EBA/GL/2017/17

12/01/2018

Riktlinjer

för säkerhetsåtgärder för operativa risker och säkerhetsrisker för betaltjänster enligt direktiv (EU) nr 2015/2366 (PSD2)

1. Efterlevnads- och rapporteringsskyldigheter

Riktlinjernas status

1. Detta dokument innehåller riktlinjer som har utfärdats enligt artikel 16 i förordning (EU) nr 1093/2010[1]. I enlighet med artikel 16.3 i förordning (EU) nr 1093/2010 måste behöriga myndigheter och finansinstituten med alla tillgängliga medel försöka följa riktlinjerna.

2. Avriktlinjerframgår Europeiska bankmyndighetens (EBA) syn på lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn eller på hur unionslagstiftningen ska tillämpas inom ett särskilt område. Behöriga myndigheter enligt definitionen i artikel 4.2 i förordning (EU) nr 1093/2010 som berörs av riktlinjerna ska följa dem genom att på lämpligt sätt införliva dem i sin praxis (till exempel genom att ändra sina rättsliga ramar eller tillsynsrutiner), även när riktlinjerna i första hand riktas till finansinstitut.

Rapporteringskrav

3. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 måste de behöriga myndigheterna meddela EBA om de följer eller avser att följa dessa riktlinjer, alternativt ange skälen till att de inte gör det, senast den 12.03.2018. Om någon sådan anmälan inte inkommer inom denna tidsfrist kommer EBA att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningar ska lämnas på det formulär som tillhandahålls på EBA:s webbplats till compliance@eba.europa.eu med hänvisningen ”EBA/GL/2017/17”. Anmälningar ska inges av personer som har befogenhet att rapportera om hur reglerna efterlevs på de behöriga myndigheternas vägnar. Alla förändringar i graden av efterlevnad måste rapporteras till EBA.

4. Anmälningarna kommer att offentliggöras på EBA:s webbplats i enlighet med artikel 16.3.

[1] Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12).

2. Syfte, tillämpningsområde och definitioner

Syfte och tillämpningsområde

5. Dessa riktlinjer härrör från EBA:s mandat enligt artikel 95.3 i förordning (EU) nr 2015/2366[2] (PSD2).

6. Dessa riktlinjer anger kraven för att fastställa, genomföra och kontrollera de säkerhetsåtgärder som betaltjänstleverantörer måste vidta i enlighet med artikel 95.1 i direktiv (EU) nr 2015/2366 för att hantera de operativa riskerna och säkerhetsriskerna förknippade med betaltjänsterna de tillhandahåller.

Adressater

7. Dessa riktlinjer riktar sig till betaltjänstleverantörer i enlighet med artikel 4.11 i direktiv (EU) nr 2015/2366 och som hänvisas till i definitionen av ”finansiella institut” i artikel 4.1 i förordning (EU) nr1093/2010 och till behöriga myndigheter i enlighet med punkt i av artikel 4.2 av nämnda förordning som hänvisat till det upphävda direktivet 2007/64/EG[3] (numera direktiv (EU) nr 2015/2366[4]).

Definitioner

8. Om inte annat anges har de termer som används och definieras i direktiv (EU) 2015/2366 samma betydelse i dessa riktlinjer. Dessutom gäller följande definitioner i dessa riktlinjer:

Ledningsorgan	– För betaltjänstleverantörer som är kreditinstitut ska denna term ha samma betydelse som definitionen i punkt 7 av artikel 3.1 i direktiv 2013/36/EU[5]. – För betaltjänstleverantörer som är betalningsinstitut eller

[2] Europaparlamentets och rådets direktiv 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden och om ändring av direktiven 2002/65/EG, 2009/110/EG, 2013/36/EG samt förordning (EU) nr 1093/2010 samt upphävande av direktiv 2007/64/EG (EUT L 337, 23.12.2015, s. 35).
[3] Europaparlamentets och rådets direktiv 2007/64/EG av den 13 november 2007 om betaltjänster på den inre marknaden och om ändring av direktiven 97/7/EG, 2002/65/EG, 2005/60/EG och 2006/48/EG samt upphävande av direktiv 97/5/EG (EUT L 319, 5.12.2007, s. 1).
[4] I enlighet med det andra understycket i artikel 114 i direktiv (EU) 2015/2366 ska alla hänvisningar till det upphävda direktivet 2007/64/EG tolkas som att de hänvisar till direktiv (EU) 2015/2366 och ska läsas i enlighet med korrelationstabellen i bilaga II i direktiv (EU) 2015/2366.
[5] Europaparlamentets och rådets direktiv 2013/36/EU om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG (EUT L 176, 27.6.2013, s. 338).

	institut för elektroniska pengar avser denna term chefer och verksamhetsansvariga för betaltjänstleverantören och, om tillämpligt, ansvariga för betaltjänstleverantörens betaltjänster. – För betaltjänstleverantörer som avses i punkt c, e och f i artikel 1.1 i direktiv (EU) 2015/2366 har denna term samma mening som i tillämpliga EU-direktiv och nationell lagstiftning.
Operativa incidenter eller säkerhetsincidenter	En enskild händelse eller en serie av sammanhängande händelser som inte har planerats av betaltjänstleverantören vilka har eller sannolikt kommer att få negativa effekter på betalningsrelaterade tjänster vad gäller integritet, tillgänglighet, konfidentialitet, autenticitet och/eller kontinuitet.
Den verkställande ledningen	(a) För betaltjänstleverantörer som är kreditinstitut ska denna term ha samma betydelse som definitionen i punkt 9 av artikel 3.1 i direktiv 2013/36/EU. (b) För betaltjänstleverantörer som är betalningsinstitut och institut för elektroniska pengar avser denna term fysiska personer med beslutsfattande roller inom institutet och som är ansvariga mot ledningsorganet för betaltjänstleverantörens dagliga drift. (c) För betaltjänstleverantörer som avses i punkt c, e och f i artikel 1.1 i direktiv (EU) 2015/2366 har denna term samma mening som i tillämpliga EU-direktiv och nationell lagstiftning.
Säkerhetsrisk	Risken för otillräckliga eller felaktiga interna processer eller externa händelser som har eller kan negativt påverka tillgängligheten, integriteten eller konfidentialiteten av alla informations- och kommunikationstekniska system (ICT) och/eller information som används för att tillhandahålla betaltjänsterna. Detta inkluderar risken för cyberattacker eller otillräcklig fysisk säkerhet.
Riskaptit	Den aggregerade risknivå och de risktyper som ett institut är villigt att ta inom ramen för sin riskkapacitet, i enlighet med sin affärsmodell, för att uppnå sina strategiska mål.

3. Genomförande

Datum för tillämpning

9. Dessa riktlinjer gäller från den 13 januari 2018.

4. Riktlinjer

Riktlinje 1: Allmänna principer

1.1 Alla betaltjänstleverantörer bör följa alla bestämmelser i dessa riktlinjer. Detaljnivån bör stå i proportion till betaltjänstleverantörens storlek samt art, omfattningen och komplexiteten hos de tjänster som betaltjänstleverantören har för avsikt att tillhandahålla och de risker dessa medför.

Riktlinje 2: Styrning

Ramverk för hantering av operativa risker och säkerhetsrisker

2.1 Betaltjänstleverantörer bör ha ett effektivt ramverk för hantering av operativa risker och säkerhetsrisker (hädanefter kallat ”riskhanteringsramverk”), vilket bör godkännas och granskas minst en gång om året av ledningen och, om tillämpligt, den verkställande ledningen. Ramverket bör fokusera på säkerhetsåtgärder för att minska operativa risker och säkerhetsrisker och bör vara helt integrerat i betaltjänstleverantörens övergripande riskhanteringsprocesser.

2.2 Riskhanteringsramverket bör

a) innehålla ett omfattande säkerhetspolicydokument i enlighet med artikel 5.1 j i direktiv (EU) 2015/2366,

b) överensstämma med betaltjänstleverantörens riskaptit,

c) definiera och tilldela nyckelroller och ansvar samt alla relevanta rapporteringslinjer som krävs för att genomföra säkerhetsåtgärderna och hantera alla säkerhetsrisker och operativa risker,

d) fastställa alla nödvändiga processer och system för att identifiera, mäta, övervaka och hantera riskerna förknippade med betaltjänstleverantörens betalningsrelaterade verksamhet och för vilka betaltjänstleverantören är utsatt, inklusive arrangemang för verksamhetens driftskontinuitet.

2.3 Betaltjänstleverantören bör säkerställa att riskhanteringsramverket är korrekt dokumenterat och uppdateras med ’lärdomar’ som erhålls under tiden det genomförs och övervakas.

2.4 Betaltjänstleverantörer bör säkerställa att de utan onödig fördröjning granskar om riskhanteringsramverket behöver ändras eller förbättras, innan en stor förändring av infrastruktur, processer eller förfaranden genomförs och efter alla större operativa incidenter eller säkerhetsincidenter som påverkar säkerheten hos deras betaltjänster.

Modeller för riskhantering och kontroller

2.5 Betaltjänstleverantörer bör inrätta tre effektiva försvarslinjer, eller liknande modell för intern riskhantering och kontroller, för att identifiera och hantera operativa risker och säkerhetsrisker. Betaltjänstleverantörerna bör säkerställa att ovannämnda interna kontrollmodeller har tillräcklig behörighet, självständighet, resurser och direkta rapporteringslinjer till ledningsorganet och, om tillämpligt, den verkställande ledningen.

2.6 Säkerhetsåtgärderna som anges i dessa riktlinjer bör granskas av revisorer med kunskap om it-säkerhet och betalningar och som är självständiga inom eller från betaltjänstleverantören. Hur ofta sådana granskningar genomförs och fokus för dem bör beakta alla motsvarande säkerhetsrisker.

Uppdragsavtal

2.7 Betaltjänstleverantörerna bör säkerställa effektiviteten av de säkerhetsåtgärder som anges i dessa riktlinjer om driften av betaltjänster, inklusive it-system, läggs ut på entreprenad.

2.8 Betaltjänstleverantörerna bör säkerställa att alla lämpliga och proportionerliga säkerhetsmål, -mått och resultatmått ingår i alla kontrakt och tjänsteavtal som ingås med leverantörerna av dessa funktioner. Betaltjänstleverantörerna bör kontrollera och erhålla intyg på sådana entreprenörers efterlevnad av sådana säkerhetsmål, -mått och -resultatmått.

Riktlinje 3: Riskbedömning

Identifiera funktioner, processer och tillgångar

3.1 Betaltjänstleverantörerna bör identifiera, fastställa och regelbundet uppdatera en lista över deras verksamhetsfunktioner, nyckelroller och stödprocesser för att kartlägga vikten av varje funktion, roll och stödprocess samt deras ömsesidiga beroenden avseende operativa risker och säkerhetsrisker.

3.2 Betaltjänstleverantörerna bör identifiera, fastställa och regelbundet uppdatera listan med informationstillgångar, såsom ICT-system, deras konfigurationer, övriga infrastrukturer och deras ömsesidiga beroende med interna och externa system för att hantera tillgångarna som stöttar deras kritiska verksamhetsfunktioner och processer.

Klassificera funktioner, processer och tillgångar

3.3 Betaltjänstleverantörerna bör klassificera de identifierade verksamhetsfunktionerna, stödprocesserna och informationstillgångarna i fråga om kritisk nivå.

Riskbedömning av funktioner, processer och tillgångar

3.4 Betaltjänstleverantörerna bör kontinuerligt övervaka hot och sårbarheter och regelbundet granska riskscenarion som kan påverka deras verksamhetsfunktioner, kritiska processer och

informationstillgångar. Som en del av sitt åtagande att hålla och tillhandahålla behöriga myndigheter med uppdaterade och omfattande riskbedömningar av operativa risker och säkerhetsrisker avseende betaltjänsterna som de erbjuder och lämpligheten av de genomförda säkerhetsåtgärderna och kontrollmekanismerna i enlighet med artikel 95.2 i direktiv (EU) 2015/2366 bör betaltjänstleverantörerna utföra och dokumentera riskbedömningar minst årligen eller mer regelbundet enligt vad den behöriga myndigheten fastställer för funktionerna, processerna och informationstillgångarna som har identifierats och klassificerats för att identifiera och bedöma stora operativa risker och säkerhetsrisker. Sådana riskbedömningar bör utföras innan större förändringar av infrastruktur, processer eller förfaranden som påverkar betaltjänsternas säkerhet.

3.5 Baserat på riskbedömningarna bör betaltjänstleverantörerna avgöra om och i vilken mån ändringar krävs av de befintliga säkerhetsåtgärderna, tekniken och procedurerna eller betaltjänsterna som erbjuds. Betaltjänstleverantörerna bör beakta tiden som krävs för att genomföra ändringarna och tiden som krävs för eventuella tillfälliga säkerhetsåtgärder som krävs för att minimera eventuella risker för operativa incidenter eller säkerhetsincidenter, bedrägerier eller störningar av tillhandahållandet av betaltjänsterna.

Riktlinje 4: Skydd

4.1 Betaltjänstleverantörerna bör ta fram och genomföra säkerhetsåtgärder mot identifierade operativa risker och säkerhetsrisker. Dessa åtgärder bör säkerställa en lämplig säkerhetsnivå i enlighet med de identifierade riskerna.

4.2 Betaltjänstleverantörerna bör ta fram och genomföra en ”defence-in-depth”-strategi som använder flera lager av kontroller för personer, processer och teknik, där varje lager fungerar som ett skyddsnät för de föregående lagren. Defence-in-depth innebär att mer än en kontroll finns för samma risk, såsom principen om ”fyra ögon”, tvåfaktorsautentisering, nätverkssegmentering och multipla brandväggar.

4.3 Betaltjänstleverantörerna bör säkerställa konfidentialiteten, integriteten och tillgängligheten av deras betaltjänstanvändarers kritiska logiska och fysiska tillgångar, resurser och känsliga betalningsuppgifter oavsett om de befinner sig i viloläge, under överföring eller i bruk. Om dessa data inkluderar personuppgifter måste sådana åtgärder genomföras i enlighet med förordning (EU) 2016/679[6] eller, om tillämpligt, förordning (EG) 45/2001.[7]

4.4 Betaltjänstleverantörerna bör kontinuerligt avgöra om förändringar av den befintliga driftmiljön påverkar befintliga säkerhetsåtgärder eller kräver att fler åtgärder genomförs för att motverka

[6] Europaparlamentets och rådets förordning (EU) av den 27 april 2016 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, och som ersätter direktiv 95/46/EG (Allmänna dataskyddsförordningen) (EGT L 119, 4.5.2016, p. 1).

[7] Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda personer med avseende på behandling av personuppgifter av gemenskapsinstitutioner och organ och om det fria flödet av sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

de aktuella riskerna. Sådana förändringar bör utgöra en del av betaltjänstleverantörernas formella ändringshanteringsprocess och säkerställa att ändringarna planeras, testas, dokumenteras och godkänns korrekt. Baserat på observerade säkerhetshot och genomförda ändringar bör tester utföras som inkluderar scenarier med relevanta eller kända potentiella attacker.

4.5 Som en del av att utforma, utveckla och tillhandahålla betaltjänster bör betaltjänstleverantörerna säkerställa att ansvarsfördelning och principen för begränsad behörighet tillämpas. Betaltjänstleverantörerna bör vara särskilt noga med uppdelningen av IT-miljöer, i synnerhet avseende utvecklings-, test- och produktionsmiljöer.

Data- och systemintegritet och -konfidentialitet

4.6 Vid utformning, utveckling och tillhandahållande av betaltjänster bör betaltjänstleverantörerna säkerställa att insamlingen, dirigeringen, behandlingen, lagringen och/eller arkiveringen samt visualiseringen av känsliga betalningsuppgifter för betaltjänstanvändaren är ändamålsenlig, relevant och begränsad till det som är nödvändigt för att tillhandahålla betaltjänsterna.

4.7 Betaltjänstleverantörerna bör regelbundet kontrollera att programvaran som används för att tillhandahålla betaltjänsterna, inklusive användarnas betalningsrelaterade programvara, är uppdaterad och att alla kritiska säkerhetsuppdateringar har installerats. Betaltjänstleverantörerna bör regelbundet kontrollera att mekanismerna för integritetskontroll fungerar för att bekräfta integriteten av programvaran, den fasta programvaran och informationen om deras betaltjänster.

Fysisk säkerhet

4.8 Betaltjänstleverantörerna bör ha lämpliga fysiska säkerhetsåtgärder, i synnerhet för att skydda betaltjänstanvändares känsliga betalningsuppgifter samt ICT-systemen som används för att tillhandahålla betaltjänster.

Åtkomstkontroll

4.9 Fysisk och logisk åtkomstkontroll bör endast vara tillgänglig för behöriga personer. Behörighet bör tilldelasutifrån personalens uppgifter och ansvar, och begränsas till personer med lämplig utbildning som står under kontroll. Betaltjänstleverantörerna bör genomföra kontroller som konsekvent begränsar åtkomsten till ICT-system till personer med legitima affärsbehov. Elektronisk åtkomst genom programvara till data och system bör hållas till det minimum som krävs för tjänsten i fråga.

4.10 Betaltjänstleverantörerna bör genomföra noggranna kontroller över privilegierad systemåtkomst genom att strikt begränsa och noga kontrollera personal med utökad systemåtkomst. Kontroller såsom rollbaserad åtkomst, inloggning och kontroll av privilegierade användares systemaktiviteter, stark autentisering och kontroll av avvikelser bör genomföras.

Betaltjänstleverantörerna bör hantera åtkomsträttigheter till informationstillgångar och deras supportsystem på en behovsenlig grund. Åtkomsträttigheter bör granskas regelbundet.

4.11 Åtkomstloggar bör lagras under en period som står i relation till den kritiska nivå de identifierade verksamhetsfunktionerna, stödprocesserna eller informationstillgångarna motsvarar, i enlighet med riktlinje 3.1 och riktlinje 3.2, dock med beaktande av lagringskraven i europeisk och nationell lagstiftning. Betaltjänstleverantörerna bör använda denna information för att identifiera och undersöka avvikande aktivitet som har upptäckts under tillhandahållandet av betaltjänsterna.

4.12 För att säkerställa säker kommunikation och förebygga risker bör fjärradministratörsåtkomst till kritiska ICT-komponenter endast ges på en behovsenlig grund och förutsatt att starka autentiseringslösningar används.

4.13 Användandet av produkter, verktyg och procedurer avseende åtkomstkontrollprocesser bör skydda åtkomstprocesserna från att kompromitteras eller kringgås. Detta inkluderar registrering, leverans, återkallning och tillbakadragande av motsvarande produkter, verktyg och procedurer.

Riktlinje 5: Detektering

Kontinuerlig övervakning och detektering

5.1 Betaltjänstleverantörerna bör ta fram och genomföra processer och funktioner för att kontinuerligt övervaka verksamhetsfunktioner, stödprocesser och informationstillgångar för att detektera avvikande aktiviteter under tillhandahållandet av betaltjänster. Som en del av denna kontinuerliga övervakning bör betaltjänstleverantörerna genomföra lämpliga och effektiva funktioner för att upptäcka fysiska och logiska intrång samt brott mot konfidentialiteten, integriteten och tillgängligheten av informationstillgångar som används för tillhandahållandet av betaltjänster.

5.2 Den kontinuerliga övervaknings- och detekteringsprocessen bör inkludera

a) relevanta interna och externa faktorer, inklusive affärs- och ICT-administreringsfunktioner,

b) transaktioner för att upptäcka åtkomstmissbruk av tjänsteleverantörer eller andra juridiska personer och

c) potentiella interna och externa hot.

5.3 Betaltjänstleverantörerna bör genomföra detekteringsåtgärder för att identifiera informationsläckage, skadlig kod och andra säkerhetshot, och allmänt kända sårbarheter för mjukvara och hårdvara, och leta efter motsvarande nya säkerhetsuppdateringar.

Övervakning och rapportering av operativa incidenter eller säkerhetsincidenter

5.4 Betaltjänstleverantörerna bör ta fram lämpliga kriterier och tröskelvärden för att klassificera händelser som operativa incidenter eller säkerhetsincidenter i enlighet med definitionerna i dessa riktlinjer, samt tidiga varningsindikatorer som kan varna betaltjänstleverantören och möjliggöra tidig upptäckt av operativa incidenter eller säkerhetsincidenter.

5.5 Betaltjänstleverantörerna bör ta fram lämpliga processer och organisationsstrukturer för att säkerställa konsekvent och integrerad övervakning, hantering och uppföljning av operativa incidenter eller säkerhetsincidenter.

5.6 Betaltjänstleverantörerna bör ta fram procedurer för att rapportera sådana operativa incidenter eller säkerhetsincidenter samt säkerhetsrelaterade kundklagomål till den verkställande ledningen.

Riktlinje 6: Driftskontinuitet

6.1 Betaltjänstleverantörerna bör inrätta en plan för god kontinuitetshantering för att maximera sin förmåga att tillhandahålla betaltjänster kontinuerligt och begränsa förlusterna vid en allvarlig störning i verksamheten.

6.2 För att ha en god kontinuitetshantering bör betaltjänstleverantören noggrant analysera sin exponering för allvarliga verksamhetsstörningar och göra (kvantitativa och kvalitativa) bedömningar av dess potentiella inverkan med hjälp av interna och/eller externa uppgifter och scenarieanalyser. Baserat på de identifierade och klassificerade kritiska funktionerna, processerna, systemen, transaktionerna och ömsesidiga beroenden i enlighet med riktlinje 3.1–3.3, bör betaltjänstleverantörerna prioritera driftskontinuitetsåtgärder med en riskbaserad metod, vilken kan baseras på riskbedömningen som utförs i enlighet med riktlinje 3. Beroende på betaltjänstleverantörens affärsmodell kan detta till exempel möjliggöra fortsatt utförande av kritiska transaktioner medan åtgärderna pågår.

6.3 Baserat på analysen enligt riktlinje 6.2 bör betaltjänstleverantören införa följande:

a) Kontinuitetsplaner som säkerställer att de kan reagera på nödfall och fortsätta kritiska affärsaktiviteter och

b) lindrande åtgärder som antas i händelse av avstängning av dess betaltjänster eller befintliga kontrakt för att undvika att de negativt påverkar betalningssystemen och betaltjänstanvändarna, och för att säkerställa att utstående betalningstransaktioner utförs.

Scenariobaserad driftskontinuitetsplanering

6.4 Betaltjänstleverantören bör beakta en rad olika scenarier, inklusive extrema men sannolika sådana för vilka den kan vara utsatt samt bedöma den potentiella effekten av sådana scenarier.

6.5 Baserat på analysen som utförs enligt riktlinje 6.2 och möjliga scenarier som identifierats enligt riktlinje 6.4 bör betaltjänstleverantören ta fram svars- och återställningsplaner som bör

a) fokusera på påverkan på kritiska funktioner, processer, system, transaktioner och ömsesidiga beroenden,

b) dokumenteras och göras tillgängliga för verksamhets- och stödenheter samt vara lätt tillgänglig i nödfall och

c) uppdateras baserat på information från tester, nya identifierade risker och hot samt ändrade återställningsmål och -prioriteter.

Test av driftskontinuitetsplaner

6.6 Betaltjänstleverantörerna bör testa sina driftkontinuitetsplaner och säkerställa att alla kritiska funktioner, processer, system, transaktioner och ömsesidiga beroenden testas minst en gång om året. Planerna bör innehålla mål för att skydda och vid behov återupprätta integriteten och tillgängligheten av deras funktion samt deras informationstillgångars konfidentialitet.

6.7 Planerna bör uppdateras minst årligen baserat på testresultaten, befintlig kunskap om aktuella hot, informationsdelning, erfarenheter från tidigare händelser och föränderliga återställningsmål, samt en analys av möjliga driftsscenarier och tekniska scenarier som ännu inte har inträffat, och om tillämpligt efter ändringar av system och processer. Betaltjänstleverantörerna bör rådgöra och koordinera med relevanta interna och externa intressenter vid upprättandet av sina kontinuitetsplaner.

6.8 Betaltjänstleverantörernas tester av sina kontinuitetsplaner bör inkludera

a) en lämplig uppsättning scenarier i enlighet med riktlinje 6.4,

b) vara utformade för att utmana förutsättningarna för kontinuitetsplanerna, inklusive styrnings- och kriskommunikationsplaner och

c) inkludera procedurer för att bekräfta personalens och processernas förmåga att korrekt bemöta ovannämnda scenarier.

6.9 Betaltjänstleverantörerna bör regelbundet kontrollera sina kontinuitetsplaners effektivitet, och dokumentera och analysera alla utmaningar eller misslyckanden som uppstår under testerna.

Kriskommunikation

6.10 I händelse av störningar eller nödfall, samt vid införandet av kontinuitetsplaner, bör betaltjänstleverantörerna säkerställa att de har effektiva kriskommunikationsåtgärder så att alla relevanta interna och externa intressenter, inklusive externa tjänsteleverantörer, informeras i tid och på ett lämpligt sätt.

Riktlinje 7: Test av säkerhetsåtgärder

7.1 Betaltjänstleverantörerna bör ta fram och genomföra ett testramverk som validerar robustheten och effektiviteten av säkerhetsåtgärderna och säkerställa att testramverket anpassas efter nya hot och sårbarheter som identifieras genom riskövervakningen.

7.2 Betaltjänstleverantörerna bör säkerställa att alla tester utförs vid ändringar av infrastruktur, processer eller förfaranden, och om ändringar görs på grund av stora operativa incidenter eller säkerhetsincidenter.

7.3 Testramverket bör också omfatta relevanta säkerhetsåtgärder för (i) betalningsterminaler och -enheter som används för att tillhandahålla betaltjänster, (ii) betalningsterminaler och -enheter som används för att autentisera betaltjänstanvändaren, och (iii) enheter och programvara som tillhandahålls av betaltjänstleverantören till betaltjänstanvändaren för att generera/ta emot autentiseringskoder.

7.4 Testramverket bör säkerställa att testerna

a) utförs som en del av betaltjänstleverantörens formella ändringshanteringsprocess för att säkerställa deras robusthet och effektivitet,

b) utförs av fristående testare med den nödvändiga kunskapen, färdigheterna och expertisen i att testa säkerhetsåtgärder för betaltjänster och som inte är involverade i utvecklingen av säkerhetsåtgärder för motsvarande betaltjänster eller betalsystem som ska testas, åtminstone för de slutliga testerna innan säkerhetsåtgärderna genomförs och

c) inkludera lämpliga sårbarhetssökningar och penetrationstester för risknivåerna identifierade för betaltjänsterna.

7.5 Betaltjänstleverantörerna bör utföra kontinuerliga och upprepade tester av säkerhetsåtgärderna för sina betaltjänster. För system som är kritiska för tillhandahållandet av betaltjänsterna (enligt riktlinje 3.2) bör dessa tester utföras minst en gång om året. Icke-kritiska system bör testas regelbundet enligt en riskbaserad metod, och minst varje tre år.

7.6 Betaltjänstleverantörerna bör övervaka och utvärdera resultaten av testerna och uppdatera sina säkerhetsåtgärder därefter och omgående för kritiska system.

Riktlinje 8: Situationsmedvetenhet och kontinuerlig inlärning

Hotlandskap och situationsmedvetenhet

8.1 Betaltjänstleverantörerna bör ta fram och genomföra processer och organisationsstrukturer för att identifiera och konstant övervaka säkerhets- och drifthot som kan påverka deras förmåga att tillhandahålla betaltjänster.

8.2 Betaltjänstleverantörerna bör analysera operativa incidenter eller säkerhetsincidenter som har identifierats eller uppstår inom och/eller utanför organisationen. Betaltjänstleverantörerna bör beakta viktig information som inhämtats från dessa analyser och uppdatera säkerhetsåtgärderna därefter.

8.3 Betaltjänstleverantörerna bör aktivt hålla sig uppdaterade med tekniska framsteg för att säkerställa att de är medvetna om alla säkerhetsrisker.

Utbildnings- och säkerhetsmedvetenhetsprogram

8.4 Betaltjänstleverantörerna bör ta fram ett utbildningsprogram för all personal för att säkerställa att de har den nödvändiga utbildningen för att utföra sina uppgifter och ansvar i enlighet med alla relevanta säkerhetspolicyer och -procedurer för att minska risken för mänskligt fel, stöld, bedrägeri, missbruk eller förlust. Betaltjänstleverantörerna bör säkerställa att deras personalutbildningsprogram hålls minst en gång om året eller oftare om det krävs.

8.5 Betaltjänstleverantörerna bör säkerställa att all personal i nyckelroller som identifierats enligt riktlinje 3.1 får årlig säkerhetsutbildning i riktad information, eller oftare om det krävs.

8.6 Betaltjänstleverantörerna bör ta fram och genomföra regelbundna säkerhetsinformationsprogram för att utbilda sin personal och bemöta informationssäkerhetsrelaterade risker. Dessa program bör kräva att betaltjänstleverantörernas personal rapporterar all ovanlig aktivitet och incidenter.

Riktlinje 9: Hantering av relationer till betaltjänstanvändare

Betaltjänstanvändarens medvetenhet om säkerhetsrisker och säkerhetsåtgärder

9.1 Betaltjänstleverantören bör ta fram och genomföra processer för att förbättra betaltjänstanvändarnas medvetenhet om säkerhetsrisker med betaltjänsterna genom att ge betaltjänstanvändarna information och vägledning.

9.2 Informationen och vägledningen till betaltjänstanvändarna bör uppdateras om nya hot och sårbarheter, och betaltjänstanvändarna måste meddelas om alla ändringar.

9.3 Om produktens funktioner tillåter bör betaltjänstleverantörerna ge betaltjänstanvändarna möjligheten att avaktivera specifika betalningsfunktioner för betaltjänsten som betaltjänstleverantören tillhandahåller betaltjänstanvändaren.

9.4 Om betaltjänstleverantören i enlighet med artikel 68.1 i direktiv (EU) 2015/2366 samtycker till betalningsgränser för betalningstransaktioner som utförs genom de specifika betalningsinstrumenten bör betaltjänstleverantören ge betalaren möjligheten att justera dessa gränser upp till den högsta överenskomna gränsen.

9.5 Betaltjänstleverantörerna bör ge betaltjänstanvändarna möjligheten att ta emot meddelanden om påbörjade och/eller misslyckade försök att utföra betalningstransaktioner för att låta dem upptäcka bedräglig eller skadlig användning av deras konto.

9.6 Betaltjänstleverantörerna bör informera betaltjänstanvändarna om uppdaterade säkerhetsprocedurer som påverkar betaltjänstanvändarens tillgång till betaltjänsterna.

9.7 Betaltjänstleverantörerna bör svara på alla betaltjänstanvändarnas frågor, begäran om hjälp eller rapporter om avvikelser eller problem avseende betaltjänsternas säkerhet. Betaltjänstanvändarna bör informeras om hur sådan hjälp kan erhållas.