EBA/GL/2017/17

12/01/2018

Richtsnoeren

inzake beveiligingsmaatregelen voor operationele en beveiligingsrisico's van betaaldiensten uit hoofde van Richtlijn (EU) 2015/2366 (PSD2)

1. Nalevings- en rapportageverplichtingen

Status van deze richtsnoeren

1. Dit document bevat richtsnoeren die zijn uitgebracht op grond van artikel 16 van Verordening (EU) nr. 1093/2010[1]. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 moeten bevoegde autoriteiten en financiële instellingen zich tot het uiterste inspannen om aan die richtsnoeren te voldoen.

2. Richtsnoeren geven weer wat in de opvatting van de EBA passende toezichtpraktijken binnen het Europees Systeem voor financieel toezicht zijn en hoe het recht van de Unie op een specifiek gebied dient te worden toegepast. Bevoegde autoriteiten als bedoeld in artikel 4, lid 2, van Verordening (EU) nr. 1093/2010 voor wie richtsnoeren gelden, dienen hieraan te voldoen door deze op passende wijze in hun praktijken te integreren (bijvoorbeeld door hun wettelijk kader of hun toezichtprocessen aan te passen), ook wanneer richtsnoeren primair tot instellingen zijn gericht.

Kennisgevingsverplichtingen

3. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 stellen bevoegde autoriteiten EBA vóór 12.03.2018 ervan in kennis of zij aan deze richtsnoeren voldoen of voornemens zijn deze op te volgen, of, indien dit niet het geval is, wat de redenen van de niet-naleving zijn. Bevoegde autoriteiten die bij het verstrijken van de termijn niet hebben gereageerd, worden geacht niet te hebben voldaan aan de richtsnoeren. Kennisgevingen worden ingediend door het formulier op de EBA-website te versturen naar compliance@eba.europa.eu onder vermelding van "EBA/GL/2017/17". Kennisgevingen worden ingediend door personen die bevoegd zijn om namens hun bevoegde autoriteiten te melden of zij aan de richtsnoeren voldoen. Elke verandering in de status van de naleving dient eveneens aan EBA te worden gemeld.

4. Kennisgevingen worden overeenkomstig artikel 16, lid 3, van de EBA-verordening op haarwebsite bekendgemaakt.

[1] Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (PB L 331 van 15.12.2010, blz. 12).

2. Onderwerp, toepassingsgebied en definities

Onderwerp en toepassingsgebied

1. Met deze richtsnoeren vervult EBA de opdracht die haar in artikel 95, lid 3, van Verordening (EU) nr. 2015/2366 (PSD2) is gegeven[2].

2. Deze richtsnoeren leggen de vereisten vast voor de vaststelling, implementatie en monitoring van de beveiligingsmaatregelen die betalingsdienstaanbieders moeten treffen, in overeenstemming met artikel 95, lid 1 van Richtlijn (EU) 2015/2366, ter beheersing van de operationele en beveiligingsrisico's die verbonden zijn aan de door hen aangeboden betalingsdiensten.

Adressaten

3. Deze richtsnoeren zijn bedoeld voor betalingsdienstaanbieders zoals gedefinieerd in artikel 4, lid 11 van Richtlijn (EU) 2015/2366 en waarnaar verwezen wordt in de definitie van 'financiële instellingen' in artikel 4, lid 1 van Verordening (EU) 1093/2010 en voor bevoegde autoriteiten zoals gedefinieerd in punt (i) van artikel 4, lid 2 van die Verordening, in verwijzing naar de ingetrokken Richtlijn 2007/64/EG[3] (nu Richtlijn (EU) 2015/2366[4]).

Definities

4. Tenzij anders aangegeven hebben de termen die in Richtlijn (EU) 2015/2366 worden gebruikt en gedefinieerd, in deze richtsnoeren dezelfde betekenis. In deze richtsnoeren gelden bovendien de volgende definities:

[2] Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt tot wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG, 2013/36/EG en Verordening (EU) nr. 1093/2010, en tot intrekking van Richtlijn 2007/64/EG (PB L 337 van 23.12.2015, blz. 35).

[3] Richtlijn 2007/64/EG van het Europees Parlement en de Raad van 13 november 2007 betreffende betalingsdiensten in de interne markt tot wijziging van de Richtlijnen 97/7/EG, 2002/65/EG, 2005/60/EG en 2006/48/EG, en tot intrekking van Richtlijn 97/5/EG (PB L 319 van 5.12.2007, blz. 1).

[4] Overeenkomstig de tweede alinea van artikel 114 van Richtlijn (EU) 2015/2366 gelden verwijzingen naar de ingetrokken Richtlijn 2007/64/EG als verwijzingen naar Richtlijn (EU) 2015/2366 en moeten ze worden gelezen volgens de concordantietabel in bijlage II bij Richtlijn (EU) 2015/2366.

Leidinggevend orgaan	– Voor betalingsdienstaanbieders die kredietinstellingen zijn, heeft deze term dezelfde betekenis als de definitie in punt (7) van artikel 3, lid 1 van Richtlijn 2013/36/EU[5]; – Voor betalingsdienstaanbieders die betalingsinstellingen zijn of instellingen voor elektronisch geld, verwijst deze term naar de bestuurders of personen verantwoordelijk voor het bestuur van de betalingsdienstaanbieder en, waar dit relevant is, naar personen verantwoordelijk voor het beheer van de betalingsdienstactiviteiten van de betalingsdienstaanbieder; – Voor de betalingsdienstaanbieders waarnaar verwezen wordt in punt (c), (e) en (f) van artikel 1, lid 1 van Richtlijn (EU) 2015/2366, heeft deze term de betekenis die geldt in de toepasselijke nationale of EU-wetgeving.
Operationeel of veiligheidsincident	Een losse gebeurtenis of een reeks met elkaar verbonden gebeurtenissen die niet is gepland door de betalingsdienstaanbieder en die een nadelig effect heeft of waarschijnlijk zal hebben op de integriteit, beschikbaarheid, vertrouwelijkheid, authenticiteit en/of continuïteit van betalingsgerelateerde diensten.
Directie	(a) Voor betalingsdienstaanbieders die kredietinstellingen zijn, heeft deze term dezelfde betekenis als de definitie in punt (9) van artikel 3, lid 1 van Richtlijn 2013/36/EU; (b) Voor betalingsdienstaanbieders die betalingsinstellingen zijn of instellingen voor elektronisch geld, betekent deze term de natuurlijke personen die een uitvoerende bestuursfunctie uitoefenen in een instelling en die verantwoordelijk zijn voor het dagelijks bestuur van de betalingsdienstaanbieder en hierover rekenschap moeten geven aan het leidinggevend orgaan; (c) Voor de betalingsdienstaanbieders waarnaar verwezen wordt in punt (c), (e) en (f) van artikel 1, lid 1 van Richtlijn (EU) 2015/2366, heeft deze term de betekenis die geldt in de toepasselijke nationale of EU-wetgeving.
Beveiligingsrisico	Het risico dat voortvloeit uit ontoereikende of gebrekkige interne processen of externe gebeurtenissen die een ongunstig effect hebben of kunnen hebben op de beschikbaarheid, integriteit, vertrouwelijkheid van informatie- en communicatietechnologie (ICT)-systemen en/of gegevens die gebruikt worden voor het aanbieden van betaaldiensten. Dit omvat het risico van cyberaanvallen of een ontoereikende fysieke beveiliging.

[5] Richtlijn 2013/36/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende toegang tot het bedrijf van kredietinstellingen en het prudentieel toezicht op kredietinstellingen en beleggingsondernemingen, tot wijziging van Richtlijn 2002/87/EG en tot intrekking van de Richtlijnen 2006/48/EG en 2006/49/EG (PB L 176 van 27.6.2013, blz. 338).

Risicobereidheid	Het totale risiconiveau en de soorten risico's die een instelling binnen haar risicodraagkracht en overeenkomstig haar bedrijfsmodel bereid is te nemen om haar strategische doelen te bereiken.

3. Uitvoering

Toepassingsdatum

5. Deze richtsnoeren gelden vanaf 13 januari 2018.

4. Richtsnoeren

Richtsnoer 1: Algemeen beginsel

1.1 Alle betalingsdienstaanbieders dienen alle voorschriften in deze richtsnoeren in acht te nemen. De mate van gedetailleerdheid dient in verhouding te staan tot de omvang van de betalingsdienstaanbieder en tot de aard, de reikwijdte, de complexiteit en het risiconiveau van de specifieke dienst(en) die de betalingsdienstaanbieder aanbiedt of van plan is om aan te bieden.

Richtsnoer 2: Governance

Regeling ter beheersing van operationele en beveiligingsrisico's

2.1 Betalingsdienstaanbieders dienen een doeltreffend kader voor de beheersing van operationele en beveiligingsrisico's te creëren (hierna "het risicobeheersingskader"), dat minstens een keer per jaar goedgekeurd en gecontroleerd moet worden door het leidinggevend orgaan en, indien nodig, door de directie. Deze regeling dient te voorzien in beveiligingsmaatregelen om de operationele en beveiligingsrisico's te beperken en moet volledig geïntegreerd worden in de allesomvattende risicobeheersingsprocessen van de betalingsdienstaanbieder.

2.2 Dit risicobeheersingskader moet:

a) een beschrijving van het beveiligingsbeleid omvatten in de zin van artikel 5, lid 1, onder (j) van Richtlijn (EU) 2015/2366;

b) overeenstemmen met de risicobereidheid van de betalingsdienstaanbieder;

c) cruciale rollen en verantwoordelijkheden omlijnen en toekennen, evenals de desbetreffende rapporteringslijnen die nodig zijn om de toepassing van de beveiligingsmaatregelen af te dwingen en om de operationele en beveiligingsrisico's te beheersen;

d) de nodige procedures en systemen vastleggen voor het identificeren, meten, monitoren en beheersen van de risico's verbonden aan de betalingsgerelateerde activiteiten van de betalingsdienstaanbieder en waaraan de betalingsdienstaanbieder blootgesteld is, met inbegrip van maatregelen voor de bedrijfscontinuïteit.

2.3 Betalingsdienstaanbieders dienen ervoor te zorgen dat het risicobeheersingskader naar behoren gedocumenteerd is en bijgewerkt wordt op basis van 'getrokken lessen' tijdens de implementatie en monitoring.

2.4 Voorafgaand aan ingrijpende wijzigingen in de infrastructuur, processen of procedures en na elk groot operationeel of veiligheidsincident moeten betalingsdienstaanbieders nagaan of er al dan

niet onverwijld wijzigingen of verbeteringen in het risicobeheersingskader aangebracht moeten worden.

Modellen voor risicobeheersing en -controle

2.5 Betalingsdienstaanbieders dienen drie doeltreffende verdedigingslinies toe te passen, of een equivalent intern model voor risicobeheersing en -controle, om de operationele en beveiligingsrisico's te identificeren en te beheren. Betalingsdienstaanbieders dienen ervoor te zorgen dat het voornoemde interne controlemodel beschikt over de nodige autoriteit, onafhankelijkheid, middelen en directe rapporteringslijnen naar het leidinggevend orgaan, en waar nodig, de directie.

2.6 De beveiligingsmaatregelen die in deze richtsnoeren beschreven worden, dienen gecontroleerd te worden door auditors met expertise in IT-beveiliging en betalingen en die operationeel onafhankelijk zijn binnen of van de betalingsdienstaanbieder. Bij het bepalen van de frequentie en de focus van deze controles dienen de overeenkomstige beveiligingsrisico's in acht te worden genomen.

Uitbesteding

2.7 Betalingsdienstaanbieders moeten ervoor zorgen dat de doeltreffendheid van de beveiligingsmaatregelen in deze richtsnoeren gewaarborgd wordt wanneer operationele functies van betalingsdiensten, onder meer IT-systemen, uitbesteed worden.

2.8 Betalingsdienstaanbieders dienen ervoor te zorgen dat de nodige en proportionele veiligheidsdoelstellingen, maatstaven en prestatiedoelstellingen worden opgenomen in de contracten en dienstverleningsovereenkomsten met de verstrekkers van deze uitbestede diensten. Betalingsdienstaanbieders moeten controleren en nagaan in welke mate deze verstrekkers de veiligheidsdoelstellingen, maatstaven en prestatiedoelstellingen naleven.

Richtsnoer 3: Risicobeoordeling

Identificatie van functies, processen en activa

3.1 Betalingsdienstaanbieders dienen een inventarisatie te maken en deze regelmatig bij te werken van hun bedrijfsfuncties, cruciale rollen en ondersteunende processen om het belang van elke functie, rol en ondersteunend proces in kaart te brengen, evenals hun onderlinge verbondenheid betreffende de operationele en beveiligingsrisico's.

3.2 Betalingsdienstaanbieders dienen een inventarisatie te maken, en deze regelmatig bij te werken, van hun informatie-activa zoals ICT-systemen, hun configuraties, overige infrastructuuronderdelen, evenals hun onderlinge verbondenheid met andere interne en externe systemen teneinde de activa die hun kritieke bedrijfsfuncties en -processen ondersteunen te kunnen beheren.

Classificatie van functies, processen en activa

3.3 Betalingsdienstaanbieders dienen bedrijfsfuncties, ondersteunende processen en informatie-activa te classificeren naargelang hun kritieke karakter.

Risicobeoordeling van functies, processen en activa

3.4 Betalingsdienstaanbieders dienen te waarborgen dat zij voortdurend bedreigingen en kwetsbaarheden monitoren en regelmatig de risicoscenario's evalueren die een impact hebben op hun bedrijfsfuncties, kritieke processen en informatie-activa. Als onderdeel van de verplichting om de bevoegde autoriteiten een geactualiseerde en uitgebreide beoordeling te verstrekken van de operationele en beveiligingsrisico's die aan de door hen aangeboden betalingsdiensten verbonden zijn en de toereikendheid van de in reactie op deze risico's getroffen risicobeperkende maatregelen en ingevoerde controlemechanismen, zoals beschreven in artikel 95, lid 2 van Richtlijn (EU) 2015/2366, dienen betalingsdienstaanbieders risicobeoordelingen uit te voeren en te documenteren, deze minstens een keer per jaar, of met de door de bevoegde autoriteit vastgestelde kortere intervallen, van de functies, processen en informatie-activa die zij geïdentificeerd en geclassificeerd hebben om cruciale operationele en beveiligingsrisico's te identificeren en te beoordelen. Dergelijke risicobeoordelingen dienen ook te gebeuren voordat grote wijzigingen aangebracht worden in de infrastructuur, processen of procedures die de veiligheid van de betalingsdiensten beïnvloeden.

3.5 Op basis van deze risicobeoordelingen dienen betalingsdienstaanbieders te bepalen of en in welke mate er wijzigingen aangebracht moeten worden in de bestaande beveiligingsmaatregelen, de gebruikte technologieën en de procedures of aangeboden betalingsdiensten. Betalingsdienstaanbieders dienen hierbij rekening te houden met de tijd die nodig is om wijzigingen aan te brengen en de tijd die nodig is om voorlopige beveiligingsmaatregelen te treffen om operationele en veiligheidsincidenten, fraude en potentieel verstorende effecten bij de verlening van de betalingsdiensten te minimaliseren.

Richtsnoer 4: Bescherming

4.1 Betalingsdienstaanbieders dienen de nodige preventieve beveiligingsmaatregelen te nemen tegen geïdentificeerde operationele en beveiligingsrisico's. Deze maatregelen dienen een gepast veiligheidsniveau te garanderen dat in verhouding staat tot de geïdentificeerde risico's.

4.2 Betalingsdienstaanbieders dienen een diepgaande verdedigingsstrategie uit te werken en toe te passen waarbij meerdere controlelagen worden ingevoerd die werknemers, processen en technologie omspannen, en waarbij elke laag als veiligheidsnet dient voor de voorgaande laag. Onder deze diepteverdediging moet worden verstaan de toepassing van meer dan één controle voor een en hetzelfde risico, zoals bijvoorbeeld het vierogenprincipe, authenticatie met behulp van twee elementen (two-factor), netwerksegmentatie en verschillende firewalls.

4.3 Betalingsdienstaanbieders dienen de vertrouwelijkheid, integriteit en beschikbaarheid van hun kritieke digitale en fysieke activa, middelen en gevoelige betalingsgegevens van hun betalingsdienstgebruikers te verzekeren, zowel in rust-, als in overgangs- of gebruikstoestand. Indien deze gegevens ook persoonsgegevens bevatten, dienen deze maatregelen toegepast te worden in overeenstemming met Verordening (EU) 2016/679 [6] of, indien van toepassing, Verordening (EG) 45/2001.[7]

4.4 Betalingsdienstaanbieders dienen op doorlopende basis na te gaan of wijzigingen in de bestaande operationele omgeving de bestaande beveiligingsmaatregelen beïnvloeden en of er extra maatregelen genomen moeten worden om het risico in kwestie te beperken. Deze wijzigingen dienen deel uit te maken van het formele veranderingsmanagementproces ('change management') van de betalingsdienstaanbieder, die ervoor moet zorgen dat de wijzigingen naar behoren worden gepland, getest, gedocumenteerd en geautoriseerd worden. Op basis van de waargenomen dreigingen en de aangebrachte wijzigingen, moeten er tests worden uitgevoerd waarin scenario's van relevante en bekende potentiële aanvallen zijn opgenomen.

4.5 Bij het ontwerpen, ontwikkelen en aanbieden van betalingsdiensten moeten betalingsdienstaanbieders waarborgen dat functiescheiding ('segregation of duties) en 'least privilige'-principes toegepast worden. Betalingsdienstaanbieders moeten in het bijzonder aandacht besteden aan de scheiding van IT-omgevingen, vooral wat betreft de ontwikkelings-, test- en productieomgevingen.

Integriteit en vertrouwelijkheid van gegevens en systemen

4.6 Bij het ontwerpen, ontwikkelen en aanbieden van betaaldiensten, dienen betalingsdienstaanbieders ervoor te zorgen dat de verzameling, verzending, verwerking, opslag en/of archivering en weergave van gevoelige betalingsgegevens van een betalingsdienstgebruiker adequaat en relevant is en beperkt blijft tot het strikt noodzakelijke voor het aanbieden van de betaaldiensten.

4.7 Betalingsdienstaanbieders dienen regelmatig te controleren of de software die gebruikt wordt voor het aanbieden van betalingsdiensten, met inbegrip van de betalingsgerelateerde software van de gebruiker, up-to-date is en dat de kritieke beveiligingsupdates geïnstalleerd zijn. Betalingsdienstaanbieders moeten ervoor zorgen dat de nodige integriteitscontrolemechanismen aanwezig zijn om de integriteit van de software, firmware en gegevens over hun betalingsdiensten te controleren.

[6] Verordening (EU) van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, en tot intrekking van Richtlijn 95/46/EG (algemene verordening persoonsgegevens) (PB L 119 van 4.5.2016, blz. 1).
[7] Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB L 8 van 12.1.2001, blz. 1).

Fysieke beveiliging

4.8 Betalingsdienstaanbieders dienen de nodige fysieke beveiligingsmaatregelen te nemen, met name om gevoelige gegevens van betalingsdienstgebruikers te beschermen, evenals de ICT-systemen de gebruikt worden om de betalingsdiensten aan te bieden.

Toegangscontrole

4.9 De fysieke en digitale toegang tot ICT-systemen mag alleen toegestaan worden aan bevoegde personen. Autorisaties moeten verleend worden overeenkomstig de taken en verantwoordelijkheden van de medewerker, en beperkt worden tot personen die naar behoren opgeleid en gecontroleerd worden. Betalingsdienstaanbieders dienen controles in te voeren die deze toegang tot ICT-systemen op betrouwbare wijze beperken tot de personen die deze voor legitieme bedrijfsdoeleinden nodig hebben. Elektronische toegang van applicaties tot gegevens en systemen dient beperkt te worden tot het minimum dat nodig is om de desbetreffende diensten te kunnen aanbieden.

4.10 Betalingsdienstaanbieders dienen strenge controles toe te passen op de bevoorrechte toegang tot systemen door het personeel met hoge toegangsrechten strikt te beperken en nauw toezicht te houden op hen. Er dienen controles toegepast te worden zoals rolgebaseerde toegang ('roles-based'), registratie en controle van de handelingen van bevoorrechte gebruikers, een sterke authenticatieprocedure en controle op afwijkingen. Betalingsdienstaanbieders dienen toegangsrechten tot informatie-activa en hun ondersteunende systemen toe te kennen op een 'need-to-know'-basis. De toegangsrechten moeten regelmatig geëvalueerd worden.

4.11 Er dienen logbestanden bijgehouden te worden gedurende een periode die in verhouding staat tot het kritieke karakter van de geïdentificeerde bedrijfsfuncties, ondersteunende processen en informatie-activa, in overeenstemming met richtsnoer 3.1 en 3.2, onder voorbehoud van de gegevensbewaringsvereisten van de nationale en EU-wetgeving. Betalingsdienstaanbieders dienen deze gegevens te gebruiken om de identificatie en het onderzoek te vergemakkelijken van abnormale activiteiten die geconstateerd werden bij het verlenen van de betalingsdiensten.

4.12 Om een veilige communicatie te garanderen en het risico te verminderen, dient de toegang op afstand tot kritieke ICT-onderdelen alleen toegekend worden op een 'need-to-know'-basis en wanneer er sterke authenticatieoplossingen gebruikt worden.

4.13 Het gebruik van producten, tools en procedures voor toegangscontroleprocessen moet ervoor zorgen dat de toegangscontrole niet in gevaar komt of omzeild kan worden. Dit omvat het intekenen op, verstrekken, herroepen en annuleren van de overeenkomstige producten, tools en procedures.

Richtsnoer 5: Detectie

Continue monitoring en detectie

5.1 Betalingsdienstaanbieders dienen processen en middelen vast te leggen en toe te passen om de bedrijfsfuncties, de ondersteunende processen en informatie-activa voortdurend te kunnen monitoren om zo abnormale activiteiten bij het verstrekken van betalingsdiensten te detecteren. Als onderdeel van deze continue monitoring moeten betalingsdienstaanbieders beschikken over geschikte en effectieve middelen om fysieke of digitale binnendringing te detecteren, evenals inbreuken op de vertrouwelijkheid, integriteit en beschikbaarheid van informatie-activa die gebruikt worden om betalingsdiensten aan te bieden.

5.2 De continue monitoring- en detectieprocessen dienen betrekking te hebben op:

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

b) transacties teneinde misbruik van toegangsrechten door dienstverleners of andere entiteiten te detecteren; en

c) potentiële interne en externe bedreigingen.

5.3 Betalingsdienstaanbieders moeten detectiemaatregelen nemen om eventuele gegevenslekken, malware en andere bedreigingen te identificeren, evenals publiek bekende kwetsbaarheden van software en hardware, en controleren op de beschikbaarheid van overeenkomstige beveiligingsupdates .

Monitoring en verslaggeving over operationele of veiligheidsincidenten

5.4 Betalingsdienstaanbieders dienen de gepaste criteria en drempelwaarden vast te leggen om een gebeurtenis te classificeren als een operationeel of veiligheidsincident, zoals beschreven in het hoofdstuk 'Definities' van deze richtsnoeren, evenals vroegtijdige waarschuwingsindicatoren om een vroegtijdige detectie van operationele en veiligheidsincidenten mogelijk te maken.

5.5 Betalingsdienstaanbieders dienen de gepaste processen en organisatorische structuren vast te stellen om een consistente en geïntegreerde monitoring, aanpak en opvolging van operationele en veiligheidsincidenten mogelijk te maken.

5.6 Betalingsdienstaanbieders dienen een procedure vast te stellen om deze operationele en veiligheidsincidenten, evenals klachten van klanten gerelateerd aan beveiliging te rapporteren aan de directie.

Richtsnoer 6: Bedrijfscontinuïteit

6.1 Betalingsdienstaanbieders stellen een gedegen bedrijfscontinuïteitsbeheerplan op dat ervoor zorgt dat zij op permanente basis betaaldiensten kunnen aanbieden en dat verliezen door ernstige verstoringen van de bedrijfsactiviteiten worden beperkt.

6.2 Om een gedegen bedrijfscontinuïteitsbeheerplan te kunnen opstellen dienen betalingsdienstaanbieders zorgvuldig het risico te analyseren van blootstelling aan ernstige bedrijfsonderbrekingen en een beoordeling te maken van de hieruit volgende potentiële effecten (in zowel kwantitatief als kwalitatief opzicht). Daarbij worden interne en/of externe gegevens en scenario's benut. Betalingsdienstaanbieders dienen op basis van de geïdentificeerde en geclassificeerde kritieke functies, processen, systemen, transacties, en hun onderlinge verbondenheden, conform richtsnoeren 3.1 en 3.3, prioriteiten te stellen voor bedrijfscontinuïteitsmaatregelen met behulp van een risicogebaseerde benadering, die gebaseerd kan zijn op de risicobeoordeling waarnaar verwezen werd in richtsnoer 3. Afhankelijk van het bedrijfsmodel van de betalingsdienstaanbieder, kan dit er bijvoorbeeld voor zorgen dat kritieke transacties verder verwerkt kunnen worden terwijl de corrigerende maatregelen voortgezet worden.

6.3 Op basis van de analyse uit hoofde van richtsnoer 6.2 dient een betalingsdienstaanbieder te beschikken over:

a) Bedrijfscontinuïteitsplannen, zodat hij op gepaste wijze kan reageren op noodsituaties en de kritieke bedrijfsactiviteiten kan voortzetten; en

b) risicobeperkende maatregelen die getroffen moeten worden bij de stopzetting van zijn betalingsdiensten en de ontbinding van bestaande contracten, om ongunstige effecten op betaalsystemen en betalingsdienstgebruikers te vermijden en de uitvoering van nog niet volledig uitgevoerde betalingstransacties te garanderen.

Bedrijfscontinuïteitsplannen op basis van scenarioanalyses

6.4 De betalingsdienstaanbieder dient een aantal verschillende scenario's in aanmerking te nemen, inclusief extreme maar plausibele scenario's, waaraan hij blootgesteld kan zijn, en de potentiële impact van deze scenario's beoordelen.

6.5 Op basis van de analyse uitgevoerd onder richtsnoer 6.2 en de plausibele scenario's geïdentificeerd op basis van richtsnoer 6.4, dient de betalingsdienstaanbieder reactie- en herstelplannen uit te werken, die:

a) focussen op de impact op de werking van kritieke functies, processen, systemen, transacties en hun onderlinge verbondenheden;

b) gedocumenteerd en beschikbaar zijn voor de business en ondersteunende afdelingen en die gemakkelijk raadpleegbaar zijn in geval van nood; en

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

Testen van bedrijfscontinuïteitsplannen

6.6 Betalingsdienstaanbieders dienen hun bedrijfscontinuïteitsplannen te testen, en ervoor te zorgen dat de werking van hun kritieke functies, processen, systemen, transacties en hun onderlinge verbondenheden minstens een keer per jaar getest wordt. De plannen moeten doelstellingen ondersteunen om de integriteit en beschikbaarheid van hun activiteiten en de vertrouwelijkheid van hun informatie-activa te beschermen, en indien nodig, te herstellen.

6.7 De plannen moeten minstens een keer per jaar bijgewerkt worden, op basis van de testresultaten, actuele informatie over bedreigingen, gedeelde informatie en lessen die getrokken werden uit vorige gebeurtenissen, en veranderende hersteldoelstellingen, evenals de analyse van operationeel en technisch plausibele scenario's die zich nog niet voorgedaan hebben, en indien nodig, nadat systemen en processen gewijzigd werden. Betalingsdienstaanbieders dienen de relevante interne en externe belanghebbenden te consulteren en hen betrekken bij het opstellen van hun bedrijfscontinuïteitsplannen.

6.8 De tests van de bedrijfscontinuïteitsplannen door betalingsdienstaanbieders:

a) moeten een geschikt aantal scenario's omvatten, zoals vermeld in richtsnoer 6.4;

b) moeten zodanig ontworpen zijn dat ze de veronderstellingen testen waarop de bedrijfscontinuïteitsplannen berusten, met inbegrip van regelingen op het gebied van bestuur (governance) en crisiscommunicatieplannen; en

c) procedures bevatten om na te gaan of hun personeel en processen in staat zijn om correct te reageren op de bovenstaande scenario's.

6.9 Betalingsdienstaanbieders moeten regelmatig de doeltreffendheid van hun bedrijfscontinuïteitsplannen te controleren, en eventuele moeilijkheden of gebreken die uit de tests blijken analyseren en documenteren.

Crisiscommunicatie

6.10 Bij een storing of noodsituatie, en tijdens de implementatie van de bedrijfscontinuïteitsplannen, dienen betalingsdienstaanbieders ervoor te zorgen dat ze doeltreffende crisiscommunicatiemaatregelen treffen, zodat alle relevante interne en externe belanghebbenden, met inbegrip van externe dienstverleners, tijdig en op gepaste wijze op de hoogte gebracht worden.

Richtsnoer 7: Testen van beveiligingsmaatregelen

7.1 Betalingsdienstaanbieders moeten een testkader uitwerken en invoeren waarmee de robuustheid en doeltreffendheid van de beveiligingsmaatregelen gevalideerd worden en moeten ervoor zorgen dat dit testkader aangepast kan worden aan nieuwe dreigingen en kwetsbaarheden die via de risicomonitoringactiviteiten geïdentificeerd worden.

7.2 Betalingsdienstaanbieders moeten waarborgen dat tests worden uitgevoerd wanneer de infrastructuur, processen of procedures gewijzigd worden, en wanneer er wijzigingen aangebracht worden als gevolg van grote operationele en veiligheidsincidenten.

7.3 Het testkader moet ook oog hebben voor de beveiligingsmaatregelen die betrekking hebben op (i) betaalterminals en -toestellen die gebruikt worden voor het aanbieden van betalingsdiensten, (ii) betaalterminals en -toestellen die gebruikt worden om de betalingsdienstgebruiker te authenticeren en (iii) toestellen en software die door de betalingsdienstaanbieder ter beschikking gesteld worden voor de betalingsdienstgebruiker om een authenticatiecode te genereren/ontvangen.

7.4 Het testkader moet ervoor zorgen dat tests:

a) uitgevoerd worden als onderdeel van het formele veranderingsmanagementproces ('change management') van de betalingsdienstaanbieder om de robuustheid en doeltreffendheid ervan te garanderen;

b) uitgevoerd worden door onafhankelijke testers die over voldoende kennis, vaardigheden en deskundigheid beschikken wat het testen van beveiligingsmaatregelen van betalingsdiensten betreft en die niet betrokken zijn bij de ontwikkeling van de beveiligingsmaatregelen van de desbetreffende betalingsdiensten of -systemen die getest worden, tenminste voor eindtesten vooraleer de beveiligingsmaatregelen in werking treden; en

c) scans naar kwetsbaarheden en penetratietesten omvatten die overeenstemmen met het geïdentificeerde risiconiveau voor de betalingsdiensten.

7.5 Betalingsdienstaanbieders dienen doorlopend en herhaaldelijk de beveiligingsmaatregelen van hun betaaldiensten te testen. Voor systemen die als kritisch beschouwd worden voor het aanbieden van hun betaaldiensten (zoals beschreven in richtsnoer 3.2) moeten deze tests minstens een keer per jaar uitgevoerd worden. Niet-kritische systemen dienen regelmatig getest te worden op een risicogebaseerde basis, maar minstens een keer per drie jaar.

7.6 Betalingsdienstaanbieders moeten de resultaten van de uitgevoerde tests controleren en evalueren, en hun beveiligingsmaatregelen dienovereenkomstig aanpassen, en onverwijld wanneer het gaat om kritische systemen.

Richtsnoer 8: Situationeel bewustzijn en permanent leerproces

Bedreigingslandschap en situationeel bewustzijn

8.1 Betalingsdienstaanbieders dienen processen en organisatorische structuren op te stellen en toe te passen om continue operationele bedreigingen en bedreigingen voor de veiligheid die een wezenlijk effect kunnen hebben op hun vermogen om betalingsdiensten aan te bieden te identificeren en te monitoren.

8.2 Betalingsdienstaanbieders moeten de operationele en veiligheidsincidenten die geïdentificeerd zijn of die zich binnen en/of buiten de organisatie voorgedaan hebben, analyseren. Betalingsdienstaanbieders dienen belangrijke lessen te trekken uit deze analyses en op basis daarvan hun beveiligingsmaatregelen bij te werken.

8.3 Betalingsdienstaanbieders dienen de technologische ontwikkelingen actief te volgen om ervoor te zorgen dat ze zich bewust zijn van de beveiligingsrisico's.

Opleiding en programma's voor veiligheidsbewustzijn

8.4 Betalingsdienstaanbieders dienen in een opleidingsprogramma te voorzien voor alle medewerkers zodat zij opgeleid worden om de verantwoordelijkheden en verplichtingen uit te oefenen in overeenstemming met de relevante beveiligingsmaatregelen en -procedures teneinde menselijke fouten, diefstal, fraude, misbruik of verlies te verminderen. Betalingsdienstaanbieders moeten ervoor zorgen dat dit opleidingsprogramma minstens een keer per jaar voorziet in de training van de medewerkers, en vaker indien nodig.

8.5 Betalingsdienstaanbieders moeten ervoor zorgen dat de medewerkers die een cruciale rol hebben, in de zin van richtsnoer 3.1, een gerichte informatiebeveiligingsopleiding krijgen, op jaarbasis of vaker indien nodig.

8.6 Betalingsdienstaanbieders dienen regelmatige programma's voor veiligheidsbewustzijn op te stellen en uit te voeren om hun medewerkers op te leiden en te informeren over informatiebeveiligingsrisico's. Deze programma's dienen ervoor te zorgen dat medewerkers van de betalingsdienstaanbieder abnormale activiteiten en gebeurtenissen melden.

Richtsnoer 9: Relatie met de betalingsdienstgebruikers

Bewustzijn van de betalingsdienstgebruiker op het gebied van beveiligingsrisico's en risicobeperkende maatregelen

9.1 Betalingsdienstaanbieders dienen processen op te stellen en toe te passen om het bewustzijn van de betalingsdienstgebruiker te verhogen op het gebied van de beveiligingsrisico's die met de betalingsdiensten verbonden zijn door betalingsdienstgebruikers ondersteuning en richtlijnen aan te bieden.

9.2 Deze ondersteuning en richtlijnen voor de betalingsdienstgebruikers moeten bijgewerkt worden in het licht van nieuwe bedreigingen en kwetsbaarheden, en wijzigingen dienen meegedeeld te worden aan de betalingsdienstgebruikers.

9.3 Wanneer de producteigenschappen dit toelaten, dienen betalingsdienstaanbieders het voor betalingsdienstgebruikers mogelijk te maken om specifieke betaalfuncties uit te schakelen in het kader van de betalingsdiensten die door de betalingsdienstaanbieder aangeboden worden aan de betalingsdienstgebruiker.

9.4 Wanneer een betalingsdienstaanbieder overeenkomstig artikel 68, lid 1 van Richtlijn (EU) 2015/2366 ingestemd heeft met de uitgavenlimieten voor betalingstransacties die met specifieke

betaalinstrumenten worden uitgevoerd, dient de betalingsdienstaanbieder de betaler de mogelijkheid te geven om deze limieten aan te passen tot de overeengekomen maximumlimiet.

9.5 Betalingsdienstaanbieders moeten betalingsdienstgebruikers de mogelijkheid geven om waarschuwingen te ontvangen over geïnitieerde en/of mislukte pogingen om betalingstransacties te verrichten, waarmee zij frauduleus of onrechtmatig gebruik van hun rekening kunnen detecteren.

9.6 Betalingsdienstaanbieders dienen betalingsdienstgebruikers op de hoogte te houden van updates van de veiligheidsprocedures die gevolgen hebben voor de betalingsdienstgebruikers betreffende het aanbieden van de betalingsdiensten.

9.7 Betalingsdienstaanbieders moeten de betalingsdienstgebruikers helpen bij alle vragen, verzoeken om hulp en kennisgevingen van afwijkingen of problemen betreffende de beveiliging van betalingsdiensten. Betalingsdienstgebruikers moeten naar behoren geïnformeerd worden over hoe zij om hulp kunnen vragen.