EIOPA-BoS-20/600

Richtsnoeren betreffende beveiliging en governance van informatie- en communicatietechnologie

Eiopa – Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurt – Germany - Tel.: + 49 69-951119-20;
Fax: + 49 69-951119-19; e-mail: info@eiopa.europa.eu site: www.eiopa.europa.eu

Inhoudsopgave

Achtergrond **3**
Inleiding **6**
Definities 6
Richtsnoer 1 – Evenredigheid 9
Richtsnoer 2 – ICT binnen het governancesysteem 9
Richtsnoer 3 – ICT-strategie 9
Richtsnoer 4 – ICT- en beveiligingsrisico's binnen het risicobeheerssysteem 9
Richtsnoer 5 – Audit 11
Richtsnoer 6 – Beleidslijnen en maatregelen op het gebied van informatiebeveiliging 11
Richtsnoer 7 – Informatiebeveiligingsfunctie 11
Richtsnoer 8 – Logische beveiliging 12
Richtsnoer 9 – Fysieke beveiliging 13
Richtsnoer 10 – Beveiliging van ICT-operaties 13
Richtsnoer 11 – Beveiligingsmonitoring 14
Richtsnoer 12 – Evaluaties, beoordeling en testen van informatiebeveiliging 14
Richtsnoer 13 – Opleiding en bewustmaking op het gebied van informatiebeveiliging 15
Richtsnoer 14 – Beheer van ICT-operaties 15
Richtsnoer 15 – Beheer van ICT-incidenten en -problemen 16
Richtsnoer 16 – ICT-projectbeheer 17
Richtsnoer 17 – Verwerving en ontwikkeling van ICT-systemen 17
Richtsnoer 18 - ICT-wijzigingenbeheer 18
Richtsnoer 19 – Beheer van de bedrijfscontinuïteit 18
Richtsnoer 20 – Bedrijfseffectbeoordeling 19
Richtsnoer 21 – Planning van de bedrijfscontinuïteit 19
Richtsnoer 22 – Interventie- en herstelplannen 19
Richtsnoer 23 – Testen van plannen 20
Richtsnoer 24 – Crisiscommunicatie 20
Richtsnoer 25 – Uitbesteding van ICT-diensten en ICT-systemen 21
Regels inzake naleving en rapportage **22**
Slotbepaling inzake herziening **22**

Achtergrond

1. Krachtens artikel 16 van Verordening (EU) nr. 1094/2010 kan Eiopa met het oog op het invoeren van consistente, efficiënte en effectieve toezichtpraktijken en het verzekeren van de gemeenschappelijke, uniforme en consistente toepassing van het Unierecht richtsnoeren en aanbevelingen tot bevoegde autoriteiten of financiële instellingen richten.

2. Overeenkomstig artikel 16, lid 3, van die verordening moeten de bevoegde autoriteiten en financiële instellingen zich tot het uiterste inspannen om aan deze richtsnoeren en aanbevelingen te voldoen.

3. In het kader van de analyse die is uitgevoerd naar aanleiding van het FinTech-actieplan van de Commissie (COM(2018)0109 final) en het plan van Eiopa voor de convergentie van toezicht 2018-2019[1], en na overleg met verschillende andere belanghebbenden[2] heeft Eiopa geconstateerd dat er behoefte bestond aan de ontwikkeling van specifieke richtsnoeren over de beveiliging en governance van informatie- en communicatietechnologie (ICT) in het licht van de artikelen 41 en 44 van Richtlijn 2009/138/EG.

4. Zoals vermeld in het gezamenlijk advies van de Europese toezichthoudende autoriteiten aan de Europese Commissie is in de Eiopa-richtsnoeren voor het governancesysteem onvoldoende rekening gehouden met het belang om het ICT-risico's (met inbegrip van cyberveiligheidsrisico's) aan te pakken. Tevens ontbraken volgens dat advies richtsnoeren inzake cruciale elementen die algemeen geacht worden deel uit te maken van een passende ICT-beveiliging en -governance.

5. Uit een analyse van de huidige (wetgevings)situatie in de EU die met het oog op het voormelde gezamenlijke advies is gemaakt, bleek dat het merendeel van de EU-lidstaten nationale regels heeft opgesteld voor ICT-beveiliging en -governance. Hoewel de eisen vergelijkbaar zijn, is het regelgevingskader toch versnipperd. Daarnaast heeft een onderzoek naar de huidige toezichtpraktijken een grote verscheidenheid aan praktijken laten zien, variërend van "geen specifiek toezicht" tot "sterk toezicht" (inclusief "inspecties op afstand" en "inspecties ter plaatse").

6. Bovendien wordt ICT steeds complexer en neemt ook het aantal ICT-gerelateerde incidenten (waaronder cyberincidenten) toe, evenals de negatieve gevolgen van dergelijke incidenten voor de bedrijfsactiviteiten van ondernemingen. Daarom is ICT- en beveiligingsrisicobeheer van fundamenteel belang voor een onderneming om haar strategische, zakelijke, operationele en reputatiedoelstellingen te behalen.

7. Daarnaast is er in het gehele verzekeringswezen, zowel bij traditionele als innovatieve bedrijfsmodellen, sprake van een toenemende afhankelijkheid van ICT bij de verlening van verzekeringsdiensten en bij de normale bedrijfsactiviteiten van ondernemingen, vanwege onder meer de digitalisering van het verzekeringswezen (InsurTech, IoT, enz.) en de interconnectiviteit via telecommunicatiekanalen (internet, mobiele en draadloze verbindingen en wide-areanetwerken). Dit zorgt ervoor dat de operationele activiteiten van ondernemingen kwetsbaar worden voor beveiligingsincidenten, waaronder

[1] https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

[2] Het door Eiopa naar aanleiding van het FinTech-actieplan van de Commissie gepubliceerde verslag is hier te vinden.

cyberaanvallen. Daarom is het belangrijk om ervoor te zorgen dat ondernemingen voldoende zijn voorbereid op het beheer van hun ICT- en beveiligingsrisico's.

8. Gezien de noodzaak van een goede voorbereiding op cyberrisico's[3] en van een degelijk cyberveiligheidskader bij ondernemingen, beslaan deze richtsnoeren daarnaast ook cyberveiligheid als onderdeel van de informatiebeveiligingsmaatregelen van de onderneming. Het uitgangspunt van deze richtsnoeren is dat cyberveiligheid onderdeel moet vormen van het algemene ICT- en beveiligingsrisicobeheer van een onderneming, maar er zij ook op gewezen dat cyberaanvallen een aantal specifieke kenmerken hebben waarmee rekening moet worden gehouden om ervoor te zorgen dat cyberrisico's op toereikende wijze door informatiebeveiligingsmaatregelen worden beperkt:

   a) cyberaanvallen zijn vaak moeilijker aan te pakken (d.w.z. te identificeren, te voorkomen, op te sporen, te bestrijden en te verhelpen) dan de meeste andere bronnen van ICT- en beveiligingsrisico's, terwijl ook de omvang van de schade moeilijk is vast te stellen;

   b) bij sommige cyberaanvallen kunnen normale risicobeheers- en bedrijfscontinuïteitsregelingen, evenals herstelprocedures, niet doeltreffend blijken, aangezien malware in back-upsystemen kan terechtkomen, waardoor deze niet langer beschikbaar zijn, en back-upgegevens kunnen worden beschadigd;

   c) dienstverrichters, makelaars, (gevolmachtigd) agenten en tussenpersonen kunnen een toegangspoort worden voor de verspreiding van cyberaanvallen. Onopgemerkte besmettelijke dreigingen kunnen als gevolg van interconnectiviteit via externe telecommunicatieverbindingen het ICT-systeem van de onderneming binnendringen. Daarom kan een verbonden onderneming die op zichzelf minder relevant is, kwetsbaar worden en een bron worden voor de verspreiding van risico's, met alle systemische gevolgen van dien. Overeenkomstig het beginsel van de zwakste schakel moeten niet alleen marktdeelnemers of cruciale dienstverrichters de nodige aandacht besteden aan cyberveiligheid.

9. Deze richtsnoeren hebben ten doel:

   a) marktdeelnemers duidelijkheid en transparantie te bieden over de minimale verwachte mogelijkheden op het gebied van informatie- en cyberveiligheid (basisveiligheid);

   b) mogelijke regelgevingsarbitrage te voorkomen;

   c) de convergentie van het toezicht met betrekking tot de eisen en toepasselijke procedures op het gebied van ICT-beveiliging en -governance te bevorderen als fundamentele voorwaarde voor een goed ICT- en beveiligingsrisicobeheer.

[3] Raadpleeg voor een definitie van "cyberrisico" het FSB Cyber Lexicon, 12 november 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf

Richtsnoeren betreffende beveiliging en governance van informatie- en communicatietechnologie

Inleiding

1. In overeenstemming met artikel 16 van Verordening (EU) nr. 1094/2010[4] vaardigt Eiopa deze tot de toezichthoudende autoriteiten gerichte richtsnoeren uit over de wijze waarop verzekerings- en herverzekeringsondernemingen (hierna gezamenlijk aangeduid als "ondernemingen") de governancebepalingen van Richtlijn 2009/138/EG[5] (hierna: "richtlijn Solvabiliteit II") en van Gedelegeerde Verordening (EU) 2015/35 van de Commissie[6] (hierna: "gedelegeerde verordening") dienen toe te passen in het kader van de beveiliging en governance op het gebied van informatie- en communicatietechnologie (hierna: "ICT"). Daartoe bouwen deze richtsnoeren voort op de governancebepalingen van de artikelen 41, 44, 46, 47, 132 en 246 van de richtlijn Solvabiliteit II en de artikelen 258 tot en met 260, 266, 268 tot en met 271 en 274 van de gedelegeerde verordening. Daarnaast bouwen deze richtsnoeren voort op de adviezen die zijn opgenomen in de Eiopa-richtsnoeren voor het governancesysteem (EIOPA-BoS-14/253)[7] en de Eiopa-richtsnoeren voor uitbesteding aan aanbieders van clouddiensten (EIOPA-BoS-19/270)[8].
2. De richtsnoeren gelden voor individuele ondernemingen en mutatis mutandis ook op groepsniveau[9].
3. De bevoegde autoriteiten moeten, wanneer zij deze richtsnoeren naleven of toezien op de naleving van deze richtsnoeren, rekening houden met het evenredigheidsbeginsel[10], dat moet waarborgen dat governanceregelingen, met inbegrip van regelingen voor ICT-beveiliging en -governance, in verhouding staan tot de aard, schaal en complexiteit van de overeenkomstige risico's waarmee ondernemingen geconfronteerd worden of kunnen worden.
4. Deze richtsnoeren moeten worden gelezen in samenhang met en onverminderd de toepassing van de richtlijn Solvabiliteit II, de gedelegeerde verordening, de Eiopa-richtsnoeren voor het governancesysteem en de Eiopa-richtsnoeren voor uitbesteding aan aanbieders van clouddiensten. Deze richtsnoeren beogen technologie- en methodologieneutraal te zijn.

Definities

5. Termen die niet zijn gedefinieerd in deze richtsnoeren, hebben de betekenis die is vastgelegd in de richtlijn Solvabiliteit II.
6. Voor de toepassing van deze richtsnoeren wordt verstaan onder:

---

4 Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/79/EG van de Commissie (PB L 331 van 15.12.2010, blz. 48).

5 Richtlijn 2009/138/EG van het Europees Parlement en de Raad van 25 november 2009 betreffende de toegang tot en uitoefening van het verzekerings- en het herverzekeringsbedrijf (Solvabiliteit II) (PB L 335 van 17.12.2009, blz. 1).

6 Gedelegeerde Verordening (EU) 2015/35 van de Commissie van 10 oktober 2014 tot aanvulling van Richtlijn 2009/138/EG van het Europees Parlement en de Raad betreffende de toegang tot en uitoefening van het verzekerings- en het herverzekeringsbedrijf (Solvabiliteit II) (PB L 12 van 17.1.2015, blz. 1).

7 https://www.eiopa.europa.eu/content/guidelines-system-governance_nl?source=search

8 https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en

9 Artikel 212, lid 1, van Richtlijn 2009/138/EG.

10 Artikel 29, lid 3, van Richtlijn 2009/138/EG.

eigenaar van een asset	Een persoon of entiteit met de verantwoordelijkheid voor en het gezag over een informatie- en ICT-asset.
Beschikbaarheid	De eigenschap van toegankelijkheid en (tijdige) beschikbaarheid voor gebruik op verzoek voor een bevoegde entiteit.
Vertrouwelijkheid	De eigenschap dat informatie niet beschikbaar wordt gesteld aan of verstrekt aan niet-geautoriseerde personen, entiteiten, processen of systemen.
Cyberaanval	Iedere vorm van hacken die leidt tot een aanval of kwaadaardige poging tot een aanval gericht op ICT-systemen met het doel om een informatie-asset te vernietigen, openbaar te maken, te wijzigen, uit te schakelen of te stelen of hiertoe onbevoegde toegang te verkrijgen of hiervan onbevoegd gebruik te maken.
Cyberveiligheid	Het behoud van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en/of informatiesystemen via het cybermedium.
ICT-asset	Een software of hardware asset die deel uitmaakt van de bedrijfsomgeving.
ICT-projecten	Elk project of onderdeel daarvan waarbij ICT-systemen en -diensten worden gewijzigd, vervangen of uitgevoerd.
ICT- en beveiligingsrisico	Onderdeel van het operationeel risico, bestaand in het risico van verliezen als gevolg van inbreuken op de vertrouwelijkheid, falende integriteit van systemen en gegevens, ongeschiktheid of onbeschikbaarheid van systemen en gegevens, of onvermogen om ICT aan te passen binnen een redelijke termijn en tegen redelijke kosten wanneer de omgeving of de bedrijfsvereisten veranderen ("agility"). Dit omvat ook cyber- en informatiebeveiligingsrisico's die voortvloeien uit ontoereikende of falende interne processen of externe gebeurtenissen met inbegrip van cyberaanvallen of ontoereikende fysieke beveiliging.

Informatiebeveiliging	Het behoud van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en/of informatiesystemen. Tevens kan het gaan om andere eigenschappen, zoals authenticiteit, verantwoording, onweerlegbaarheid en betrouwbaarheid.
ICT-diensten	Diensten die door ICT-systemen en dienstverrichters aan een of meerdere interne of externe gebruikers worden verstrekt.
ICT-systemen	Reeks toepassingen, diensten, IT-assets, ICT-assets of andere informatieverwerkende componenten, met inbegrip van de bedrijfsomgeving.
Informatie-asset	Een materiële of immateriële verzameling informatie, die het beschermen waard is.
Integriteit	De eigenschap van nauwkeurigheid en volledigheid.
Operationeel of veiligheidsincident	Een op zichzelf staande gebeurtenis of een reeks met elkaar verbonden niet-geplande gebeurtenissen die een nadelig effect heeft of waarschijnlijk zal hebben op de integriteit, beschikbaarheid en vertrouwelijkheid van ICT-systemen en -diensten.
Dienstverrichter	Een derde die een proces, dienst of activiteit, of onderdelen daarvan, verricht op grond van een uitbestedingsovereenkomst.
Hacktesten op basis van dreigingsinformatie (Threat Led Penetration Testing – TLPT)	Een gecontroleerde poging om de cyberweerbaarheid van een entiteit te doorbreken door de tactieken, technieken en procedures van daadwerkelijke dreigingsactoren te simuleren. Een dergelijke poging is gebaseerd op gerichte dreigingsinformatie en richt zich op medewerkers, processen en technologie van een entiteit, bij minimale voorkennis en met minimale gevolgen voor de bedrijfsvoering.
Kwetsbaarheid	Een zwak punt, vatbaarheid voor risico's of defect in een asset of de controle daarover waardoor zich een dreiging kan voordoen.

7. Deze richtsnoeren zijn van toepassing vanaf 1 juli 2021.

Richtsnoer 1 – Evenredigheid

8. Ondernemingen dienen deze richtsnoeren toe te passen op een wijze die in verhouding staat tot de aard, schaal en complexiteit van de risico's die verbonden zijn aan hun bedrijf.

Richtsnoer 2 – ICT binnen het governancesysteem

9. Het bestuurlijk, beleidsbepalend of toezichthoudend orgaan (Administrative, Management or Supervisory Body, hierna: "AMSB") moet waarborgen dat het governancesysteem van de ondernemingen, in het bijzonder het risicobeheers- en het interne-controlesysteem, de ICT- en beveiligingsrisico's van de onderneming op adequate wijze beheert.

10. Het AMSB moet ervoor zorgen dat de omvang en vaardigheden van het personeel van de onderneming passend zijn om doorlopend aan hun operationele ICT-behoeften en risicobeheerprocedures inzake ICT en beveiliging van de onderneming te voldoen en de uitvoering van de ICT-strategie ervan te waarborgen. Daarnaast moet het personeel regelmatig passende scholing met betrekking tot ICT- en beveiligingsrisico's krijgen, met inbegrip van informatieveiligheid, zoals beschreven in richtsnoer 13.

11. Het AMSB moet ervoor zorgen dat de toegekende middelen geschikt zijn om aan de bovenstaande vereisten te voldoen.

Richtsnoer 3 – ICT-strategie

12. Het AMSB heeft de algemene verantwoordelijkheid voor het vaststellen en goedkeuren van de schriftelijke ICT-strategie van de onderneming als onderdeel van en afgestemd op de algehele bedrijfsstrategie, evenals voor het toezicht op de communicatie en uitvoering ervan.

13. In de ICT-strategie moet ten minste het volgende worden vastgelegd:

    a) hoe de ICT van de onderneming moet worden ontwikkeld om de bedrijfsstrategie doeltreffend te ondersteunen en uit te voeren, met inbegrip van de ontwikkeling van de organisatiestructuur, bedrijfsmodellen, het ICT-systeem en cruciale dienstverlening door dienstverrichters;

    b) de ontwikkeling van de ICT-architectuur, met inbegrip van de dienstverlening door dienstverrichters; en

    c) duidelijke doelstellingen inzake informatiebeveiliging, met de nadruk op ICT-systemen en -diensten, personeel en processen.

14. Ondernemingen moeten waarborgen dat de ICT-strategie tijdig wordt uitgevoerd, vastgesteld en meegedeeld aan al het relevante personeel en de relevante dienstverrichters, voor zover van toepassing en relevant.

15. Ondernemingen moeten ook een procedure ontwikkelen om de doeltreffendheid van de uitvoering van de ICT-strategie te monitoren en meten. Die procedure moet regelmatig worden herzien en bijgewerkt.

Richtsnoer 4 – ICT- en beveiligingsrisico's binnen het risicobeheerssysteem

16. Het AMSB heeft de algehele verantwoordelijkheid voor het opzetten van een doeltreffend systeem voor het beheer van ICT- en beveiligingsrisico's als onderdeel van het algehele risicobeheerssysteem van de onderneming. Dit omvat de

vaststelling van de risicotolerantie voor deze risico's, in overeenstemming met de risicostrategie van de onderneming, en een periodiek schriftelijk verslag over het resultaat van het risicobeheersproces dat is gericht aan het AMSB.

17. Als onderdeel van het totale risicobeheerssysteem moeten ondernemingen voor wat betreft ICT- en beveiligingsrisico's (bij het opstellen van de vereisten op het gebied van ICT-bescherming zoals hieronder beschreven) ten minste het volgende in acht nemen:

    a) ondernemingen moeten hun bedrijfsprocessen en -activiteiten, bedrijfsfuncties, rollen en assets (zoals informatie- en ICT-assets) in kaart brengen en regelmatig bijwerken, om daarvan het belang voor ICT- en beveiligingsrisico's vast te stellen en hun onderlinge afhankelijkheden te bepalen;

    b) ondernemingen moeten alle relevante ICT- en beveiligingsrisico's waaraan zij zijn blootgesteld, identificeren en meten en de geïdentificeerde bedrijfsprocessen en -activiteiten, bedrijfsfuncties, rollen en assets (zoals informatie- en ICT-assets) indelen op basis van hun kriticiteit. Ondernemingen moeten ook de beschermingsvereisten beoordelen van, ten minste, de vertrouwelijkheid, integriteit en beschikbaarheid van deze bedrijfsprocessen en-activiteiten, bedrijfsfuncties, rollen en assets (zoals informatie- en ICT-assets). Eigenaren van een asset, die verantwoordelijk zijn voor de classificatie ervan, moeten worden geïdentificeerd;

    c) de methoden die worden gebruikt ter bepaling van de kriticiteit, evenals het vereiste beschermingsniveau, met name in verband met de beschermingsdoelstellingen van integriteit, beschikbaarheid en vertrouwelijkheid, moeten waarborgen dat de resulterende beschermingsvereisten consistent en alomvattend zijn;

    d) de meting van de ICT- en beveiligingsrisico's moet worden uitgevoerd op basis van de vastgestelde ICT- en beveiligingsrisicocriteria waarbij rekening wordt gehouden met de kriticiteit van de bedrijfsprocessen en -activiteiten, bedrijfsfuncties, rollen en assets (zoals informatie- en ICT-assets), de omvang van bekende kwetsbaarheden en eerdere incidenten die invloed hebben gehad op de onderneming;

    e) de beoordeling van de ICT- en beveiligingsrisico's moet regelmatig worden uitgevoerd en gedocumenteerd. Deze beoordeling moet ook worden uitgevoerd voorafgaand aan eventuele belangrijke wijzigingen in de infrastructuur, processen of procedures die van invloed zijn op de bedrijfsprocessen en -activiteiten, bedrijfsfuncties, rollen en assets (zoals informatie- en ICT-assets);

    f) ondernemingen moeten op basis van hun risicobeoordeling ten minste maatregelen vaststellen en uitvoeren om de geïdentificeerde ICT- en beveiligingsrisico's te beheren en de informatie-assets te beschermen in overeenstemming met hun classificatie. Hiertoe behoort tevens de vaststelling van maatregelen om de resterende risico's te beheren.

18. De resultaten van het beheersproces voor ICT- en beveiligingsrisico's moet worden goedgekeurd door het AMSB en worden opgenomen in het proces van het operationeel risicobeheer, als onderdeel van het totale risicobeheer van de ondernemingen.

Richtsnoer 5 – Audit

19. De governance, systemen en processen van ondernemingen voor hun ICT- en beveiligingsrisico's moeten periodiek worden gecontroleerd in overeenstemming met het auditplan[11] van de ondernemingen door auditors met voldoende kennis, vaardigheden en deskundigheid op het gebied van ICT- en beveiligingsrisico's om onafhankelijke waarborging van hun doeltreffendheid te verstrekken aan het AMSB. De frequentie en gerichtheid van dergelijke audits moeten evenredig zijn aan de relevante ICT- en beveiligingsrisico's.

Richtsnoer 6 – Beleidslijnen en maatregelen op het gebied van informatiebeveiliging

20. Ondernemingen moeten schriftelijke beleidslijnen op het gebied van informatiebeveiliging opstellen, die moeten worden goedgekeurd door het AMSB en waarin de hoofdbeginselen en -voorschriften zijn vastgesteld voor de bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie van de onderneming om de uitvoering van de ICT-strategie ervan te ondersteunen.

21. Het beleid omvat een omschrijving van de belangrijkste taken en verantwoordelijkheden inzake informatiebeveiligingsbeheer en zet de vereisten voor personeel, processen en technologie met betrekking tot informatiebeveiliging uiteen, waarbij wordt erkend dat personeelsleden op alle niveaus verantwoordelijkheid dragen om de informatiebeveiliging van de ondernemingen te waarborgen.

22. De beleidslijnen moeten worden verspreid binnen de onderneming en van toepassing zijn op alle personeelsleden. Indien van toepassing en relevant moeten de beleidslijnen voor informatiebeveiliging of delen daarvan ook worden meegedeeld aan en toegepast op dienstverrichters.

23. Ondernemingen moeten op basis van de beleidslijnen specifiekere informatiebeveiligingsprocedures en -maatregelen vaststellen en uitvoeren om, onder andere, de ICT- en beveiligingsrisico's waaraan zij zijn blootgesteld, te beperken. Deze procedures en informatiebeveiligingsmaatregelen moeten elk proces omvatten dat in deze richtsnoeren wordt beschreven, voor zover van toepassing.

Richtsnoer 7 – Informatiebeveiligingsfunctie

24. Ondernemingen moeten, binnen hun governancesysteem en in overeenstemming met het evenredigheidsbeginsel, een informatiebeveiligingsfunctie opzetten, waarbij de verantwoordelijkheden worden toegewezen aan een specifieke persoon. De onderneming moet de onafhankelijkheid en objectiviteit van deze informatiebeveiligingsfunctie waarborgen door deze op passende wijze te scheiden van processen inzake ICT-activiteiten en bedrijfsvoering. De functie moet verslag uitbrengen aan het AMSB.

25. De taken van de informatiebeveiligingsfunctie bestaan in de regel in het volgende:

    a) ondersteunen van het AMSB bij de opstelling en het bijhouden van de beleidslijnen voor informatiebeveiliging voor ondernemingen en de uitrol ervan controleren;

[11] Artikel 271 van de gedelegeerde verordening.

b) aan het AMSB regelmatig en op ad-hocbasis verslag uitbrengen en het orgaan adviseren over de status van de informatiebeveiliging en de ontwikkelingen ervan;

c) de uitvoering van de informatiebeveiligingsmaatregelen monitoren en beoordelen;

d) waarborgen dat aan de vereisten op het gebied van informatiebeveiliging wordt voldaan wanneer dienstverrichters worden ingezet;

e) waarborgen dat alle medewerkers en dienstverrichters die toegang hebben tot informatie en systemen, op passende wijze zijn geïnformeerd over de beleidslijnen voor informatiebeveiliging, bijvoorbeeld door middel van opleidings- en bewustmakingssessies voor informatiebeveiliging;

f) coördineren van het onderzoek van operationele of veiligheidsincidenten en relevante incidenten rapporteren aan het ASMB.

Richtsnoer 8 – Logische beveiliging

26. Ondernemingen moeten procedures definiëren, documenteren en uitvoeren voor logische toegangscontrole of logische beveiliging (identiteits- en toegangsbeheer) in overeenstemming met de in richtsnoer 4 gedefinieerde beschermingsvereisten. Deze procedures moeten worden uitgevoerd, gehandhaafd, gemonitord en periodiek herzien en moeten tevens controles omvatten voor de monitoring van onregelmatigheden. Deze procedures moeten ten minste de volgende onderdelen uitvoeren, waarbij de term "gebruiker" ook technische gebruikers omvat:

    a) "need-to-know", "least privilege" en functiescheiding: ondernemingen dienen toegangsrechten, met inbegrip van toegang op afstand, voor informatie-assets en hun ondersteunende systemen te beheren volgens het beginsel van "kennisnemingsbehoefte". Gebruikers krijgen de minimale toegangsrechten toegekend die strikt noodzakelijk zijn om hun taken uit te voeren (beginsel van "least privilege"), d.w.z. om ongerechtvaardigde toegang tot gegevens te voorkomen of te voorkomen dat de toewijzing van combinaties van toegangsrechten kan worden gebruikt om controles te omzeilen (beginsel van "scheiding van functies");

    b) gebruikersverantwoordelijkheid: ondernemingen moeten het gebruik van generieke en gedeelde gebruikersaccounts zo veel mogelijk beperken en waarborgen dat gebruikers te allen tijde kunnen worden geïdentificeerd en getraceerd naar een verantwoordelijke natuurlijke persoon of een bevoegde taak voor de handelingen die worden verricht in de ICT-systemen;

    c) geprivilegieerde toegangsrechten: ondernemingen dienen beheersmaatregelen uit te voeren voor geprivilegieerde systeemtoegang door accounts met meer systeemtoegang (zoals beheerdersaccounts) strikt te beperken en hier nauw op toe te zien;

    d) toegang op afstand: om een veilige communicatie te garanderen en risico's te verminderen, dient de toegang op afstand tot kritieke ICT-systemen alleen toegekend te worden volgens kennisnemingsbehoefte en wanneer er sterke authenticatiemiddelen worden gebruikt;

    e) registreren van gebruikersactiviteiten: de activiteiten van gebruikers moeten op een risico-evenredige manier worden gelogd en gemonitord en minimaal bestaan uit de activiteiten van geprivilegieerde gebruikers. Logbestanden dienen beveiligd te zijn om ongeoorloofde wijziging of verwijdering te

voorkomen, en dienen bijgehouden te worden gedurende een periode die in verhouding staat tot het kritieke karakter van de geïdentificeerde bedrijfsfuncties, ondersteunende processen en informatie-assets, onverminderd de gegevensbewaringsvereisten van de nationale en EU-wetgeving. Ondernemingen dienen deze gegevens te gebruiken om de identificatie en het onderzoek te vergemakkelijken van onregelmatigheden die worden geconstateerd bij het verlenen van de diensten;

f) toegangsbeheer: toegangsrechten moeten tijdig worden verleend, verwijderd en aangepast overeenkomstig vooraf vastgestelde goedkeuringsprocedures, waarbij de betreffende eigenaar van een informatie-asset wordt betrokken. Indien toegang niet langer noodzakelijk is, moeten toegangsrechten onmiddellijk worden ingetrokken;

g) toegangsbeoordeling: toegangsrechten dienen regelmatig te worden herzien om te garanderen dat gebruikers geen buitensporige voorrechten hebben en dat toegangsrechten zijn ingetrokken/verwijderd wanneer ze niet langer noodzakelijk zijn;

h) het verlenen, aanpassen en intrekken van toegangsrechten moet zodanig worden gedocumenteerd dat inzicht en analyse worden vergemakkelijkt; en

i) authenticatiemethoden: ondernemingen dienen authenticatiemethoden te handhaven die voldoende robuust zijn om er passend en doeltreffend voor te zorgen dat beleidslijnen en procedures inzake toegangscontrole worden nageleefd. Authenticatiemethoden dienen in verhouding te staan tot het kritieke karakter van de ICT-systemen, de informatie of het proces waar toegang tot wordt verkregen. Dit betreft ten minste sterke wachtwoorden of sterkere authenticatiemethoden (zoals tweefactorauthenticatie), gebaseerd op relevante risico's.

27. Elektronische toegang van applicaties tot gegevens en ICT-systemen dient beperkt te worden tot het minimum dat nodig is om de desbetreffende diensten te kunnen aanbieden.

Richtsnoer 9 – Fysieke beveiliging

28. De fysieke beveiligingsmaatregelen van ondernemingen (zoals bescherming tegen stroomstoringen, brand, water en onbevoegde fysieke toegang) moeten worden vastgelegd, gedocumenteerd en uitgevoerd om het terrein, de datacentra en gevoelige gebieden te beschermen tegen onbevoegde toegang en milieugevaren.

29. De fysieke toegang tot ICT-systemen mag alleen worden toegestaan aan bevoegde personen. Bevoegdheden moeten worden verleend overeenkomstig de taken en verantwoordelijkheden van de persoon, en worden beperkt tot personen die naar behoren worden opgeleid en gecontroleerd. De fysieke toegang moet regelmatig worden herzien om te waarborgen dat onnodige toegangsrechten onmiddellijk worden ingetrokken/verwijderd.

30. Passende maatregelen ter bescherming tegen milieugevaren moeten in verhouding staan tot het belang van de gebouwen en het kritieke karakter van de werkzaamheden of ICT-systemen die in deze gebouwen gevestigd zijn.

Richtsnoer 10 – Beveiliging van ICT-operaties

31. Ondernemingen moeten procedures uitvoeren om de vertrouwelijkheid, integriteit en beschikbaarheid van ICT-systemen en -diensten te waarborgen om de gevolgen van beveiligingsproblemen bij de verlening van ICT-diensten te minimaliseren. In

deze procedures moeten op passende wijze de volgende maatregelen opgenomen zijn:

a) identificatie van potentiële kwetsbaarheden die geëvalueerd en hersteld dienen te worden door ervoor te zorgen dat ICT-systemen bijgewerkt zijn, met inbegrip van de software die door de ondernemingen aan hun interne en externe gebruikers wordt verstrekt, door kritieke veiligheidspatches, met inbegrip van updates van antivirusdefinities, uit te rollen, of door compenserende controles uit te voeren;

b) uitvoering van veilige referentiescenario's voor de configuratie van alle kritieke componenten, zoals besturingssystemen, databases, routers of schakelaars;

c) uitvoering van netwerksegmentatie, systemen voor de voorkoming van gegevenslekken en de versleuteling van netwerkverkeer (in overeenstemming met de classificatie van het informatie-asset);

d) uitvoering van de bescherming van eindpunten, met inbegrip van servers, werkstations en mobiele apparaten. Ondernemingen moeten evalueren of een eindpunt voldoet aan de door hen gedefinieerde beveiligingsnormen voordat toegang wordt verleend tot het bedrijfsnetwerk;

e) waarborgen dat mechanismen voor integriteitscontrole zijn ingevoerd om de integriteit van ICT-systemen te verifiëren;

f) versleuteling van gegevens in rust- en in overgangstoestand (in overeenstemming met de classificatie van het informatie-asset).

Richtsnoer 11 – Beveiligingsmonitoring

32. Ondernemingen moeten procedures en processen opstellen en uitvoeren om activiteiten die van invloed zijn op de informatiebeveiliging van de onderneming voortdurend te monitoren. Deze monitoring omvat ten minste het volgende:

    a) interne en externe factoren, inclusief bedrijfs- en ICT-beheersfuncties;

    b) transacties door dienstverrichters, andere entiteiten en interne gebruikers; en

    c) potentiële interne en externe bedreigingen.

33. Op basis van de monitoring moeten de ondernemingen passende en doeltreffende mogelijkheden uitvoeren voor het opsporen en rapporteren van, en reageren op onregelmatigheden en dreigingen, zoals fysieke of logische binnendringing, schendingen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie-assets, kwaadaardige code en algemeen bekende kwetsbaarheden voor software en hardware.

34. De rapportage van de beveiligingsmonitoring moet ondernemingen helpen inzicht te krijgen in de aard van zowel operationele als veiligheidsincidenten, voor het identificeren van trends en het ondersteunen van de interne onderzoeken van ondernemingen om hen in staat te stellen passende beslissingen te nemen.

Richtsnoer 12 – Evaluaties, beoordeling en testen van informatiebeveiliging

35. Ondernemingen dienen een verscheidenheid aan verschillende evaluaties, beoordelingen en tests van de informatiebeveiliging uit te voeren om een doeltreffende identificatie van kwetsbaarheden in hun ICT-systemen en -diensten te waarborgen. Zo kunnen ondernemingen bijvoorbeeld gapanalysen uitvoeren op

het gebied van informatiebeveiligingsnormen, nalevingscontroles, interne en externe audits van de informatiesystemen, of fysieke beveiligingsevaluaties.

36. Ondernemingen moeten een toetsingskader voor informatiebeveiliging opstellen en uitvoeren dat de robuustheid en doeltreffendheid van de informatiebeveiligingsmaatregelen valideert, en ervoor zorgen dat dit binnen dit kader rekening wordt gehouden met bedreigingen en kwetsbaarheden die zijn geïdentificeerd via monitoring van bedreigingen en het risicobeoordelingsproces inzake ICT en beveiliging.
37. Tests moeten op een veilige manier worden uitgevoerd door onafhankelijke testers met voldoende kennis, vaardigheden en deskundigheid in het testen van informatiebeveiligingsmaatregelen.
38. Ondernemingen moeten regelmatig tests uitvoeren. De omvang, frequentie en methode van het testen (zoals penetratietests, inclusief hacktests op basis van dreigingsinformatie) moeten zijn afgestemd op het geïdentificeerde risiconiveau. Het testen van kritieke ICT-systemen en kwetsbaarheidsscans moet jaarlijks worden uitgevoerd.
39. Ondernemingen moeten ervoor zorgen dat tests van beveiligingsmaatregelen worden uitgevoerd in het geval van wijzigingen aan de infrastructuur, processen of procedures, en indien wijzigingen worden doorgevoerd wegens grote operationele of beveiligingsincidenten, of wegens de vrijgave van nieuwe of aanzienlijk gewijzigde kritieke toepassingen. Ondernemingen moeten resultaten van de beveiligingstests controleren en evalueren, en hun beveiligingsmaatregelen dienovereenkomstig onverwijld aanpassen wanneer het gaat om kritische ICT-systemen.

Richtsnoer 13 – Opleiding en bewustmaking op het gebied van informatiebeveiliging

40. Ondernemingen moeten opleidingsprogramma's op het gebied van informatiebeveiliging opstellen voor alle personeelsleden, inclusief leden van het AMSB, om ervoor te zorgen dat ze zijn opgeleid voor de uitvoering van hun taken en verantwoordelijkheden en om menselijke fouten, diefstal, fraude, misbruik of verlies te beperken. Ondernemingen moeten ervoor zorgen dat het opleidingsprogramma regelmatig opleiding verzorgt voor alle personeelsleden.
41. Ondernemingen moeten regelmatige programma's voor veiligheidsbewustzijn opstellen en uitvoeren om hun personeelsleden, inclusief leden van het AMSB, op te leiden en te informeren over informatiebeveiligingsrisico's.

Richtsnoer 14 – Beheer van ICT-operaties

42. Ondernemingen moeten hun ICT-operaties beheren op basis van de ICT-strategie. In documenten moet worden vastgesteld hoe ondernemingen de ICT-systemen en -diensten uitvoeren, monitoren en controleren, met inbegrip van het documenteren van kritieke ICT-processen, -procedures en -operaties.
43. Ondernemingen moeten procedures inzake het bijhouden van logbestanden en monitoring uitvoeren voor kritieke ICT-activiteiten zodat fouten kunnen worden opgespoord, geanalyseerd en gecorrigeerd.
44. Ondernemingen moeten een actuele inventaris van hun ICT-assets bijhouden. De inventaris van de ICT-assets moet voldoende gedetailleerd zijn om een onmiddellijke identificatie van een ICT-asset, de locatie, de beveiligingsclassificatie en de eigenaar ervan mogelijk te maken.

45. Ondernemingen moeten de levenscyclus van ICT-assets monitoren en beheren, om te waarborgen dat deze blijven voldoen aan vereisten inzake bedrijfs- en risicobeheer, en deze ondersteunen. Ondernemingen moeten monitoren of hun ICT-assets worden ondersteund door hun toeleveranciers of interne ontwikkelaars, en of alle relevante patches en upgrades worden toegepast op basis van een gedocumenteerd proces. De risico's die afkomstig zijn van verouderde of niet-ondersteunde ICT-assets, moeten worden beoordeeld en beperkt. Uit bedrijf genomen ICT-assets moeten op veilige wijze worden verwerkt en afgevoerd.

46. Ondernemingen moeten plannings- en monitoringsprocessen met betrekking tot prestaties en capaciteit uitvoeren om belangrijke prestatieproblemen van ICT-systemen en ICT-capaciteitstekorten te voorkomen en tijdig op te sporen en aan te pakken.

47. Ondernemingen moeten back-up- en herstelprocedures voor gegevens en ICT-systemen vaststellen en uitvoeren zodat deze waar nodig kunnen worden hersteld. De omvang en frequentie van back-ups moeten worden vastgesteld in overeenstemming met de bedrijfsvereisten inzake herstel en met het kritieke karakter van de gegevens en de ICT-systemen, en moeten worden geëvalueerd volgens de uitgevoerde risicobeoordeling. De back-up- en herstelprocedures moeten op regelmatige basis worden uitgevoerd.

48. Ondernemingen moeten ervoor zorgen dat gegevens- en ICT-systeemback-ups worden opgeslagen op één of meer locaties buiten de primaire locatie, die veilig moeten zijn en zich op voldoende afstand van de primaire locatie moeten bevinden om te voorkomen dat ze worden blootgesteld aan dezelfde risico's.

Richtsnoer 15 – Beheer van ICT-incidenten en -problemen

49. Ondernemingen moeten een beheerproces voor incidenten en problemen opstellen en uitvoeren om operationele of veiligheidsincidenten te monitoren en hiervan logbestanden bij te houden en om ondernemingen in staat te stellen kritieke bedrijfsfuncties en -processen voort te zetten of weer op te nemen wanneer verstoringen optreden.

50. Ondernemingen dienen de gepaste criteria en drempelwaarden vast te leggen om een gebeurtenis te classificeren als een operationeel of veiligheidsincident, evenals vroegtijdige waarschuwingsindicatoren om een vroegtijdige detectie van deze incidenten mogelijk te maken.

51. Om de impact van ongewenste voorvallen tot een minimum te beperken en tijdig herstel mogelijk te maken, moeten ondernemingen passende processen en organisatiestructuren invoeren om een consistente en geïntegreerde monitoring, behandeling en opvolging van operationele en veiligheidsincidenten te waarborgen teneinde te waarborgen dat de onderliggende oorzaken worden geïdentificeerd en aangepakt en correctieve acties worden ondernomen en/of maatregelen worden getroffen om te voorkomen dat het incident zich nogmaals voordoet. Het proces voor incidenten- en probleembeheer moet, ten minste, het volgende omvatten:

    a) de procedures om incidenten te identificeren, te registreren via logbestanden, te categoriseren en in te delen volgens een prioriteit die door de onderneming is vastgesteld en is gebaseerd op het bedrijfskritieke karakter ervan en dienstenovereenkomsten;

    b) de taken en verantwoordelijkheden voor verschillende incidentenscenario's (bv. fouten, slecht functioneren, cyberaanvallen);

c) een probleembeheerprocedure om de onderliggende oorzaak van één of meerdere incidenten te identificeren, te analyseren en op te lossen — een onderneming moet de operationele of veiligheidsincidenten analyseren die zijn geïdentificeerd of die zich hebben voorgedaan binnen of buiten de organisatie, en zij moet belangrijke lessen trekken uit deze analysen en de veiligheidsmaatregelen dienovereenkomstig bijwerken;

d) effectieve plannen voor interne communicatie, inclusief procedures voor incidentmelding en escalatie, die ook de behandeling van beveiligingsgerelateerde klachten van klanten omvatten, om te waarborgen dat:

   i. incidenten met potentieel ernstige negatieve gevolgen voor kritieke ICT-systemen en ICT-diensten worden gemeld aan de relevante hogere leidinggevenden;

   ii. het AMSB in het geval van ernstige incidenten op ad-hocbasis in kennis wordt gesteld en ten minste op de hoogte wordt gebracht van de impact, de reactie en de bijkomende controles die moeten worden vastgesteld als gevolg van de incidenten.

e) procedures voor de reactie op incidenten om de effecten die verband houden met de incidenten te verminderen en waarborgen dat de dienst snel operationeel en veilig wordt;

f) specifieke externe communicatieplannen voor kritieke bedrijfsfuncties en -processen om:

   i. samen te werken met de relevante belanghebbenden teneinde effectief te reageren op en te herstellen van het incident;

   ii. tijdige informatie, met inbegrip van incidentrapportage, te verstrekken aan externe partijen (bv. klanten, andere marktdeelnemers, de relevante (toezichthoudende) autoriteiten, indien van toepassing en in overeenstemming met geldende regelgeving).

Richtsnoer 16 – ICT-projectbeheer

52. Ondernemingen moeten een ICT-projectmethode invoeren (met inbegrip van een onafhankelijke beoordeling van de beveiligingsvereisten) met een toereikend governanceproces en verantwoording voor de projectuitvoering om de uitvoering van de ICT-strategie door middel van ICT-projecten op doeltreffende wijze te ondersteunen.

53. Ondernemingen moeten de risico's die voortvloeien uit de portefeuille van ICT-projecten op gepaste wijze monitoren en verminderen, ook rekening houdend met de risico's die het gevolg kunnen zijn van onderlinge afhankelijkheden tussen verschillende projecten en van afhankelijkheden van meerdere projecten van dezelfde hulpbronnen en/of deskundige partijen.

Richtsnoer 17 – Verwerving en ontwikkeling van ICT-systemen

54. Ondernemingen moeten een proces ontwikkelen en uitvoeren dat de verwerving, de ontwikkeling en het onderhoud van ICT-systemen beheert om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens voor de verwerking uitgebreid te beveiligen en ervoor te zorgen dat aan de vastgestelde beschermingsvereisten is voldaan. Dit proces moet worden ontworpen door middel van een risicogebaseerde benadering.

55. Ondernemingen moeten ervoor zorgen dat voordat systeemverwerkingen of ontwikkelingsactiviteiten worden uitgevoerd, de functionele en niet-functionele voorschriften (met inbegrip van de vereisten op het gebied van informatiebeveiliging), en technische doelstellingen duidelijk zijn gedefinieerd.

56. Ondernemingen moeten ervoor zorgen dat er maatregelen zijn ingevoerd om onbedoelde wijziging of opzettelijke manipulatie van de ICT-systemen tijdens de ontwikkeling te voorkomen.

57. Ondernemingen dienen een methode toe te passen voor het testen en goedkeuren van ICT-systemen, ICT-diensten en informatiebeveiligingsmaatregelen.

58. Ondernemingen moeten ICT-systemen, ICT-diensten en informatiebeveiligingsmaatregelen op passende wijze testen om potentiële zwakheden in de beveiliging, inbreuken en incidenten te identificeren.

59. Ondernemingen moeten de scheiding van productieomgevingen en ontwikkelings-, test- en andere niet-productieomgevingen waarborgen.

60. Ondernemingen moeten maatregelen uitvoeren ter bescherming van de integriteit van de broncode (indien beschikbaar) van ICT-systemen. Ook moeten ze de ontwikkeling, uitvoering, werking en/of configuratie van de ICT-systemen uitvoerig documenteren om alle onnodige afhankelijkheden van deskundigen over het onderwerp te verminderen.

61. De processen van ondernemingen voor de aankoop en ontwikkeling van ICT-systemen moeten ook van toepassing zijn op de ICT-systemen die worden ontwikkeld of beheerd door de eindgebruikers van de bedrijfsfunctie buiten de ICT-organisatie (bv. bedrijfsbeheerde toepassingen of informaticatoepassingen voor eindgebruikers) door middel van een risicogebaseerde benadering. De ondernemingen moeten een register bijhouden van deze toepassingen die kritieke bedrijfsfuncties of -processen ondersteunen.

Richtsnoer 18 - ICT-wijzigingenbeheer

62. Ondernemingen moeten een proces voor ICT-wijzigingenbeheer opstellen en uitvoeren om te waarborgen dat alle veranderingen aan ICT-systemen op gecontroleerde wijze worden geregistreerd, beoordeeld, getest, goedgekeurd, gecontroleerd en uitgevoerd. Wijzigingen tijdens dringende of noodzakelijke ICT-wijzigingen moeten traceerbaar zijn en achteraf worden gemeld aan de betreffende eigenaar van de asset voor analyse achteraf.

63. Ondernemingen dienen op doorlopende basis na te gaan of wijzigingen in de bestaande operationele omgeving gevolgen hebben voor de bestaande veiligheidsmaatregelen en of er bijkomende maatregelen genomen moeten worden om het risico in kwestie te verminderen. Deze wijzigingen moeten overeenstemmen met het formele wijzigingenbeheerproces van de onderneming.

Richtsnoer 19 – Beheer van de bedrijfscontinuïteit

64. Als onderdeel van de algehele beleidslijnen voor bedrijfscontinuïteit is het AMSB verantwoordelijk voor het vaststellen en goedkeuren van de beleidslijnen voor de ICT-continuïteit van de ondernemingen. De beleidslijnen voor de ICT-continuïteit moeten op passende wijze worden gecommuniceerd binnen ondernemingen en moeten van toepassing zijn op alle relevante personeelsleden en, indien relevant, op dienstverrichters.

Richtsnoer 20 – Bedrijfseffectbeoordeling

65. Als onderdeel van een solide beheer van de bedrijfscontinuïteit moeten ondernemingen een bedrijfseffectbeoordeling uitvoeren om de blootstelling te beoordelen van de onderneming aan ernstige bedrijfsonderbrekingen en de potentiële gevolgen ervan, zowel kwantitatief als kwalitatief, met behulp van interne en/of externe gegevens en scenarioanalyse. De bedrijfseffectbeoordeling moet tevens rekening houden met de kriticiteit van de geïdentificeerde en geclassificeerde bedrijfsprocessen en -activiteiten, bedrijfsfuncties, rollen en assets (zoals informatie- en ICT-assets) en de onderlinge afhankelijkheden in overeenstemming met richtsnoer 4.

66. Ondernemingen moeten ervoor zorgen dat hun ICT-systemen en ICT-diensten ontworpen en afgestemd zijn op hun bedrijfseffectbeoordeling, bijvoorbeeld door het vervangen van bepaalde kritieke onderdelen om verstoringen te voorkomen die het gevolg zijn van gebeurtenissen die een invloed hebben op deze onderdelen.

Richtsnoer 21 – Planning van de bedrijfscontinuïteit

67. De algemene bedrijfscontinuïteitsplannen van de ondernemingen moeten rekening houden met materiële risico's die een negatieve invloed kunnen hebben op ICT-systemen en -diensten. De plannen moeten de doelstellingen ondersteunen voor de bescherming en, indien noodzakelijk, het opnieuw vaststellen van de vertrouwelijkheid, integriteit en beschikbaarheid van de bedrijfsprocessen en -activiteiten, bedrijfsfuncties, rollen en assets (zoals informatie- en ICT-assets) van de ondernemingen. Ondernemingen moeten samenwerken met relevante interne en externe belanghebbenden, indien van toepassing, tijdens de opstelling van deze plannen.

68. Ondernemingen moeten bedrijfscontinuïteitsplannen invoeren om ervoor te zorgen dat ze op passende wijze kunnen reageren op mogelijke catastrofale scenario's binnen de doelstelling van een hersteltijd (de maximale tijd waarbinnen een systeem of proces moet worden hersteld na een incident) en een herstelpuntdoelstelling (de maximale periode waarin gegevens verloren kunnen gaan in geval van een incident op een vooraf vastgesteld dienstenniveau).

69. Ondernemingen moeten rekening houden met een reeks verschillende scenario's in hun bedrijfscontinuïteitsplannen, waaronder extreme, maar plausibele scenario's en cyberaanvalscenario's en de mogelijke gevolgen van dergelijke scenario's beoordelen. Op basis van deze scenario's moet een onderneming beschrijven hoe de continuïteit van de ICT-systemen en -diensten, evenals de informatiebeveiliging van de onderneming, worden gewaarborgd.

Richtsnoer 22 – Interventie- en herstelplannen

70. Op basis van de bedrijfseffectbeoordeling en plausibele scenario's moeten ondernemingen interventie- en herstelplannen ontwikkelen. In deze plannen moet worden gespecificeerd welke omstandigheden activering van de plannen op gang kunnen brengen, en welke acties moeten worden ondernomen om de integriteit, de beschikbaarheid, de continuïteit en het herstel van ten minste de kritieke ICT-systemen, ICT-diensten en gegevens te waarborgen. De interventie- en herstelplannen moeten erop zijn gericht de hersteldoelstellingen met betrekking tot de activiteiten van de ondernemingen te verwezenlijken.

71. De interventie- en herstelplannen moeten herstelmogelijkheden op zowel korte als, indien noodzakelijk, lange termijn in aanmerking nemen. De plannen moeten ten minste:

    a) gericht zijn op het herstel van de werking van belangrijke ICT-diensten, bedrijfsfuncties, ondersteunende processen, informatie-assets en de onderlinge afhankelijkheden ervan om negatieve gevolgen voor het functioneren van de onderneming te voorkomen;

    b) gedocumenteerd en beschikbaar zijn voor de zakelijke en ondersteunende afdelingen en gemakkelijk raadpleegbaar zijn in geval van nood, met inbegrip van een duidelijke definitie van rollen en verantwoordelijkheden; en

    c) voortdurend bijgewerkt worden in overeenstemming met de lessen die getrokken werden uit de incidenten, tests, nieuwe risico's en bedreigingen die geïdentificeerd worden, en gewijzigde hersteldoelstellingen en -prioriteiten.

72. In de plannen moet ook rekening worden gehouden met alternatieve mogelijkheden indien herstel op korte termijn niet haalbaar is omwille van de kosten, risico's, logistiek of onvoorziene omstandigheden.

73. Als onderdeel van de interventie- en herstelplannen moeten ondernemingen continuïteitsmaatregelen uit te werken en uit te voeren om eventueel falen van dienstverrichters op te vangen die van groot belang zijn voor de continuïteit van de ICT-diensten van de onderneming (in overeenstemming met de bepalingen in de Eiopa-richtsnoeren over het governancesysteem en de richtsnoeren over uitbesteding aan aanbieders van clouddiensten).

Richtsnoer 23 – Testen van plannen

74. Ondernemingen moeten hun bedrijfscontinuïteitsplannen testen en waarborgen dat de werking van hun kritieke bedrijfsprocessen en -activiteiten, bedrijfsfuncties, rollen en assets (zoals informatie- en ICT-assets) en hun onderlinge afhankelijkheden (waaronder die welke worden verleend door dienstverrichters) regelmatig worden getest op basis van het risicoprofiel van de onderneming.

75. Bedrijfscontinuïteitsplannen moeten regelmatig worden geactualiseerd, op basis van testresultaten, huidige inlichtingen inzake dreigingen en lessen die werden getrokken uit eerdere gebeurtenissen. Eventuele relevante wijzigingen in hersteldoelstellingen (waaronder de doelstelling voor hersteltijd en de herstelpuntdoelstelling) en/of wijzigingen in bedrijfsprocessen en -activiteiten, bedrijfsfuncties, rollen en assets (zoals informatie- en ICT-assets) moeten daarin ook worden opgenomen.

76. Het testen van bedrijfscontinuïteitsplannen moet aantonen dat deze plannen de levensvatbaarheid van het bedrijf kunnen volhouden totdat de kritieke werking is hersteld tot een vooraf vastgesteld dienstenniveau of impacttolerantie.

77. Testresultaten moeten worden gedocumenteerd en alle geïdentificeerde tekortkomingen die het resultaat zijn van de tests moeten worden geanalyseerd en aangepakt en worden gerapporteerd aan het AMSB.

Richtsnoer 24 – Crisiscommunicatie

78. Bij een storing of noodsituatie, en tijdens de uitvoering van de bedrijfscontinuïteitsplannen, dienen ondernemingen ervoor te zorgen dat ze doeltreffende crisiscommunicatiemaatregelen treffen, zodat alle relevante interne en externe belanghebbenden, waaronder relevante toezichthoudende autoriteiten,

indien vereist onder nationale regelgeving, evenals relevante dienstverleners, tijdig en op gepaste wijze op de hoogte worden gebracht.

Richtsnoer 25 – Uitbesteding van ICT-diensten en ICT-systemen

79. Onverminderd de Eiopa-richtsnoeren over uitbesteding aan aanbieders van clouddiensten moeten ondernemingen ervoor zorgen dat wanneer ICT-diensten en ICT-systemen worden uitbesteed, aan de relevante vereisten voor de ICT-dienst of het ICT-systeem wordt voldaan.

80. In geval van uitbesteding van kritieke of belangrijke functies moeten ondernemingen ervoor zorgen dat de contractuele verplichtingen van de dienstverrichter (zoals contract, overeenkomst inzake dienstverleningsniveau, beëindigingsbepalingen in de relevante contracten), ten minste het volgende omvatten:

    a) passende en evenredige informatiebeveiligingsdoelstellingen en -maatregelen, waaronder vereisten zoals de minimale informatiebeveiligingsvereisten, specificaties van de levenscyclus van de gegevens van ondernemingen, audit- en toegangsrechten en eventuele vereisten betreffende de locatie van datacentra en vereisten op het gebied van gegevensversleuteling, netwerkveiligheid en processen voor veiligheidsmonitoring;

    b) overeenkomsten inzake dienstverleningsniveau om de continuïteit van ICT-diensten en ICT-systemen en prestatiedoelen onder normale omstandigheden te waarborgen, evenals die welke zijn opgenomen in noodplannen in geval van dienstenonderbreking; en

    c) operationele procedures en behandelingsprocedures inzake veiligheidsincidenten inclusief escalatie en rapportage.

81. Ondernemingen moeten controleren en nagaan in welke mate deze dienstverrichters hun veiligheidsdoelstellingen, maatstaven en prestatiedoelstellingen naleven.

Regels inzake naleving en rapportage

82. Dit document bevat richtsnoeren die zijn uitgebracht op grond van artikel 16 van Verordening (EU) nr. 1094/2010. Overeenkomstig artikel 16, lid 3, van die verordening moeten de bevoegde autoriteiten en ondernemingen zich tot het uiterste inspannen om aan de richtsnoeren en aanbevelingen te voldoen.

83. Bevoegde autoriteiten die aan deze richtsnoeren voldoen of voornemens zijn deze op te volgen, moeten deze op een passende manier integreren in hun regelgevings- of toezichtskader.

84. Bevoegde autoriteiten moeten binnen twee maanden na publicatie van de vertaalde versies aan Eiopa bevestigen of zij voldoen of voornemens zijn te voldoen aan deze richtsnoeren. Indien zij er niet aan voldoen of niet voornemens zijn eraan te voldoen, moeten zij de Autoriteit daarvan in kennis stellen, met opgave van de redenen.

85. Bij uitblijven van een antwoord binnen deze termijn worden de bevoegde autoriteiten geacht niet te voldoen aan de rapportageverplichting en als zodanig gemeld.

Slotbepaling inzake herziening

86. Deze richtsnoeren kunnen door Eiopa worden herzien.