevens, activa en intellectueel eigendom. Hierom roept de AFM ondernemingen op om ook externe dreigingen mee te nemen in het risicoanalyseproces. De AFM gaat in haar toezicht meer aandacht besteden aan cyberrisico's.

Aankondiging *deep dive* onderzoek

De aandacht van de AFM voor incidenten heeft tot op heden niet geleid tot een significante toename van het aantal incidentmeldingen. De AFM verwacht met dit document eventuele onduidelijkheden over incidenten en de incidentmeldingsplicht weg te nemen. In aanvulling op de verschillende uitingen die de

AFM inmiddels over dit onderwerp heeft gedaan, zal op korte termijn onder een aantal ondernemingen een *deep dive* onderzoek worden uitgevoerd. Hierbij zal worden gekeken naar de wijze waarop ondernemingen beleid en maatregelen hebben geïmplementeerd ten aanzien van incidenten en de wijze waarop ondernemingen de incidentmeldingsplicht naleven. De te selecteren ondernemingen zullen hiervoor individueel benaderd worden.

Tot slot

Indien u nog vragen heeft over incidenten of de incidentmeldingsplicht, kunt u contact opnemen met het Ondernemersloket via ondernemersloket@afm.nl. Vermeld bij vragen altijd uw vergunningnummer. Vanwege de coronamaatregelen is ons Ondernemersloket momenteel uitsluitend per e-mail bereikbaar. U kunt wel een terugbelverzoek in uw e-mail opnemen. Geef in dat geval aan op welk telefoonnummer u bereikbaar bent.

Hoogachtend,
Autoriteit Financiële Markten