

Per post

Datum	23 december 2020
Ons kenmerk	
Pagina	1 van 4
Email	ondernemersloket@afm.nl
Betreft	Het registreren en melden van incidenten

Geacht bestuur,

Uw onderneming wordt geregeld geconfronteerd met risico's die impact op uw onderneming en uw cliënten kunnen hebben. Mogelijk leidt dit tot incidenten. In deze brief vragen wij uw aandacht voor het melden van incidenten die een ernstige bedreiging vormen voor de integere en beheerste bedrijfsvoering. Sinds de uitbraak van het coronavirus wordt er binnen ondernemingen meer op afstand met elkaar samengewerkt. Dat brengt specifieke risico's met zich mee¹. Daarom vragen wij in het bijzonder aandacht voor integriteits- en informatiebeveiligingsincidenten.

Integriteitsincidenten

De integriteit van de financiële ondernemingen is belangrijk voor het maatschappelijk vertrouwen in de financiële sector. Het publiek en marktdeelnemers moeten kunnen vertrouwen op de betrouwbaarheid van de beleidsbepalers en op een beheerste en integere bedrijfsuitoefening van financiële ondernemingen. Financiële ondernemingen moeten proactief tegengaan dat zij, hun beleidsbepalers of andere medewerkers betrokken raken bij wetsovertredingen en strafbare feiten, zoals bijvoorbeeld ongewenste belangenverstrengeling en fiscale fraude. Het risico op dergelijke incidenten kan echter niet volledig worden voorkomen. Daarom is het zaak om hier adequaat op te reageren teneinde de gematerialiseerde risico's te beheersen en om herhaling te voorkomen.

Informatiebeveiligingsincidenten

Door de toenemende afhankelijkheid van informatiesystemen ziet de AFM risico's rond informatiebeveiliging sterk toenemen. Een informatiebeveiligingsincident is een gebeurtenis die daadwerkelijk of mogelijk de vertrouwelijkheid, integriteit of beschikbaarheid van een informatiesysteem of de informatie die het systeem verwerkt, opslaat, of verzendt, in gevaar brengt².

¹ Zie ook de inventarisatie van thuiswerkrisico's van de AFM op <https://www.afm.nl/nl-nl/nieuws/2020/mei/risicos-informatiebeveiliging-coronacrisis>

² Zie ook de AFM principes voor informatiebeveiliging op <https://www.afm.nl/nl-nl/nieuws/2019/dec/principes-informatiebeveiliging>

Datum 23 december 2020
Ons kenmerk
Pagina 2 van 4

De wettelijke verplichting: wat verwachten wij van u?

Incidentmeldingen aan de AFM zijn verplicht. De AFM gebruikt deze in haar toezicht op individuele ondernemingen en om tijdig risico's in de sector te signaleren en op basis daarvan richting te geven aan haar risicogestuurd toezicht. Meldingen dragen daarmee bij aan eerlijke en transparante markten.

De wettelijke verplichting³ vereist dat:

- 1) uw onderneming beleid heeft voor de omgang met en vastlegging van incidenten;
- 2) uw onderneming maatregelen neemt als een incident zich voordoet, gericht op het beheersen van de opgetreden risico's en het voorkomen van herhaling;
- 3) uw onderneming een registratie van incidenten onderhoudt;
- 4) u incidenten die een ernstige bedreiging vormen voor de integere of beheerste bedrijfsvoering onverwijld aan de AFM meldt.

Gelet op het voorgaande, verwacht de AFM dat u incidenten die een ernstige bedreiging vormen voor de integere of beheerste bedrijfsvoering, onverwijld bij de AFM meldt. Dit onderwerp heeft momenteel verhoogde aandacht in het toezicht van de AFM. In de toekomst kan de AFM onderzoek doen naar de naleving van de verplichtingen die in deze brief zijn vermeld.

In de bijlage bij deze brief vindt u een niet-limitatieve lijst van voorbeelden van incidenten en het meldproces.

Meer informatie

Op de webpagina [https://www.afm.nl/nl-nl/professionals/onderwerpen/misstanden-wat vindt u meer informatie over incidenten en de incidentmeldingsplicht](https://www.afm.nl/nl-nl/professionals/onderwerpen/misstanden-wat-vindt-u-meer-informatie-over-incidenten-en-de-incidentmeldingsplicht). Als het antwoord op uw vraag hier niet tussen staat, kunt u contact opnemen met het Ondernemersloket. Het Ondernemersloket is door de ontwikkelingen rond het coronavirus momenteel alleen bereikbaar via e-mail: ondernemersloket@afm.nl. U kunt een terugbelverzoek sturen. Vermeld dan s.v.p. wel het telefoonnummer waarop u bereikbaar bent. Zodra het Ondernemersloket weer telefonisch bereikbaar is, vermelden wij dit op onze website.

Met vriendelijke groet,
Autoriteit Financiële Markten

³ Wettelijke grondslag per populatie

Voorbeelden van incidenten

Informatiebeveiliging

Voor informatiebeveiligingsincidenten geldt dat u deze moet melden wanneer het incident een ernstige bedreiging vormt voor de integere en beheerste bedrijfsvoering van uw onderneming. Een aantal voorbeelden van informatiebeveiligingsincidenten kunnen zijn:

- 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.

Integriteitsincidenten

Integriteitsincidenten moet u melden wanneer deze een ernstige bedreiging vormen voor de integere en beheerste bedrijfsvoering van uw onderneming. Hieronder staan een aantal voorbeelden uit de praktijk die bij de AFM worden gemeld:

- 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.

Meldproces

Incidentmeldingen kunt u aan de AFM doorgeven via het e-mailadres meldingenformulier@afm.nl. Maak hiervoor gebruik van Cryptshare⁴. Vermeld in uw melding altijd de volgende gegevens:

- Een omschrijving van het incident;
- De datum waarop het incident plaatsvond;
- De datum van ontdekken van het incident;
- Indien van toepassing: het aantal klanten van uw onderneming dat getroffen is door het incident.
- Indien van toepassing: de (geschatte) omvang van de schade.
- Wat uw onderneming doet/heeft gedaan om het incident te beheersen.

⁴ Voor meer informatie over Cryptshare: <https://www.afm.nl/nl-nl/over-afm/contact/bestanden>

Datum 23 december 2020
Ons kenmerk
Pagina 4 van 4

- Welke maatregelen uw onderneming treft om toekomstige gelijksoortige incidenten te voorkomen.

Als uw onderneming zelf onderzoek doet of laat doen naar het incident, moet uw onderneming het incident onverwijld aan de AFM melden, ook al is het onderzoek nog niet afgerond. Wel ontvangen wij graag achteraf de uitkomst van het onderzoek als aanvullende melding. Ook adviseren wij u bij twijfel altijd te melden.

Indien sprake is van een incident met significante prudentiële gevolgen voor uw onderneming, dient u daar eveneens melding van te maken bij DNB. In geval van een (potentieel) kapitaaltekort dient dit onverwijld te worden gemeld bij DNB.