Consultatie Principes voor Informatiebeveiliging

Verwachtingen van de AFM ten aanzien van informatiebeveiliging

Publicatiedatum: 14-mei-2019
Classificatie: AFM - Publiek

Autoriteit Financiële Markten

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

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

Inhoudsopgave

1. Inleiding

De Autoriteit Financiële Markten (AFM) consulteert de Principes voor informatiebeveiliging. Met deze beleidsuiting spreekt de AFM haar verwachting uit zodat financiële ondernemingen en accountantsorganisaties (hierna “ondernemingen”) hier zelf invulling aan kunnen geven.

De principes vormen geen nieuwe regels, maar bevatten algemene uitgangspunten over een breder onderwerp waar verschillende wettelijke normen onder liggen waarop de AFM toezicht houdt. Principes schrijven daarom niet voor hóe ondernemingen aan een bepaalde norm kunnen voldoen, maar schetsen verwachtingen die de AFM heeft bij de uitgangspunten voor het betreffende onderwerp en de uitkomsten van de toepassing hiervan. De toepassing en uitwerking van principes kan per onderneming verschillen, afhankelijk van de omvang en het type dienstverlener, het type dienstverlening en het soort product dat aangeboden wordt. Een verdere toelichting op het gebruik van principes is opgenomen in bijlage 1.

De AFM gaat de komende jaren met ondernemingen, zowel individueel als sectorbreed, het gesprek aan over de invulling van de principes. Naar aanleiding van deze gesprekken publiceert de AFM waar nodig ’good practices’ of nadere uitleg. De consultatie van de Principes voor informatiebeveiliging vormt het startpunt voor deze dialoog.

1.1 Voor wie zijn de Principes voor informatiebeveiliging?

Deze principes zijn bedoeld voor (beheerders van) alternatieve beleggingsinstellingen, (beheerders van) instellingen voor collectieve belegging en effecten, beleggingsondernemingen, bewaarders, financiëledienstverleners (voor zover het geen bank, verzekeraar of financiële instelling betreft), pensioenbewaarders, verleners van datarapporteringsdiensten, gereglementeerde markten en accountantsorganisaties. De AFM nodigt de hierboven genoemde ondernemingen en andere geïnteresseerden uit om voor 25 juni 2019 te reageren op de consultatie. Dit kan door het invullen van het consultatie formulier en deze per mail te sturen naar consultatieprincipes@afm.nl.

Daarbij stellen wij u de volgende vragen:

1. **Op welke punten kunt u zich vinden in de beleidsuiting Principes voor informatiebeveiliging?**
2. **Op welke punten kunt u zich niet vinden in de beleidsuiting; voorziet u problemen en waarom?**
3. **Wat is uw voorstel om verbeteringen aan te brengen?**

Na sluiting van de consultatieperiode verwerkt de AFM de reacties in een definitieve versie van de Principes voor informatiebeveiliging. Deze publiceert de AFM, samen met een feedback statement op haar website.

2. Het belang van informatiebeveiliging

De beheersing van informatiebeveiligingsrisico's wordt steeds belangrijker. Door de steeds verdere digitalisering van financiële ondernemingen en accountantsorganisaties (zie bijlage 1), maar ook door toenemende cyberdreiging.

Informatiebeveiliging is belangrijk voor de onderneming én voor haar klant. De klant moet namelijk kunnen vertrouwen op beschikbare dienstverlening en dat er integer en vertrouwelijk haar gegevens wordt omgegaan. De AFM verwacht daarom dat ondernemingen zorgvuldig omgaan met informatiebeveiligingsrisico's.

De AFM helpt ondernemingen daarbij door met twaalf principes[1] haar verwachtingen over informatiebeveiliging te duiden. De uitvoering zal per onderneming verschillen, als gevolg van de aard van de dienstverlening en de omvang van de onderneming.

Bij haar toezicht op informatiebeveiliging sluit de AFM inhoudelijk zo veel mogelijk aan bij de toetsingskaders van De Nederlandsche Bank (DNB).

[1] De principes zijn opgesteld volgens internationaal geaccepteerde ICT-risk-managementraamwerken, zoals COBIT (COBIT 5, gepubliceerd door ISACA), National Institute of Standards and Technology Cybersecurity Framework (NIST) en richtlijnen van CPMI-IOSCO (Guidance on cyber resilience for financial market infrastructures) en het reeds bestaande toezicht op informatiebeveiliging door Nederlandse financiële ondernemingen.

3. De Principes voor informatiebeveiliging

De AFM heeft twaalf Principes voor informatiebeveiliging gedefinieerd. Elk principe is gericht op het realiseren van het hoofddoel:

Ondernemingen hebben maatregelen getroffen om de vertrouwelijkheid en integriteit van informatie en de beschikbaarheid van informatie, data en systemen te garanderen.

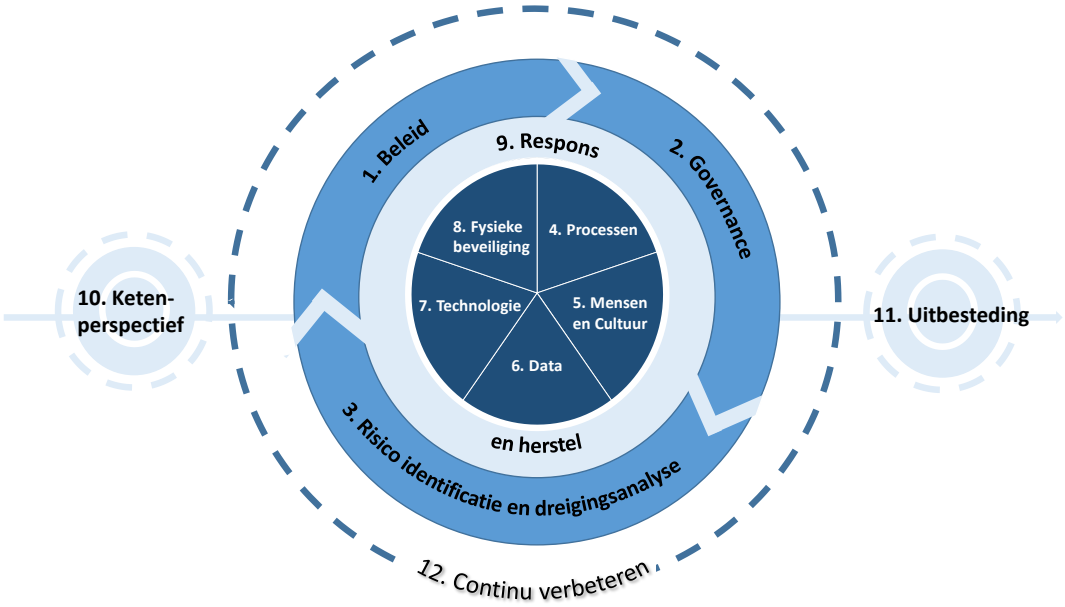
Tussen de afzonderlijke principes bestaat samenhang en een wisselwerking om dat doel te bereiken. Elk principe beslaat een onderdeel van informatiebeveiliging. Die onderdelen zijn:

1. Beleid
2. Governance
3. Risico-identificatie en dreigingsanalyse
4. Processen
5. Mensen en cultuur
6. Data
7. Technologie
8. Fysieke beveiliging
9. Respons en herstel
10. Ketenperspectief
11. Uitbesteding
12. Continu verbeteren

Daarbij onderscheidt de AFM vijf gebieden die het spectrum van informatiebeveiliging opmaken:

a) De basis (principes 1 tot en met 3)
b) De maatregelen (principes 4 tot en met 8)
c) Respons en herstel (principe 9)
d) Impact externe partijen op informatiebeveiliging van de onderneming (principes 10 en 11)
e) De dynamiek van informatiebeveiliging (principe 12)

In een grafische weergave ziet dat er zo uit:



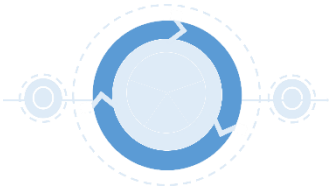
De basis van informatiebeveiliging wordt gevormd door beleid, governance en risico-identificatie en een dreigingsanalyse. Het dreigingsbeeld is bovendien niet statisch. Daarom is het belangrijk om ervoor te zorgen dat een onderneming haar informatiebeveiliging voortdurend actualiseert en verbetert.

Met een goed informatiebeveiligingsbeleid, zorgvuldige governance en het voortdurend identificeren en analyseren van risico's en dreigingen kunnen de juiste maatregelen worden getroffen op het gebied van: mensen en cultuur, processen, techniek, data en fysieke beveiliging.

Informatiebeveiligingsincidenten kunnen alsnog plaatsvinden. Daarom moeten ondernemingen respons- en herstelmaatregelen kunnen uitvoeren om de impact hiervan te beperken.

De informatiesystemen van ondernemingen zijn verweven met andere, externe partijen. Daarom zijn niet alleen risico's en maatregelen van de eigen onderneming relevant voor de onderneming, maar ook die van betrokken externe partijen.

4. De basis



De eerste drie principes betreffen de basis voor informatiebeveiliging. Op basis van een informatiebeveiligingsbeleid belegt een onderneming de verantwoordelijkheden op het gebied van informatiebeveiliging. Zo adresseert zij risico's en dreigingen.

4.1 Principe 1 – Beleid

Een actueel informatiebeveiligingsbeleid beschrijft de gelaagde[2] wijze waarop informatiebeveiligings-risico's worden beheerst.

In het beleid stelt de onderneming haar doelstellingen voor informatiebeveiliging vast en de wijze waarop zij deze doelstellingen behaalt. De onderneming maakt bij het opstellen van het informatiebeveiligingsbeleid gebruik van internationaal geaccepteerde raamwerken voor informatiebeveiliging en cyber security[3].

Het beleid beschrijft de uitgangspunten en risicobereidheid[4], de ICT-standaarden die door de onderneming worden gehanteerd, verantwoordelijkheden, procedures en processen om informatiebeveiliging in te bedden in de onderneming.

Het informatiebeveiligingsbeleid is in elk geval van toepassing op de ICT assets[5] en processen in eigen beheer en persoonlijke gegevensdragers van medewerkers en de uitbestede ICT-assets en processen.

In het beleid staat hoe de onderneming een classificatiesysteem toepast om de eisen op het gebied van integriteit, vertrouwelijkheid en beschikbaarheid van ICT-assets, inclusief fysieke locaties en data te bepalen. De specifieke maatregelen die volgen uit het informatiebeveiligingsbeleid, zijn in lijn met deze risicoclassificatie van systemen, data en fysieke locaties.

Het informatiebeveiligingsbeleid blijft actueel doordat risico's en dreigingen periodiek worden geëvalueerd. Extra evaluatie vindt plaats als er nieuwe risico's ontstaan of de grootte van risico's of dreigingen significant toeneemt.

Organisaties die onderdeel zijn van een internationale groep, zorgen ervoor dat zij het informatiebeveiligingsbeleid consistent in de organisatie en haar internationale onderdelen wordt geïmplementeerd.

---

[2] Deze gelaagdheid ontstaat doordat een combinatie van technische en procedurele maatregelen en fysieke beveiliging wordt toegepast om informatiebeveiliging te bereiken.
[3] Zoals bijvoorbeeld ISO27001 en ISO27002, COBIT, CPMI-IOSCO en NIST.
[4] Risicobereidheid expliciteert in welke mate de onderneming bereid is specifieke informatiebeveiligingsrisico's te lopen.
[5] Alle aangekochte of zelf ontwikkelde ICT-componenten van de onderneming. Dit betreft zowel hardware als software.

4.2 Principe 2 – Governance

De onderneming heeft een governance structuur ingericht die effectieve informatiebeveiliging mogelijk maakt.

De leiding van een onderneming is verantwoordelijk voor informatiebeveiliging. De belangrijkste informatiebeveiligingsrisico's, dreigingen en incidenten zijn bij de leiding van de onderneming bekend.

Daar waar onderdelen van de onderneming niet voldoen aan het informatiebeveiligingsbeleid, worden maatregelen getroffen óf wordt dit expliciet geaccepteerd door de leiding van de onderneming.

De invulling van de organisatiestructuur voor informatiebeveiliging is afgestemd op het bedrijfsmodel, de omvang en complexiteit van de onderneming, de kenmerken van de informatie en data die door de onderneming worden gecreëerd of verwerkt en de bijbehorende informatiebeveiligingsrisico's.

Een heldere taakverdeling en beschikbaarheid van voldoende deskundigheid en ervaring zijn cruciaal voor de kwaliteit van risicoanalyses en de effectiviteit van de informatiebeveiligingsmaatregelen. De rollen en verantwoordelijkheden op het gebied van het inrichten, beheren en controleren van informatiebeveiliging zijn daarom helder belegd. De onderneming heeft voldoende capaciteit, kennis en ervaring tot haar beschikking op het gebied van informatiebeveiliging om invulling aan deze rollen en verantwoordelijkheden te geven.

4.3 Principe 3 – Risico-identificatie en dreigingsanalyse

Informatiebeveiliging is ingericht op basis van een actueel inzicht in de interne en externe risico's en dreigingen, de potentiële impact van bestaande dreigingen en de risicobereidheid van de onderneming.

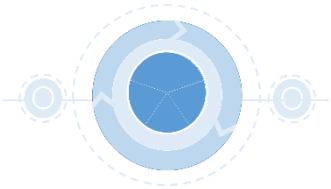
De risico- en dreigingsanalyse vindt periodiek plaats. De frequentie is afgestemd op het bedrijfsmodel, de omvang en complexiteit van de onderneming en de kenmerken van de informatie en data die door de onderneming wordt gecreëerd of verwerkt. De risicoanalyse wordt periodiek geactualiseerd of als er nieuwe informatiebeveiligingsdreigingen en kwetsbaarheden zijn geïdentificeerd.

De onderneming weegt in haar risico- en dreigingsanalyses de belangen mee van de eigen onderneming en de belangen van haar stakeholders, zoals haar klanten en van de sector waarin zij werkzaam is.

Op basis van inzicht in bestaande en voorzienbare inherente risico's en dreigingen beoordeelt de onderneming de mate waarin haar informatiebeveiligingsmaatregelen toereikend zijn en treft de

benodigde additionele maatregelen. De onderneming hanteert hiertoe wettelijke vereisten en haar doelstellingen op het gebied van continuïteit, vertrouwelijkheid en integriteit van systemen en data.

5. De maatregelen



Door de onderneming worden verschillende maatregelen genomen om het informatiebeveiligingsbeleid na te leven. Deze maatregelen betreffen in elk geval de procesinrichting, maatregelen op het gebied van mensen en cultuur, data, technologie en fysieke beveiliging.

5.1 Principe 4 – Processen

De inrichting van bedrijfsprocessen waarborgt de vertrouwelijkheid en integriteit van informatie en de beschikbaarheid van data en systemen.

Informatiebeveiliging is een integraal onderdeel van de administratieve organisatie en interne controle. Alle processen van de onderneming zijn zodanig ingericht dat deze waarborgen bevatten om continuïteit, integriteit en vertrouwelijkheid van systemen en data te garanderen in lijn met de risicobereidheid van de organisatie. De effectiviteit van deze maatregelen wordt periodiek getest, ook in combinatie met de overige informatiebeveiligingsmaatregelen die door de onderneming zijn getroffen.

Voor de inrichting van ICT ontwikkel- en beheerprocessen maakt de onderneming gebruik van algemeen erkende informatiebeveiliging- en cyberraamwerken[6]. De onderneming implementeert beheerprocessen om informatiebeveiligingsrisico's te identificeren en om dreigingen en incidenten te detecteren als deze zich voordoen. Ondernemingen worden aangemoedigd hierbij gebruik te maken van "Coordinated Vulnerability Disclosure"[7] om meldingen te ontvangen van door derden geïdentificeerde zwakke plekken in ICT-systemen van de onderneming.

5.2 Principe 5 – Mensen en Cultuur

De onderneming onderkent het risico van menselijk handelen voor informatiebeveiliging en creëert een cultuur waarin medewerkers zich bewust zijn van het risico op informatiebeveiligingsincidenten en hierover open communiceren.

Mensen zijn een zwakke schakel in informatiebeveiliging. Onverantwoord gedrag of onbewust gedrag van mensen kan leiden tot informatiebeveiligingsincidenten. Dit wordt door de onderneming erkend en gemitigeerd door middel van doeltreffende maatregelen. De onderneming richt processen in zodat mensen effectief bijdragen aan adequate informatiebeveiliging en om meldingen over incidenten door medewerkers adequaat te behandelen. In aanvulling hierop wordt bijvoorbeeld gebruik gemaakt van bewustwordingsprogramma's en trainingen. De effectiviteit van deze

[6] Zoals bijvoorbeeld ISO27001 en ISO27002, CPMI-IOSCO, COBIT en NIST.
[7] Zoals bijvoorbeeld opgenomen in 'Coordinated Vulnerability Disclosure: de leidraad' van het Nationaal Cyber Security Center (NCSC) en ISO-standaarden over dit proces, ISO 29147 en ISO 30111. Dit is een leidraad voor het op een verantwoordelijke wijze melden en afhandelen van kwetsbaarheden in informatiesystemen en (software)producten.

maatregelen wordt periodiek getest, ook in combinatie met de overige informatiebeveiligingsmaatregelen die door de onderneming zijn getroffen.

De onderneming erkent het risico van menselijk handelen op de effectiviteit van het informatiebeveiligingsbeleid en treft adequate maatregelen om dit risico te beperken. Hierin worden zowel de risico's als gevolg van interne factoren (bijvoorbeeld interne fraude) als risico's als gevolg van externe factoren (bijvoorbeeld phishing via e-mail) meegenomen. Om deze risico's te beperken, kunnen ondernemingen technische, procedurele en fysieke maatregelen treffen. Deze maatregelen ondersteunen medewerkers om hun verantwoordelijkheden op het gebied van informatiebeveiliging te vervullen. Eventuele restrisico's worden expliciet afgewogen tegen de (positieve en negatieve) effecten van additionele technische maatregelen om deze risico's te beperken.

Senior management draagt het belang van informatiebeveiliging uit en zij maakt medewerkers bewust van de bestaande dreigingen. Alle medewerkers worden op verschillende manieren actief bewust gemaakt en opgeleid om hun verantwoordelijkheid op het gebied van informatiebeveiliging te nemen.

5.3 Principe 6 – Data

Tijdens de volledige levenscyclus van data zijn maatregelen getroffen om te voldoen aan de beveiligingseisen voor data en informatie.

Informatiebeveiligingsmaatregelen zijn gedefinieerd om de benodigde integriteit, vertrouwelijkheid en beschikbaarheid van informatie, data en systemen te garanderen. Deze zijn vertaald in maatregelen om hieraan te kunnen voldoen gedurende de volledige levenscyclus van data. Deze maatregelen hebben betrekking op zowel de opslag, het gebruik als het transport van data via communicatiekanalen. De effectiviteit van deze maatregelen wordt periodiek getest, ook in combinatie met de overige informatiebeveiligingsmaatregelen die door de onderneming zijn getroffen. Bij de ontwikkeling van systemen worden beveiligingseisen voor data meegenomen.

De verantwoordelijkheid voor databronnen en het bewerken van die bronnen is belegd binnen de organisatie. Dit betreft de adequate informatiebeveiliging van actuele en historische data. Wettelijke eisen en intern beleid rondom de beschikbaarheid en integriteit van data worden door de onderneming in acht genomen. Dit geldt ook voor systeemtransformaties en datamigraties zodat historische data en de samenhang tussen data elementen beschikbaar blijven conform de eisen die voortvloeien uit het informatiebeveiligingsbeleid.

5.4 Principe 7 – Technologie

Bij de implementatie en het onderhoud van systemen wordt het uitgangspunt 'secure by design' toegepast waardoor informatiebeveiligingsmaatregelen onderdeel zijn van het ontwerp van systemen.

De onderneming wordt aangemoedigd om internationale technologiestandaarden te gebruiken om informatiebeveiliging in te bedden in het ontwerp van de ICT-architectuur en systemen.

Informatiebeveiligingsrisico's worden als realistische scenario's beschouwd, waar vanaf de ontwerpfase rekening mee gehouden wordt. De ICT-architectuur en systemen zijn ontworpen en ingericht om veilig te zijn.

De onderneming kent de risico's van het gebruik van nieuwe en verouderde technologie en heeft maatregelen getroffen om deze risico's te beperken. Wijzigingen in de onderneming en de ICT-infrastructuur worden op een dusdanige wijze doorgevoerd dat het risico op informatiebeveiligingsincidenten niet stijgt en waar mogelijk wordt verkleind.

Bij de implementatie en tijdens het onderhoud van systemen wordt de wendbaarheid van de ICT-infrastructuur meegewogen om te voorkomen dat er afhankelijkheden ontstaan van niet meer vervangbare systemen.

Het ICT-netwerk is opgedeeld in segmenten die in lijn zijn met de beveiligingsclassificatie van de informatie en data die in een specifiek segment beschikbaar zijn. Technologiestandaarden zijn in alle ICT-componenten van alle segmenten doorgevoerd. Afwijkingen worden expliciet goedgekeurd op basis van een analyse van de risico's die ontstaan als gevolg van deze afwijking.

De effectiviteit van technische maatregelen wordt periodiek getest, ook in combinatie met de informatiebeveiligingsmaatregelen die door de onderneming zijn getroffen.

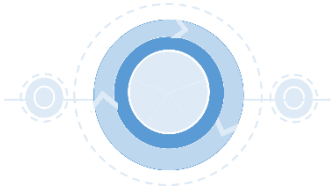
5.5 Principe 8 – Fysieke beveiliging

Het ontwerp en de inrichting van de faciliteiten en apparatuur van de onderneming is in lijn met de eisen aan informatiebeveiliging.

De onderneming heeft fysieke maatregelen getroffen in aanvulling op technische en procedurele maatregelen, bijvoorbeeld om de toegang tot faciliteiten en apparatuur te beperken. Fysieke maatregelen ter bescherming van faciliteiten en apparatuur zijn getroffen op basis van een analyse van de risico's van externe factoren (zoals de kans op natuurrampen), menselijke factoren (zoals ongeautoriseerde toegang) en crisissituaties (als gevolg van bijvoorbeeld de uitval van elektriciteit).

De informatiebeveiligingsrisico's van faciliteiten en apparatuur zijn gemitigeerd conform het informatiebeveiligingsbeleid. De effectiviteit van deze maatregelen wordt periodiek getest in lijn met het inherente risico van de faciliteit en/of de apparatuur en in combinatie met de informatiebeveiligingsmaatregelen die door de onderneming zijn getroffen.

6. Respons en herstel



De maatregelen die voortvloeien uit de toepassing van deze principes zijn gericht zijn op het verkleinen van de kans op een informatiebeveiligingsincident. Toch kunnen incidenten plaatsvinden, bijvoorbeeld door ineffectiviteit van maatregelen of door (nog) niet gedetecteerde dreigingen. Ondernemingen richten voor deze situaties respons- en herstelmechanismen in om de impact hiervan te beperken.

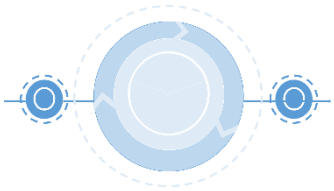
6.1 Principe 9 – Respons en herstel

De onderneming is voorbereid op informatiebeveiligingsincidenten om de impact hiervan te beperken. Wanneer zich een informatiebeveiligingsincident voordoet, treft de onderneming tijdig en doeltreffend respons- en herstelmaatregelen.

De onderneming beschikt over processen en plannen die worden geactiveerd op het moment dat een informatiebeveiligingsincident wordt gedetecteerd. Deze processen en plannen bevatten in elk geval maatregelen om (1) het incident te stoppen, (2) de negatieve impact te beperken, (3) de schade te herstellen en (4) hier goed over te communiceren.

Er vindt evaluatie plaats tijdens en na de herstelactiviteiten. De opgedane inzichten worden verwerkt in het informatiebeveiligingsbeleid, bestaande processen en systemen en de communicatie naar en opleiding van medewerkers.

7. De impact van externe partijen op de informatiebeveiliging van de onderneming



Een onderneming is verbonden met externe partijen, bijvoorbeeld via de communicatiekanalen die zij klanten aanbiedt of doordat zij een deel van haar activiteiten heeft uitbesteed aan leveranciers. Daardoor bestaan mogelijk afhankelijkheden voor de informatiebeveiliging van de onderneming.

7.1 Principe 10 – Ketenperspectief

De onderneming past een integrale ketenbenadering[8] toe waarbij de eigen plaats in de keten en de afhankelijkheden van andere ketenpartijen in acht wordt genomen bij het bepalen van informatiebeveiligingsrisico's en de benodigde beheersmaatregelen.

De onderneming hanteert als uitgangspunt dat ondernemingen in dezelfde sector en binnen een keten coalitiegenoten zijn in het beschermen van de sector tegen externe cyberrisico's. Zwakheden van een ketenpartij hebben mogelijk gevolgen voor andere partijen in dezelfde keten. Om deze risico's in kaart te brengen, participeert de onderneming indien mogelijk en relevant in informatiebeveiliging- en cybertesten die door autoriteiten voor sectoren of ketens worden georganiseerd.

De onderneming bepaalt de toegevoegde waarde van informatieuitwisseling tussen de verschillende partijen in de keten en tussen de onderneming en haar klanten en relevante autoriteiten. Deze informatie-uitwisseling heeft tot doel om een goed beeld te krijgen van dreigingen binnen de keten en heeft betrekking op informatiebeveiliging en bestaande dreigingen en incidenten.

Op basis van inzicht in ketenafhankelijkheden, streeft de onderneming ernaar afspraken te maken over informatiebeveiliging met andere partijen in de keten. Dit betreft onder meer afspraken om de impact van grootschalige incidenten te beperken voor de getroffen onderneming en de keten als geheel. Indien deze afspraken niet bestaan, gaat de onderneming ervan uit dat er geen maatregelen zijn getroffen op het gebied van informatiebeveiliging door ketenpartners en neemt zij maatregelen om dit risico te beperken.

7.2 Principe 11 – Uitbesteding

De onderneming is verantwoordelijk voor de informatiebeveiliging van uitbestede processen of systemen.

De onderneming die processen of ICT systemen uitbesteedt aan een interne partij (binnen de groep waar de onderneming deel van uitmaakt) of aan een externe partij, is zelf verantwoordelijk voor de informatiebeveiliging van deze activiteiten en systemen. Voordat ICT infrastructuur en/of processen

[8] De integrale ketenbenadering is het beheersen van meer dan alleen de risico's die ontstaan in de eigen ICT-omgeving. De keten bestaat uit verschillende schakels van interne en externe partijen, waaronder de klant en toezichthouders.

uitbesteed wordt, voert de onderneming een gedegen onderzoek naar de informatiebeveiliging van de toeleverancier uit. Hierbij worden zowel de informatiebeveiligingsrisico's van uitbesteding, als de kans om informatiebeveiliging te professionaliseren meegenomen.

De onderneming is zich bewust van de gevolgen van uitbesteding voor de rollen en verantwoordelijkheden, risicomanagement en ketenintegratie. De analyse van deze risicofactoren wordt door de onderneming regelmatig geactualiseerd. De onderneming bepaalt de impact van uitbesteding op de beschikbaarheid, vertrouwelijkheid en integriteit van data en systemen en neemt passende beheersmaatregelen.

Van de onderneming wordt verwacht dat zij contractueel heldere afspraken maakt over de samenwerking en de doelstellingen wat betreft informatiebeveiliging. Ook kunnen aanvullende beheersmaatregelen in het contract worden opgenomen, zoals de bevoegdheid om audits uit te voeren bij een leverancier. Hierbij worden niet alleen voor het begin van de samenwerking afspraken gemaakt, maar is het van belang dat partijen vooruitkijken en de gehele uitbestedingscyclus overzien, ongeacht of het een kort of langdurig samenwerkingsverband betreft.

8. De dynamiek van informatiebeveiliging

Informatiebeveiliging is dynamisch. Technologie en (externe) bedreigingsfactoren ontwikkelen zich continu. Daarmee ontstaan nieuwe risico's. De onderneming is daarom genoodzaakt haar informatiebeveiliging continu te verbeteren.

8.1 Principe 12 – Continu verbeteren

De onderneming verbetert voortdurend haar informatiebeveiliging op basis van actuele inzichten in bestaande dreigingen en ontwikkelingen op het gebied van informatiebeveiliging.

Wijzingen in de interne en externe omgeving van de onderneming worden geïdentificeerd en de mogelijke impact van deze wijzigingen op de informatiebeveiliging van de onderneming wordt geëvalueerd. De onderneming neemt actie om te zorgen dat deze wijzigingen geen negatieve impact hebben op haar informatiebeveiliging.

Bijlage 1 – Reikwijdte Principes voor informatiebeveiliging

De reikwijdte van de Principes voor informatiebeveiliging betreft op het moment van publicatie:

- Alternatieve beleggingsinstellingen (ABI)
- Beheerder van een ABI
- Instellingen voor collectieve belegging en effecten (ICBE)
- Beheerder van een ICBE
- Beleggingsonderneming
- Bewaarder
- Financiële dienstverlener (zover het geen bank, verzekeraar of financiële instelling betreft)
- Pensioenbewaarder
- Verlener van datarapporteringsdiensten
- Gereglementeerde markt
- Accountantsorganisatie

Bijlage 2 – Principes: nieuwe beleidsuiting van de AFM

De AFM-'Principes' zijn een aanvulling op bestaande beleidsuitingen, namelijk de beleidsregel, de interpretatie en de leidraad. Hieronder staat beschreven wat onder principes wordt verstaan, waarom de AFM principes introduceert, hoe de principes onderdeel vormen van het toezicht en wat toezicht met principes betekent voor de ondernemingen waar de AFM toezicht op houdt.

Wat zijn principes?

Met principes spreekt de AFM haar verwachting uit over een bepaald onderwerp zodat ondernemingen hier zelf invulling aan kunnen geven. Dit kunnen nieuwe onderwerpen zijn of onderwerpen waarover onduidelijkheden bestaan in de sector. Principes zijn geen nieuwe regels, maar een uitwerking van de 'geest van de wet', op basis van het wettelijk kader waarop de AFM toezicht houdt. De principes zijn van toepassing ongeacht het type (financiële) onderneming. Vaak zal de AFM principes formuleren op een relatief hoog abstractieniveau. Sommige onderwerpen zijn al zodanig uitgekristalliseerd dat principes concreter worden geformuleerd.

Waarom principes?

Om op een breder onderwerp heldere verwachtingen te scheppen en de voorspelbaarheid van toezicht te vergroten, neemt de AFM het initiatief tot het opstellen van principes. Hiermee beoogt de AFM te komen tot een gezamenlijk beeld over wat consumenten en andere eindgebruikers in de financiële en audit sector van ondernemingen op deze onderwerpen mogen verwachten. Aan de principes die de AFM formuleert, liggen verschillende wettelijke normen ten grondslag. Vaak zijn dat open normen die de AFM vanuit haar rol als toezichthouder interpreteert, gegeven een bepaalde context. De AFM houdt bijvoorbeeld toezicht op naleving van de regels omtrent zorgplicht, advies, integere en beheerste bedrijfsvoering en productontwikkeling.

Benutten denkkracht van ondernemingen

De AFM geeft door middel van principes richting ten aanzien van een bepaald onderwerp zonder voorschrijvend te zijn. Principes geven niet aan hóe ondernemingen aan een bepaalde norm moeten voldoen, maar schetsen verwachtingen die de AFM heeft bij de uitkomsten. Ondernemingen bepalen zelf hoe ze de principes voor hun eigen situatie zo goed mogelijk invullen. Zo blijft ruimte bestaan voor ondernemingen om zelf oplossingsrichtingen te bedenken die recht doen aan de specifieke context van de onderneming. Door ondernemingen zelf invulling te laten geven aan principes hoopt de AFM de denkkracht van ondernemingen te kunnen benutten en daarmee het toezicht efficiënter te maken.

Ruimte voor maatwerk

De principes bieden de mogelijkheid voor maatwerk zodat recht wordt gedaan aan de grote diversiteit aan ondernemingen die onder het toezicht van de AFM vallen en geven hen daarbij een actievere rol. Ondernemingen zijn zelf verantwoordelijk voor de toepassing van de principes op hun

producten, diensten, beleid en bedrijfsvoering. De wijze waarop ondernemingen invulling geven aan de principes kan verschillen, afhankelijk van de omvang van en het type dienstverlening, en het soort product dat aangeboden wordt.

Wat is het verschil met een leidraad?

Met principes geeft de AFM meer algemene verwachtingen mee aan ondernemingen ten aanzien van een breder onderwerp waar verschillende wettelijke normen aan ten grondslag liggen. Principes hebben overeenkomsten met leidraden, beide geven namelijk richting aan de sector. Bij een leidraad schetst de AFM concrete verwachtingen ten aanzien van één specifieke wettelijke norm.

Wat verwacht de AFM van ondernemingen?

De AFM gaat er vanuit dat ondernemingen kennis nemen van de principes en aan de slag gaan met de verwachtingen die gereflecteerd worden in de principes. Ondernemingen bepalen zelf hoe zij de principes vertalen naar hun producten, diensten, informatieverstrekking, beleid en bedrijfsvoering. Hiermee geven ze invulling aan de principes op een manier die past bij hun organisatie. De AFM kijkt naar de onderbouwing van de keuzes die ondernemingen maken en treedt hierover in dialoog.

Wat mogen ondernemingen van de AFM verwachten?

De AFM selecteert onderwerpen waarvoor het gebruik van principes zinvol is en stelt voor nieuwe toezichtgebieden principes op in consultatie met de sector. Hiermee neemt de AFM het initiatief voor een verdere ontwikkeling van de sector op deze onderwerpen.

Toezicht met principes

De AFM zal in de komende jaren met ondernemingen, zowel individueel als sectorbreed, het gesprek aangaan over invulling van de principes. Naar aanleiding van deze gesprekken zal de AFM waar nodig en passend ’good practices’ of nadere uitleg publiceren.

Ondernemingen mogen erop vertrouwen dat de AFM handelt overeenkomstig haar gepubliceerde principes. Principes zijn op zichzelf niet handhaafbaar. Indien nodig zal de AFM teruggrijpen op de onderliggende wettelijke kaders om te kunnen handhaven.

Autoriteit Financiële Markten
T 020 797 2000 | F 020 797 3800
Postbus 11723 | 1001 GS Amsterdam
www.afm.nl