EBA/GL/2017/17

12/01/2018

Retningslinjer

for sikkerhedsforanstaltninger for drifts- og sikkerhedsrisici ved betalingstjenester i henhold til direktiv (EU) 2015/2366 (PSD2)

1. Compliance- og indberetningsforpligtelser

Status for disse retningslinjer

1. Dette dokument indeholder retningslinjer, der er udstedt i henhold til artikel 16 i forordning (EU) nr. 1093/2010[1]. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder og finansielle institutioner bestræbe sig på at efterleve disse retningslinjer bedst muligt.

2. Retningslinjerne afspejler EBA's syn på passende tilsynspraksis inden for det europæiske finanstilsynssystem eller på, hvordan EU-retten bør anvendes inden for et bestemt område. De kompetente myndigheder, som er omhandlet i artikel 4, stk. 2, i forordning (EU) nr. 1093/2010, og som er omfattet af retningslinjerne, bør efterleve disse ved i fornødent omfang at indarbejde dem i deres praksis (f.eks. ved at ændre deres retlige rammer eller deres tilsynsprocesser), også hvor retningslinjerne primært er rettet mod institutioner.

Indberetningskrav

3. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder senest den 12.03.2018 underrette EBA om, hvorvidt de efterlever eller agter at efterleve disse retningslinjer, eller begrunde en eventuel manglende efterlevelse. Hvis EBA ikke er blevet underrettet inden denne dato, anser EBA de kompetente myndigheder for ikke at efterleve retningslinjerne. Underretninger fremsendes ved hjælp af det skema, der er tilgængeligt på EBA's websted, til compliance@eba.europa.eu med referencen "EBA/GL/2017/17". Underretninger fremsendes af personer med behørig beføjelse til at indberette efterlevelse på vegne af deres kompetente myndigheder. Enhver ændring af status med hensyn til efterlevelse skal også meddeles EBA.

4. Underretninger offentliggøres på EBA's websted i henhold til artikel 16, stk. 3.

[1] Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12).

2. Emne, anvendelsesområde og definitioner

Emne og anvendelsesområde

5. Disse retningslinjer er baseret på EBA's mandat i artikel 95, stk. 3, i direktiv (EU) 2015/23662 (PSD2).

6. Disse retningslinjer fastlægger krav til etablering, gennemførelse og overvågning af de sikkerhedsforanstaltninger, som betalingstjenesteudbydere bør tage i overensstemmelse med artikel 95, stk. 1, i direktiv (EU) 2015/2366 for at styre drifts- og sikkerhedsrisici i forbindelse med betalingstjenesterne de udbyder.

Adressater

7. Disse retningslinjer er rettet til betalingstjenesteudbydere som defineret i artikel 4, stk. 11, i direktiv (EU) 2015/2366 og som omhandlet i definitionen af "finansielle institutioner" i artikel 4, stk. 1, i forordning (EU) 1093/2010 og kompetente myndigheder som defineret i artikel 4, stk. 2, litra i, i samme forordning med henvisning til det ophævede direktiv 2007/64/EF[3] (i øjeblikket direktiv (EU) 2015/2366[4]).

Definitioner

8. Medmindre andet er angivet, har de udtryk, der er anvendt og defineret i direktiv (EU) 2015/2366, samme betydning i disse retningslinjer. I denne vejledning finder følgende definitioner endvidere anvendelse:

Ledelsesorgan	– For betalingstjenesteudbydere, der er kreditinstitutter, har dette begreb samme betydning som definitionen i artikel 3, stk. 1, nr. 7, i direktiv 2013/36/EU[5];

[2] Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (EFT L 337 af 23.12.2015, s. 35).

[3] Europa-Parlamentets og Rådets direktiv 2007/64/EF af 13. november 2007 om betalingstjenester i det indre marked og om ændring af direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om ophævelse af direktiv 97/5/EF (EUT L 319 af 5.12.2007, s. 1).

[4] I overensstemmelse med artikel 114, andet afsnit, i direktiv (EU) 2015/2366 gælder enhver henvisning til det ophævede direktiv 2007/64/EF som en henvisning til direktiv (EU) 2015/2366 og bør læses i overensstemmelse med sammenhængstabellen i bilag II til direktiv (EU) 2015/2366.

[5] Europa-Parlamentets og Rådets direktiv 2013/36/EU om adgang til at udøve virksomhed som kreditinstitutter og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EFT L 176 af 27.6.2013, s. 338).

	– For betalingstjenesteudbydere, der er betalingsinstitutter eller e-pengeinstitutter, refererer dette begreb til ledelsesmedlemmer eller personer, der er ansvarlige for betalingstjenesteudbyderens ledelse og, hvor det er relevant, personer, der er ansvarlige for ledelsen af betalingstjenesteudbyderens betalingstjenester; – For betalingstjenesteudbydere, der henvises til i artikel 1, stk. 1, litra c, e) og f, i direktiv (EU) 2015/2366 har dette begreb den betydning, den tillægges i henhold til gældende EU- eller national lovgivning.
Drifts- eller sikkerhedshændelse	En enkelt hændelse eller en række af forbundne hændelser, der ikke er planlagt af betalingstjenesteudbyderen, som har eller sandsynligvis vil have en negativ indvirkning på integriteten, tilgængeligheden, fortroligheden, ægtheden og/eller kontinuiteten af betalingsrelaterede tjenester.
Øverste ledelse	(a) For betalingstjenesteudbydere, der er kreditinstitutter, har denne betegnelse samme betydning som definitionen i artikel 3, stk. 1, nr. 9, i direktiv 2013/36/EU; (b) For betalingstjenesteudbydere, der er betalingsinstitutter og e-pengeinstitutter, refererer dette udtryk til fysiske personer, der udøver ledende funktioner inden for en institution, og som overfor ledelsesorganet står til ansvar for den daglige ledelse af betalingstjenesteudbyderen; (c) For betalingstjenesteudbydere, der henvises til i artikel 1, stk. 1, litra c, e) og f, i direktiv (EU) 2015/2366 har dette begreb den betydning, den tillægges i henhold til gældende EU- eller national lovgivning.
Sikkerhedsrisiko	Risikoen som følge af utilstrækkelige eller mislykkede interne processer eller eksterne hændelser, der har eller kan have en negativ indvirkning på tilgængeligheden, integriteten, eller fortroligheden af informations- og kommunikationsteknologi (IKT) systemer og/eller information, der anvendes til udbuddet af betalingstjenester. Dette omfatter risiko for cyberangreb eller utilstrækkelig fysisk sikkerhed.
Risikovillighed	Det samlede risikoniveau og de typer risici, som et institut er villigt til at påtage sig for at nå sine strategiske mål inden for rammerne af sin risikokapacitet og i overensstemmelse med sin forretningsmodel.

3. Implementering

Ikrafttrædelsesdato

9. Disse retningslinjer finder anvendelse fra den 13. januar 2018.

4. Retningslinjer

Retningslinje 1: Generelt princip

1.1 Alle betalingstjenesteudbydere bør overholde alle bestemmelserne i disse retningslinjer. Detaljeringsniveauet bør stå i forhold til betalingstjenesteudbyderens størrelse og til arten, omfanget, kompleksiteten og risikoen for de særlige tjenester, som betalingstjenesteudbyderen udbyder eller har til hensigt at udbyde.

Retningslinje 2: Ledelse

Rammer for drifts- og sikkerhedsrisikostyring

2.1 Betalingstjenesteudbydere bør etablere en effektiv ramme for drifts- og sikkerhedsrisikostyring (herefter »risikostyringsramme«), som bør godkendes og revideres mindst en gang om året af ledelsesorganet og, hvis det er relevant, af den øverste ledelse. Denne ramme bør fokusere på sikkerhedsforanstaltninger for at mindske drifts- og sikkerhedsrisici og bør integreres fuldt ud i betalingstjenesteudbyderens overordnede risikostyringsprocesser.

2.2 Risikostyringsrammen bør:

a) inkludere et omfattende dokument om sikkerhedspolitikken som omhandlet i artikel 5, stk. 1, litra j, i direktiv 2015/2366;

b) være i overensstemmelse med betalingstjenesteudbyderens risikovillighed;

c) definere og tildele nøgleroller og ansvar samt de relevante rapporteringslinjer, der er nødvendige for at håndhæve sikkerhedsforanstaltningerne og håndtere sikkerheds- og driftsrisici;

d) etablere de nødvendige procedurer og systemer til at identificere, måle, overvåge og styre de risici, der stammer fra betalingstjenesteudbyderens betalingsrelaterede aktiviteter, og som betalingstjenesteudbyderen er udsat for, herunder forretningskontinuitetsordninger.

2.3 Betalingstjenesteudbydere bør sikre, at risikostyringsrammen er korrekt dokumenteret og opdateret med dokumenterede "erfaringer" under implementeringen og overvågningen.

2.4 Betalingstjenesteudbydere bør sikre, at før en større ændring af infrastruktur, processer eller procedurer og efter enhver større -drifts- eller sikkerhedshændelse, der påvirker sikkerheden for de betalingstjenester, de udbyder, vurderer de, hvorvidt det er nødvendigt at foretageændringer eller forbedringer af risikostyringsrammen uden ugrundet ophold.

Risikostyring og kontrolmodeller

2.5 Betalingstjenesteudbydere bør etablere tre effektive forsvarslinjer eller en tilsvarende intern risikostyrings- og kontrolmodel for at identificere og styre drifts- og sikkerhedsrisici. Betalingstjenesteudbydere bør sikre, at ovennævnte interne kontrolmodel har tilstrækkelig autoritet, uafhængighed, ressourcer og direkte rapporteringslinjer til ledelsesorganet og, hvis det er relevant, til den øverste ledelse.

2.6 Sikkerhedsforanstaltningerne i disse retningslinjer bør revideres af revisorer med ekspertise inden for it-sikkerhed og betalinger og som er operationelt uafhængige inden for eller fra betalingstjenesteudbyderen. Hyppigheden af og fokuseringen på sådanne revisioner bør tage hensyn til de tilsvarende sikkerhedsrisici.

Outsourcing

2.7 Betalingstjenesteudbydere bør sikre effektiviteten af de sikkerhedsforanstaltninger, der er fastsat i disse retningslinjer, når driftsfunktioner i betalingstjenester, herunder it-systemer, outsources.

2.8 Betalingstjenesteudbydere bør sikre, at passende og forholdsmæssige sikkerhedsmål, foranstaltninger og præstationsmål er indbygget i kontrakter og serviceniveauaftaler med de udbydere, som de har outsourcet sådanne funktioner til. Betalingstjenesteudbydere bør kontrollere og anmode om bekræftelse på disse udbyderes efterlevelse af sådanne sikkerhedsmål, foranstaltninger og præstationsmål.

Retningslinje 3: Risikovurdering

Identifikation af funktioner, processer og aktiver

3.1 Betalingstjenesteudbydere bør identificere, etablere og regelmæssigt ajourføre en fortegnelse over deres forretningsfunktioner, nøgleroller og støtteprocesser for at kortlægge betydningen af hver funktion, rolle og støtteprocesser og deres indbyrdes afhængighed i forbindelse med drifts- og sikkerhedsrisici.

3.2 Betalingstjenesteudbydere bør identificere, etablere og regelmæssigt ajourføre en fortegnelse over informationsaktiverne, såsom IKT-systemer, deres konfigurationer, andre infrastrukturer og også sammenkobling med andre interne og eksterne systemer for at kunne styre de aktiver, der understøtter deres kritiske forretningsfunktioner og processer.

Klassificering af funktioner, processer og aktiver

3.3 Betalingstjenesteudbydere bør klassificere de identificerede forretningsfunktioner, understøttende processer og informationsaktiver under hensyn til vurderingen af kritisk niveau.

Risikovurderinger af funktioner, processer og aktiver

3.4 Betalingstjenesteudbydere bør sikre, at de løbende overvåger trusler og sårbarheder og regelmæssigt gennemgår risikoscenarierne, der kan påvirke deres forretningsfunktioner, kritiske processer og informationsaktiver. Som en del af forpligtelsen til at udføre og give de kompetente myndigheder en opdateret og omfattende risikovurdering af drifts- og sikkerhedsrisici i forbindelse med de betalingstjenester, de udbyder, og om tilstrækkeligheden af de begrænsende foranstaltninger og kontrolmekanismer, der er gennemført som følge af disse risici i henhold til artikel 95, stk. 2, i direktiv (EU) 2015/2366, bør betalingstjenesteudbydere udføre og dokumentere risikovurderinger mindst en gang årligt eller med kortere intervaller som fastlagt af den kompetente myndighed af de funktioner, processer og informationsaktiver, der er identificeret og klassificeret for at identificere og vurdere vigtige drifts- og sikkerhedsrisici. Sådanne risikovurderinger bør også foretages, inden der sker enhver større ændring af infrastrukturer, processer eller procedurer, der påvirker sikkerheden for betalingstjenesterne.

3.5 På baggrund af risikovurderingerne bør betalingstjenesteudbyderne afgøre, om og i hvilket omfang ændringer er nødvendige for de eksisterende sikkerhedsforanstaltninger, de anvendte teknologier og de procedurer eller betalingstjenester, der tilbydes. Betalingstjenesteudbydere bør tage højde for den tid, der kræves for at gennemføre ændringerne, og tidspunktet for at træffe passende midlertidige sikkerhedsforanstaltninger for at minimere drifts- eller sikkerhedshændelser, svig eller potentielt forstyrrende indvirkninger på betalingstjenesterne.

Retningslinje 4: Beskyttelse

4.1 Betalingstjenesteudbydere bør etablere og gennemføre forebyggende sikkerhedsforanstaltninger mod identificerede drifts- og sikkerhedsrisici. Disse foranstaltninger bør sikre et tilstrækkeligt sikkerhedsniveau i overensstemmelse med de identificerede risici.

4.2 Betalingstjenesteudbydere bør etablere og gennemføre en "forsvars-dybde" tilgang ved at indføre flerlags kontroller, der dækker mennesker, processer og teknologi, hvor hvert lag tjener som sikkerhedsnet for de foregående lag. Forsvars-dybde bør forstås som at have defineret mere end en kontrol, der dækker den samme risiko, som fx fire-øjne-princippet, to-faktorautentificering, netværkssegmentering og flere firewalls.

4.3 Betalingstjenesteudbydere bør sikre fortroligheden, integriteten og tilgængeligheden af deres kritiske logiske og fysiske aktiver, ressourcer og følsomme betalingsdata for deres betalingstjenestebrugere, uanset om de hviler, er transit eller i brug. Hvis dataene indeholder personoplysninger, bør sådanne foranstaltninger gennemføres i overensstemmelse med forordning (EU) 2016/679[6] eller, hvis det er relevant, forordning (EF) 45/2001.[7]

[6] Europa-Parlamentets og Rådets forordning (EU) af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46 / EF (generel forordning om databeskyttelse) (EFT L 119 af 4.5.2016, s. 1).

[7] Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8, 12.1.2001, s. 1).

4.4 Betalingstjenesteudbydere bør løbende fastslå, om ændringer i det eksisterende driftsmiljø påvirker de eksisterende sikkerhedsforanstaltninger eller kræver vedtagelse af yderligere foranstaltninger for at begrænse risikoen. Disse ændringer bør indgå i betalingstjenesteudbyderes formelle forandringsstyringsproces, som bør sikre, at ændringer er korrekt planlagt, testet, dokumenteret og godkendt. På baggrund af de konstaterede sikkerhedstrusler og de foretagne ændringer bør der udføres tests, som omfatter scenarier af relevante og kendte potentielle angreb.

4.5 Ved udformning, udvikling og udbud af betalingstjenester bør betalingstjenesteudbydere sikre, at principperne om adskillelse af pligter og "least privilege" anvendes. Betalingstjenesteudbydere bør være særligt opmærksomme på adskillelsen af it-miljøer, især med hensyn til udviklings-, test- og produktionsmiljøer.

Data og systemintegritet og fortrolighed

4.6 Ved udformning, udvikling og udbud af betalingstjenester bør betalingstjenesteudbydere sikre, at indsamling, routing, behandling, lagring og/eller arkivering og visualisering af følsomme betalingsdata fra betalingstjenestebrugere er tilstrækkelig, relevant og begrænset til det, der er nødvendigt for at udbyde betalingstjenesterne.

4.7 Betalingstjenesteudbydere bør regelmæssigt kontrollere, at den software, der anvendes til udbud af betalingstjenester, herunder brugerens betalingsrelaterede software, er opdateret, og at vigtige sikkerhedsrettelser implementeres. Betalingstjenesteudbydere bør sikre, at mekanismerne til integritetskontrol fungerer for at bekræfte integriteten af software, firmware og information om deres betalingstjenester.

Fysisk sikkerhed

4.8 Betalingstjenesteudbydere bør have passende fysiske sikkerhedsforanstaltninger på plads, især for at beskytte de følsomme betalingsdata for betalingstjenestebrugerne samt de IKT-systemer, der bruges til at udbyde betalingstjenester.

Adgangskontrol

4.9 Fysisk og logisk adgang til IKT-systemer bør kun tillades for bemyndigedepersoner. Bemyndigelse bør tildeles i overensstemmelse med medarbejdernes opgaver og ansvar, begrænset til personer, der er behørigt uddannet og overvåget. betalingstjenesteudbydere bør indføre kontroller, som konsekvent begrænser adgangen til IKT-systemer til dem med et legitimt forretningsbehov. Elektronisk adgang gennem applikationer til data og systemer bør begrænses til det minimum, der er nødvendigt for at udbyde den relevante tjeneste.

4.10 Betalingstjenesteudbydere bør indføre stærke kontroller over privilegeret systemadgang ved strengt at begrænse og nøje kontrollere personale med forhøjede systemadgangsrettigheder. Kontroller som rollebaseret adgang, logning og gennemgang af systemaktiviteterne hos privilegerede brugere, stærk autentifikation og overvågning af uregelmæssigheder bør

implementeres. Betalingstjenesteudbydere bør administrere adgangsrettigheder til informationsaktiver og deres understøttende systemer på et "need-to-know"-grundlag. Adgangsrettigheder bør regelmæssigt revideres.

4.11 Adgangslogs bør bevares i en periode, der modsvarer nødvendigheden af de identificerede forretningsfunktioner, støtteprocesser og informationsaktiver i overensstemmelse med retningslinje 3.1 og retningslinje 3.2, uden at dette berører opbevaringskravene i EU og national lovgivning. Betalingstjenesteudbydere bør bruge disse oplysninger til at lette identifikation og undersøgelse af uregelmæssige aktiviteter, der er blevet påvist ved udbud af betalingstjenester.

4.12 For at sikre sikker kommunikation og reducere risikoen bør fjernadgang til kritiske IKT-komponenter kun ydes på et "need-to-know"-grundlag, og når der anvendes stærke autentifikationsløsninger.

4.13 Anvendelsen af produkter, værktøjer og procedurer i forbindelse med adgangskontrolprocesser bør beskytte adgangskontrolprocesserne fra at blive kompromitteret eller omgået. Dette omfatter tilmelding, levering, tilbagekaldelse og tilbagetrækning af tilsvarende produkter, værktøjer og procedurer.

Retningslinje 5: Overvågning

Løbende overvågning

5.1 Betalingstjenesteudbydere bør etablere og gennemføreprocesser og foranstaltninger for løbende at overvåge forretningsfunktioner, understøttende processer og informationsaktiver for at opdage uregelmæssige aktiviteter i udbud af betalingstjenester. Som en del af denne løbende overvågning bør betalingstjenesteudbydere have passende og effektive foranstaltninger for at påvise fysisk eller logisk indtrængen samt krænkelser af fortrolighed, integritet og tilgængelighed af de informationsaktiver, der anvendes til udbud af betalingstjenester.

5.2 Den løbende overvågnings- og afsløringsproces bør omfatte:

a) relevante interne og eksterne faktorer, herunder forretnings- og IKT-administrationsfunktioner;

b) transaktioner med henblik på at opdage misbrug af adgang fra tjenesteudbydere eller andre enheder; og

c) potentielle interne og eksterne trusler.

5.3 Betalingstjenesteudbydere bør gennemføre påvisningsforanstaltninger for at identificere mulige informationslækager, skadelig kode og andre sikkerhedstrusler og offentligt kendte sårbarheder for software og hardware og kontrollere, om der er tilsvarende nye sikkerhedsopdateringer.

Overvågning og rapportering af drifts- eller sikkerhedhændelser

5.4 Betalingstjenesteudbydere bør fastsætte passende kriterier og tærskler for at klassificere en hændelse som en drifts- eller sikkerhedshændelse i overensstemmelse med definitionerne i disse retningslinjer, samt tidlige varslingsindikatorer, der bør fungere som en advarsel for betalingstjenesteudbyderen og muliggøre tidlig påvisning af drifts eller sikkerhedshændelser.

5.5 Betalingstjenesteudbydere bør etablere passende processer og organisationsstrukturer for at sikre en konsekvent og integreret overvågning, håndtering og opfølgning af drifts- eller sikkerhedshændelser.

5.6 Betalingstjenesteudbydere bør etablere en procedure for rapportering af sådanne drifts- eller sikkerhedshændelser samt sikkerhedsrelaterede kundeklager til dets øverste ledelse.

Retningslinje 6: Business continuity

6.1 Betalingstjenesteudbydere bør udarbejde en plan for tilstrækkelig beredskabshåndtering for at maksimere deres evne til løbende at udbyde betalingstjenester og begrænse tab i tilfælde af alvorlig forretningsforstyrrelse.

6.2 For at have en tilstrækkelig beredskabshåndtering bør betalingstjenesteudbydere omhyggeligt analysere deres eksponering for alvorlige forretningsforstyrrelser og kvantitativt og kvalitativt vurdere deres potentielle indvirkning ved hjælp af intern og/eller ekstern data- og scenarieanalyse. På baggrund af de identificerede og klassificerede kritiske funktioner, processer, systemer, transaktioner og indbyrdes afhængigheder i overensstemmelse med retningslinje 3.1 til retningslinje 3.3 bør betalingstjenesteudbydere prioritere beredskabsforanstaltninger ved hjælp af en risikobaseret tilgang, der kan baseres på de risikovurderinger, der udføres i overensstemmelse med retningslinje 3. Afhængigt af betalingstjenesteudbyderens forretningsmodel kan dette for eksempel lette videre behandling af kritiske transaktioner, mens afhjælpningsindsatsen pågår.

6.3 På grundlag af analysen udført under retningslinje 6.2 bør en betalingstjenesteudbyderhave følgende:

a) IT-beredskabsplaner der sikrer, at det kan reagere hensigtsmæssigt i nødsituationer og er i stand til at opretholde sine kritiske forretningsaktiviteter; og

b) afhjælpende foranstaltninger, der bør vedtages i tilfælde af opsigelse af betalingstjenester og opsigelse af eksisterende kontrakter, for at undgå negative virkninger på betalingssystemer og på betalingstjenestebrugere og for at sikre gennemførelsen af afventende betalingstransaktioner.

Scenariebaseret tilgang til beredskabsplanlægning

6.4 Betalingstjenesteudbydere bør overveje en række forskellige scenarier, herunder ekstreme men plausible eksempler, som det kan blive udsat for, og vurdere den potentielle indvirkning sådanne scenarier måtte have.

6.5 Baseret på analysen udført i henhold til retningslinje6.2 og sandsynlige scenarier, der er identificeret i henhold til retningslinje 6.4, bør betalingstjenesteudbyderen udvikle respons- og genopretningsplaner, som bør:

a) fokusere på virkningen på driften af kritiske funktioner, processer, systemer, transaktioner og indbyrdes afhængigheder;

b) dokumenteres og stilles til rådighed for forretnings- og supportenhederne og være let tilgængelige i nødsituationer; og

c) opdateres i overensstemmelse med erfaringerne fra testene, nye risici identificeret og trusler og ændrede genopretningsmål og -prioriteter.

Test af IT-beredskabsplaner

6.6 Betalingstjenesteudbydere bør teste deres IT-beredskabsplaner og sikre, at driften af deres kritiske funktioner, processer, systemer, transaktioner og indbyrdes afhængigheder testes mindst en gang årligt. Planerne bør støtte mål for at beskytte og om nødvendigt genoprette integriteten og tilgængeligheden af deres drift og fortroligheden af deres informationsaktiver.

6.7 Planerne bør opdateres mindst en gang årligt baseret på testresultater, aktuel trusselsinformation, informationsdeling og erfaringer fra tidligere hændelser og ændring af genopretningsmål samt analyse af driftsmæssige og teknisk set sandsynlige scenarier, der endnu ikke er indtruffet, og, hvis det er relevant, efter ændringer i systemer og processer. Betalingstjenesteudbydere bør høre og koordinere med relevante interne og eksterne interessenter under etableringen af deres IT-beredskabsplaner.

6.8 Betalingstjenesteudbyderes test af deres IT-beredskabsplaner bør:

a) inkludere et passende sæt scenarier som omtalt i retningslinje 6.4;

b) være udformet til at udfordre de antagelser, som IT-beredskabsplaner hviler på, herunder styringsordninger og krisekommunikationsplaner; og

c) omfatte procedurer for at kontrollere deres medarbejders og processers evne til at reagere tilstrækkeligt på scenarierne ovenfor.

6.9 Betalingstjenesteudbydere bør regelmæssigt overvåge effektiviteten af deres IT-beredskabsplaner , og dokumentere og analysere enhver udfordring eller fejl som følge af testene.

Krisekommunikation

6.10 I tilfælde af forstyrrelser eller nødsituationer og under gennemførelsen af IT-beredskabsplanerne bør betalingstjenesteudbydere sikre, at de har effektive krisekommunikationsforanstaltninger, således at alle relevante interne og eksterne interessenter, herunder eksterne tjenesteudbydere, informeres på en rettidig og hensigtsmæssig måde.

Retningslinje 7: Test af sikkerhedsforanstaltninger

7.1 Betalingstjenesteudbydere bør etablere og gennemføre en testramme, der bekræfter sikkerhedsforanstaltningernes robusthed og effektivitet og sikre, at testrammen er tilpasset til nye trusler og sårbarheder, der er identificeret gennem risikoovervågningsaktiviteter.

7.2 Betalingstjenesteudbydere bør sikre, at test udføres i tilfælde af ændringer i infrastruktur, processer eller procedurer, og hvis der foretages ændringer som følge af større drifts- eller sikkerhedshændelser.

7.3 Testrammerne bør også omfatte sikkerhedsforanstaltninger, der er relevante for (i) betalingsterminaler og enheder, der anvendes til udbud af betalingstjenester, (ii) betalingsterminaler og enheder, der anvendes til autentifikation af betalingstjenestebrugeren og (iii) enheder og software, som betalingstjenesteudbyderen leverer til betalingstjenestebrugeren for at generere / modtage autentifikationskoder.

7.4 Testrammen bør sikre, at test:

a) udføres som en del af betalingstjenesteudbyderens formelle forandringsstyringsproces for at sikre deres robusthed og effektivitet;

b) udføres af uafhængige testere, der har tilstrækkelig viden, færdigheder og ekspertise til at teste sikkerhedsforanstaltninger for betalingstjenester og ikke er involveret i udviklingen af sikkerhedsforanstaltningerne for de tilsvarende betalingstjenester eller systemer, der bør testes, i hvert fald for de afsluttende prøver inden der træffes sikkerhedsforanstaltninger; og

c) inkludere sårbarhedsscanning og penetrationstests, der er tilstrækkelige til det risikoniveau, der er identificeret for betalingstjenesterne.

7.5 Betalingstjenesteudbydere bør udføre løbende og gentagne test af sikkerhedsforanstaltningerne for deres betalingstjenester. For systemer, der er kritiske for udbuddet af betalingstjenesterne (som beskrevet i retningslinje 3.2), bør disse test udføres mindst på årsbasis. Ikke-kritiske systemer bør testes regelmæssigt på en risikobaseret tilgang, og mindst hvert tredje år.

7.6 Betalingstjenesteudbydere bør overvåge og evaluere resultaterne af de udførte tests og opdatere deres sikkerhedsforanstaltninger i overensstemmelse hermed og uden ugrundet ophold i tilfælde af kritiske systemer.

Retningslinje 8: Situationsbevidsthed og løbende læring

Trusselslandskab og situationsbevidsthed

8.1 Betalingstjenesteudbydere bør etablere og gennemføre processer og organisationsstrukturer for at identificere og konstant overvåge sikkerheds- og driftstrusler, som kan have væsentlig indflydelse på deres evne til at udbyde betalingstjenester.

8.2 Betalingstjenesteudbydere bør analysere drifts- eller sikkerhedshændelser, der er identificeret eller har fundet sted inden for og/eller uden for organisationen. Betalingstjenesteudbydere bør overveje vigtige erfaringer fra disse analyser og opdatere sikkerhedsforanstaltningerne i overensstemmelse hermed.

8.3 Betalingstjenesteudbydere bør aktivt overvåge den teknologiske udvikling for at sikre, at de er opmærksomme på sikkerhedsrisici.

Uddannelse og sikkerhedskendskabsprogrammer

8.4 Betalingstjenesteudbydere bør etablere et uddannelsesprogram for alt personale for at sikre, at de er uddannet til at udføre deres opgaver og ansvar i overensstemmelse med de relevante sikkerhedspolitikker og -procedurer for at reducere menneskelig fejl, tyveri, svig, misbrug eller tab. Betalingstjenesteudbydere bør sikre, at uddannelsesprogrammet sørger for uddannelse af medarbejdere mindst en gang årligt, og oftere, hvis det kræves.

8.5 Betalingstjenesteudbydere bør sikre, at medarbejdere, der besidder nøgleroller, der er identificeret under retningslinje 3.1, modtager målrettet informationssikkerhedsuddannelse på årsbasis eller oftere, hvis det kræves.

8.6 Betalingstjenesteudbydere bør etablere og gennemføre periodiske sikkerhedskendskabsprogrammer med henblik på at uddanne deres personale og løse informationssikkerhedsrelaterede risici. Disse programmer bør kræve, at betalingstjenesteudbyder-personale rapporterer om alle usædvanlige aktiviteter og hændelser.

Retningslinje 9: Håndtering af forholdet til betalingstjenestebrugere

Betalingstjenestebrugerenes bevidsthed om sikkerhedsrisici og risikobegrænsende handlinger

9.1 Betalingstjenesteudbydere bør etablere og gennemføre processer for at forbedre betalingstjenestebrugernes bevidsthed om sikkerhedsrisici i forbindelse med betalingstjenesterne ved at give betalingstjenestebrugere med hjælp og vejledning.

9.2 Hjælp og vejledning, der tilbydes til betalingstjenestebrugere, bør opdateres i lyset af nye trusler og sårbarheder, og ændringer bør meddeles betalingstjenestebrugeren.

9.3 Hvor produktfunktionalitet tillader det, bør betalingstjenesteudbydere tillade betalingstjenestebrugere at deaktivere specifikke betalingsfunktioner i forbindelse med betalingstjenesterne, som betalingstjenesteudbyderen tilbyder til betalingstjenestebrugeren.

9.4 Hvor en betalingstjenesteudbyder i overensstemmelse med artikel 68, stk. 1, i direktiv (EU) 2015/2366 med en betaler har aftalt beløbsgrænser for betalingstransaktioner gennemført via specifikke betalingsinstrumenter, bør betalingstjenesteudbyderen give betaleren mulighed for at tilpasse disse grænser op til den maksimalt aftalte grænse.

9.5 Betalingstjenesteudbydere bør give betalingstjenestebrugere mulighed for at modtage advarsler om initierede og/eller mislykkede forsøg på at initiere betalingstransaktioner, så de kan opdage svigagtig eller skadelig brug af deres konto.

9.6 Betalingstjenesteudbydere bør holde betalingstjenestebrugere underrettet om opdateringer i sikkerhedsprocedurer, der påvirker betalingstjenestebrugere vedrørende udbud af betalingstjenester.

9.7 Betalingstjenesteudbydere bør levere betalingstjenestebrugere hjælp til alle spørgsmål, anmodninger om support og meddelelser om uregelmæssigheder eller spørgsmål vedrørende sikkerhedsforhold i forbindelse med betalingstjenester. Betalingstjenestebrugere bør være behørigt informeret om, hvordan sådan bistand kan opnås.