EBA/GL/2014/12_Rev1

19. december 2014

Endelige retningslinjer

vedrørende sikkerheden ved internetbetalinger

Indhold

Retningslinjer vedrørende sikkerheden ved internetbetalinger

Status for disse retningslinjer

Dette dokument indeholder retningslinjer, der er udstedt i medfør af artikel 16 i 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 2009/77/EF ("EBA-forordningen"). I henhold til artikel 16, stk. 3, i EBA-forordningen skal de kompetente myndigheder og finansielle institutioner bestræbe sig på at efterleve retningslinjerne mest muligt.

Retningslinjerne fastlægger EBA's syn på hensigtsmæssig tilsynspraksis inden for Det Europæiske Finanstilsynssystem, eller hvordan EU-lovgivningen bør anvendes på et bestemt område. EBA forventer derfor, at alle kompetente myndigheder og finansieringsinstitutter, som retningslinjer er rettet til, efterlever dem. Kompetente myndigheder, som er omfattet af retningslinjer, bør efterleve disse ved at indarbejde dem i deres tilsynspraksis på passende vis (f.eks. ved at ændre deres retlige rammer eller tilsynsprocesser), herunder hvor retningslinjer er rettet direkte til institutter.

Indberetningspligt

Ifølge artikel 16, stk. 3, i EBA-forordningen skal kompetente myndigheder inden den 5. maj 2015 meddele EBA, om de efterlever eller agter at efterleve disse retningslinjer eller i modsat fald angive begrundelsen herfor. Meddeles dette ikke EBA inden for den angivne frist, anser EBA de kompetente myndigheder for ikke at efterleve retningslinjerne. Meddelelser bør indsendes på formularen i afsnit 5 til compliance@eba.europa.eu med angivelse af henvisningen "EBA/GL/2014/12". Meddelelser bør indsendes af personer med bemyndigelse til at indgive meddelelse om efterlevelse på vegne af de pågældende kompetente myndigheder.

Meddelelser offentliggøres på EBA's websted i overensstemmelse med artikel 16, stk. 3.

Afsnit I – Anvendelsesområde og definitioner

Anvendelsesområde

1. Disse retningslinjer fastlægger en række mindstekrav vedrørende sikkerheden ved internetbetalinger. Retningslinjerne er udarbejdet på baggrund af reglerne i direktiv 2007/64/EF [1] ("betalingstjenestedirektivet") vedrørende informationskrav for betalingstjenester og betalingstjenesteudbyderes forpligtelser i forbindelse med levering af betalingstjenester. Endvidere skal betalingsinstitutter ifølge artikel 10, stk. 4, i direktivet have indført robust og tilstrækkelig governance og tilstrækkelige interne kontrolmekanismer.

2. Retningslinjerne gælder for betalingstjenester, der udbydes af betalingstjenesteudbyderne via internettet som defineret i artikel 1 i direktivet.

3. Retningslinjerne er rettet mod finansielle institutter som defineret i artikel 4, stk. 1, i forordning (EU) nr. 1093/2010 og mod de kompetente myndigheder som defineret i artikel 4, stk. 2, i forordning (EU) nr. 1093/2010. De kompetente myndigheder i de 28 medlemslande i EU bør sikre, at disse retningslinjer følges af betalingstjenesteudbydere som defineret i artikel 1 i betalingstjenestedirektivet under deres tilsyn.

4. De kompetente myndigheder kan desuden beslutte, at betalingstjenesteudbydere skal indberette til de kompetente myndigheder, at de overholder retningslinjerne.

5. Disse retningslinjer har ikke indflydelse på gyldigheden af den Europæiske Centralbanks "Anbefalinger vedrørende sikkerheden ved internetbetalinger" ("Rapporten").[2] Rapporten er fortsat det dokument, som centralbankerne bør bruge i deres overvågningsfunktion af betalingssystemer og -instrumenter, når de skal foretage en vurdering af compliance med hensyn til sikkerheden ved internetbetalinger.

6. Retningslinjerne udgør minimumsforventningerne. De finder anvendelse med forbehold for det ansvar, som betalingstjenesteudbyderne har for at overvåge og vurdere de risici, der er forbundet med deres forretning, udvikle deres egne detaljerede sikkerhedspolitikker og gennemføre tilstrækkelige foranstaltninger med hensyn til sikkerhed, beredskab, styring af hændelser og forretningsvidereførelse, som står mål med de risici, der er forbundet med de udbudte betalingstjenester.

7. Formålet med retningslinjerne er at definere fælles mindstekrav til de nedenfor nævnte internetbetalingstjenester, uanset hvilken enhed der anvendes til at opnå adgang til internettet:

[1] 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).

[2] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

- [kort] gennemførelse af kortbetalinger på internettet, herunder betalinger med virtuelle kort, samt registrering af kortdata til anvendelse i "digitale tegnebøger"

- [kontooverførsler] gennemførelse af kontooverførsler på internettet

- [e-mandat] udstedelse og ændring af elektroniske mandater til direkte debitering

- [e-penge] overførsler af elektroniske penge mellem to e-pengekonti via internettet.

8. Hvor formålet med retningslinjerne er at opnå et bestemt resultat, kan dette også opnås ved en anden metode, end den i retningslinjerne angivne. Ud over de følgende retningslinjer indeholder dette dokument også eksempler på bedste praksis (i bilag 1), som der tilskyndes til, men ikke kræves, at betalingstjenesteudbyderne følger.

9. Hvis betalingstjenesterne eller -instrumenterne udbydes gennem et betalings-scheme (f.eks. scheme for kortbetalinger, kontooverførsler, direkte debiteringer osv.), bør de kompetente myndigheder og de relevante centralbanker, som har en overvågningsfunktion af betalingsinstrumenter, koordinere tilsynet og overvågningen med henblik på at sikre, at de involverede aktører anvender retningslinjerne på en ensartet måde.

10. Betalingsintegratorer[3], der udbyder betalingsinitieringstjenester, betragtes som enten indløsere af internetbetalingstjenester (og således som betalingstjenesteudbydere) eller som udbydere af eksterne tekniske tjenester i forbindelse med de pågældende løsninger eller betalingstjenesteudbydere. I sidstnævnte tilfælde bør betalingsintegratorerne kontraktuelt forpligtes til at overholde retningslinjerne.

11. Følgende er ikke omfattet af retningslinjernes anvendelsesområde:

- andre internettjenester udbudt af en betalingstjenesteudbyder via sit betalingswebsted (f.eks. elektronisk mægling, onlinekontrakter)

- betalinger, hvor anvisningen gives pr. post, telefon, talemeddelelse eller SMS-baseret teknologi

- andre mobilbetalinger end browserbaserede betalinger

- kontooverførsel, hvor en tredjepart tilgår kundens betalingskonto

- betalingstransaktioner foretaget af en virksomhed via dedikerede netværk

[3] Betalingsintegratorer stiller en standardiseret grænseflade til rådighed for betalingsmodtageren (dvs. e-handelsforretningen) til betalingsinitieringstjenester udbudt af betalingstjenesteudbydere.

- kortbetalinger ved hjælp af anonyme fysiske eller virtuelle forudbetalte kort, som ikke kan genoptankes, og hvor der ikke er noget fast forhold mellem udstederen og kortholderen

- clearing og afvikling af betalingstransaktioner.

Definitioner

12. For så vidt angår disse retningslinjer, og i tillæg til definitionerne i betalingstjenestedirektivet, gælder følgende definitioner:

- *autentificering:* en procedure, der gør det muligt for betalingstjenesteudbyderen at bekræfte en kundes identitet

- *stærk kundeautentificering:* i denne sammenhæng en procedure baseret på anvendelse af to eller flere af følgende elementer – kategoriseret som viden, ejerskab og iboende egenskab: i) noget, som kun brugeren kender, f.eks. en statisk adgangskode, en kode eller et personligt identifikationsnummer, ii) noget, som kun brugeren er i besiddelse af, f.eks. en token, et smartkort eller en mobiltelefon, iii) noget, som kendetegner brugeren, f.eks. et biometrisk kendetegn, såsom fingeraftryk. De udvalgte elementer skal desuden være indbyrdes uafhængige, dvs. at et brud på et af dem ikke svækker de andre/det andet. Mindst ét af elementerne bør ikke kunne genanvendes eller kopieres (undtagen hvad angår iboende egenskaber) og må ikke kunne stjæles uopdaget via internettet. Den stærke autentificeringsprocedure bør være udformet således, at den beskytter fortroligheden af autentificeringsdataene

- *autorisation:* en procedure, hvor det kontrolleres, om en kunde eller betalingstjenesteudbyder har ret til at udføre en bestemt handling, f.eks. retten til at overføre penge eller retten til at opnå adgang til følsomme data

- *brugeroplysninger:* de – generelt fortrolige – oplysninger, som en kunde eller betalingstjenesteudbyder giver i forbindelse med autentificering. Brugeroplysninger kan også betyde besiddelse af en fysisk enhed, der indeholder oplysningerne (f.eks. engangsadgangskodegenerator, smartkort), eller noget, brugeren har lært udenad eller repræsenterer (såsom biometriske kendetegn)

- *større sikkerhedshændelse:* en hændelse, som i væsentlig grad påvirker eller kan påvirke sikkerheden, integriteten eller kontinuiteten for betalingstjenesteudbyderens systemer og/eller sikkerheden ved følsomme betalingsdata eller midler. Ved vurderingen af væsentlighed bør antallet af potentielt berørte kunder, risiko for tab og indvirkningen på andre betalingstjenesteudbydere eller betalingsinfrastrukturer tages med i betragtning

- *transaktionsrisikoanalyse:* evaluering af den risiko, der er forbundet med en bestemt transaktion, hvor der tages højde for kriterier som for eksempel kundebetalingsmønstre (adfærd), værdien af den relaterede transaktion, produkttype og modtagerprofil

- *virtuelle kort*: en kortbaseret betalingsløsning, der kan anvendes til internetkøb, hvor der genereres et alternativt, midlertidigt kortnummer med en reduceret gyldighedsperiode, begrænset brug og en foruddefineret hævegrænse

- *digitale tegnebøger ("wallet"):* løsninger, der giver en kunde mulighed for at registrere data vedrørende ét eller flere betalingsinstrumenter med henblik på at foretage betalinger til flere forskellige e-handelsforretninger.

Afsnit II – Retningslinjer vedrørende sikkerheden ved internetbetalinger

Generelt kontrol- og sikkerhedsmiljø

Ledelse

1. Betalingstjenesteudbydere bør gennemføre og regelmæssigt revurdere en formel sikkerhedspolitik for internetbetalingstjenester.

   1.1 Sikkerhedspolitikken bør være veldokumenteret og bør revurderes regelmæssigt (i overensstemmelse med retningslinje 2.4) og godkendes af den øverste ledelse. Den bør definere betalingstjenesteudbyderens sikkerhedsmål og risikovillighed.

   1.2 Sikkerhedspolitikken bør definere roller og ansvar, herunder risikostyringsfunktionen med direkte rapporteringslinje til bestyrelsesniveau og rapporteringslinjerne for de udbudte internetbetalingstjenester, herunder håndtering af følsomme betalingsdata med hensyn til vurdering, styring og reduktion af risici.

Risikovurdering

2. Betalingstjenesteudbydere bør foretage og dokumentere grundige risikovurderinger med hensyn til sikkerheden ved internetbetalinger og relaterede tjenester, både inden tjenesten/tjenesterne etableres og regelmæssigt derefter.

   2.1 Betalingstjenesteudbydere bør gennem deres risikostyringsfunktion foretage og dokumentere detaljerede risikovurderinger for internetbetalinger og relaterede tjenester. Betalingstjenesteudbydere bør tage resultaterne af den løbende overvågning af sikkerhedstrusler vedrørende de internetbetalingstjenester, de udbyder eller har til hensigt at udbyde, med i betragtning, herunder i) de teknologiske løsninger, de anvender, ii) tjenester, der outsources til eksterne leverandører, og iii) kundernes it-miljø. Betalingstjenesteudbydere bør tage de risici, der er forbundet med de anvendte platforme, applikationsarkitekturer, programmeringsteknikker og -rutiner, både deres egne [4] og kundernes, [5] samt resultaterne af processen for sikkerhedshændelsesovervågning med i betragtning (se retningslinje 3).

   2.2 På den baggrund bør betalingstjenesteudbydere afgøre, om og i hvilket omfang det kan være nødvendigt at foretage ændringer i de eksisterende sikkerhedsforanstaltninger, de anvendte teknologier og procedurer eller de udbudte tjenester. Betalingsudbyderne bør tage højde for den tid, det kræver at gennemføre

[4] Såsom systemets følsomhed over for hijacking i betalingssessioner, SQL injection, cross-site scripting, buffer overflows osv.

[5] Såsom risici forbundet med anvendelse af multimedieapplikationer, browser plug-ins, frames, eksterne links osv.

ændringerne (herunder udrulning hos kunderne), og træffe passende midlertidige foranstaltninger til at minimere sikkerhedshændelser og svindel samt potentielle forstyrrende virkninger.

2.3 Vurderingen af risici bør omfatte en vurdering af behovet for at beskytte og sikre følsomme betalingsdata.

2.4 Betalingstjenesteudbydere bør foretage en undersøgelse af risikoscenarierne og de eksisterende sikkerhedsforanstaltninger efter større hændelser, der påvirker deres tjenester, inden der foretages væsentlige ændringer i infrastrukturen eller procedurerne, og når der identificeres nye trusler gennem risikoovervågningsaktiviteter. Der bør desuden foretages en revurdering af risikovurderingen én gang om året. Resultaterne af risikovurderingerne og revurderingen af denne bør forelægges den øverste ledelse med henblik på godkendelse.

Overvågning og indberetning af hændelser

3. Betalingstjenesteudbydere bør sikre en ensartet og integreret overvågning, håndtering af og opfølgning på sikkerhedshændelser, herunder sikkerhedsrelaterede kundeklager. Betalingstjenesteudbydere bør fastlægge en procedure for indberetning af sådanne hændelser til ledelsen og ved større betalingssikkerhedshændelser også til de kompetente myndigheder.

3.1 Betalingstjenesteudbydere bør have etableret en proces til overvågning, håndtering af og opfølgning på sikkerhedshændelser og sikkerhedsrelaterede kundeklager og indberette sådanne hændelser til ledelsen.

3.2 Betalingstjenesteudbydere bør have en procedure for øjeblikkelig underretning af de kompetente myndigheder (dvs. tilsyns- og databeskyttelsesmyndigheder), i det omfang de findes, i tilfælde af større betalingssikkerhedshændelser i forbindelse med de udbudte betalingstjenester.

3.3 Betalingstjenesteudbydere bør have en procedure for samarbejde om større betalingssikkerhedshændelser, herunder datalæk, med de relevante kompetente myndigheder.

3.4 Betalingsindløsere bør ved aftale kræve, at e-handelsforretninger, som lagrer, behandler eller overfører følsomme betalingsdata, samarbejder om større betalingssikkerhedshændelser, herunder datalæk, både med dem og de relevante kompetente myndigheder. Hvis en betalingstjenesteudbyder bliver vidende om, at en e-handelsforretning ikke samarbejder i overensstemmelse med aftalen, bør udbyderen tage skridt til at håndhæve denne aftalemæssige forpligtelse eller opsige aftalen.

Risikostyring og -reduktion

4. Betalingstjenesteudbydere bør træffe sikkerhedsforanstaltninger i overensstemmelse med deres respektive sikkerhedspolitikker med henblik på at reducere identificerede risici. Disse foranstaltninger bør inkorporere flere lag af sikkerhedsforsvar, hvor et svigt i én af forsvarslinjerne opfanges af den næste forsvarslinje.

4.1 Ved udformning, udvikling og vedligeholdelse af internetbetalingstjenester bør betalingstjenesteudbydere særligt sørge for en passende funktionsadskillelse i IT-miljøer (f.eks. udviklings-, test- og produktionsmiljøer) og gennemførelse af "least privilege"-princippet som grundlag for en sikker styring af identitet og adgang.[6]

4.2 Betalingstjenesteudbydere bør have etableret passende sikkerhedsløsninger til beskyttelse af netværk, websteder, servere og kommunikationsforbindelser mod misbrug eller angreb. Betalingstjenesteudbydere bør fjerne alle overflødige funktioner fra serverne med henblik på at beskytte (hærde) dem og fjerne eller reducere sårbarheder i applikationer. De forskellige applikationers adgang til data og ressourcer bør holdes på et absolut minimum i henhold til "least privilege"-princippet. Med henblik på at begrænse anvendelsen af "falske" websteder (der foregiver at være ægte betalingstjenesteudbyder) bør transaktionswebsteder, der udbyder internetbetalingstjenester, identificeres ved hjælp af udvidede valideringscertifikater, i betalingstjenesteudbyderens navn, eller ved hjælp af andre lignende autentificeringsmetoder.

4.3 Betalingstjenesteudbydere bør have indført passende processer til overvågning, sporing og begrænsning af adgangen til i) følsomme betalingsdata og ii) logiske og fysiske kritiske ressourcer, såsom netværk, systemer, databaser, sikkerhedsmoduler osv. Betalingstjenesteudbydere bør oprette, lagre og analysere passende logs og transaktionsspor.

4.4 Ved udformning,[7] udvikling og vedligeholdelse af internetbetalingstjenester bør betalingstjenesteudbydere sikre, at "data minimering[8]" er en væsentlig komponent i kernefunktionaliteten: Indsamling, routing, behandling, lagring og/eller arkivering og visning af følsomme betalingsdata bør holdes på et absolut minimum.

4.5 Sikkerhedsforanstaltninger vedrørende internetbetalingstjenester bør testes af risikostyringsfunktionen med henblik på at sikre foranstaltningernes robusthed og effektivitet. Alle ændringer bør gennemgå en formel ændringsstyringsproces, der sikrer, at ændringer er ordentligt planlagt, testet, dokumenteret og autoriseret. På

[6] "Ethvert program og enhver privilegeret bruger af systemet bør anvende det mindst mulige antal rettigheder, der er nødvendig for at udføre opgaven." Se Saltzer, J.H. (1974), "Protection and the Control of Information Sharing in Multics", Communications of the ACM, bind 17, nr. 7, s. 388.

[7] Privacy by design (PbD).

[8] Ved dataminimering forstås politikken om at indsamle den mindst mulige mængde personlige oplysninger, der er nødvendig for at udføre en given funktion.

baggrund af de gennemførte ændringer og de konstaterede sikkerhedstrusler bør testene gentages regelmæssigt og omfatte scenarier med relevante og kendte potentielle angreb.

4.6 Betalingstjenesteudbyderens sikkerhedsforanstaltninger vedrørende internetbetalingstjenester bør revideres med regelmæssige mellemrum med henblik på at sikre foranstaltningernes robusthed og effektivitet. Internetbetalingstjenesternes gennemførelse og virkeevne bør også revideres. Hyppigheden af og formålet med sådanne revisioner bør fastlægges under hensyntagen til de forbundne risici og bør stå i forhold til disse. Revisionerne bør udføres af pålidelige og uafhængige (interne eller eksterne) eksperter. De bør ikke på nogen måder være involveret i udviklingen, gennemførelsen eller den driftsmæssige styring af de udbudte betalingstjenester.

4.7 Når betalingstjenesteudbydere outsourcer funktioner, der er forbundet med sikkerheden ved internetbetalingstjenester, bør aftalen indeholde bestemmelser om efterlevelse af de principper og retningslinjer, der er fastlagt i dette dokument.

4.8 Betalingsindløsere, bør ved aftale kræve, at e-handelsforretninger der håndterer (dvs. lagrer, behandler eller overfører) følsomme betalingsdata, indfører sikkerhedsforanstaltninger i deres it-infrastruktur i overensstemmelse med retningslinje 4.1 til 4.7 med henblik på at undgå tyveri af disse følsomme betalingsdata via deres systemer. Hvis en betalingstjenesteudbyder bliver vidende om, at en e-handler ikke har indført de nødvendige sikkerhedsforanstaltninger, bør udbyderen tage skridt til at håndhæve denne aftalemæssige forpligtelse eller opsige aftalen.

Sporbarhed

5. Betalingstjenesteudbydere bør have indført processer, der sikrer, at alle transaktioner, herunder e-mandater, spores korrekt.

5.1 Betalingstjenesteudbydere bør sikre, at deres tjeneste indeholder sikkerhedsmekanismer til detaljeret registrering af data vedrørende transaktioner og e-mandater, herunder transaktionens sekvensnummer, tidsstempler, ændringer i parameteriseringen samt registrering af adgang til transaktions- og e-mandatdata.

5.2 Betalingstjenesteudbydere bør implementere logfiler, der gør det muligt at spore enhver tilføjelse, ændring eller sletning af transaktions- og e-mandatdata.

5.3 Betalingstjenesteudbydere bør evaluere og analysere e-mandater og transaktionsdataene og sikre, at de har værktøjer til at evaluere logfilerne. De respektive værktøjer bør kun være tilgængelige for autoriseret personale.

Specifikke kontrol- og sikkerhedsforanstaltninger vedrørende internetbetalinger

Indledende identificering af kunder, oplysninger

6. Kunder bør identificeres korrekt i overensstemmelse med EU's lovgivning om forebyggelse af hvidvask[9] og bekræfte deres intention om at foretage en internetbetaling ved at bruge tjenesten, før de gives adgang til denne. Betalingstjenesteudbydere bør "på forhånd", "regelmæssigt" eller, i det omfang det er relevant, "ad hoc" give kunden tilstrækkelige informationer om de nødvendige krav (f.eks. udstyr, procedurer) til gennemførelse af sikre internetbetalinger og om risikoen forbundet dermed.

6.1 Betalingstjenesteudbydere bør sikre, at kunden har været underkastet procedurerne med hensyn til kundelegitimation og har forelagt tilstrækkelige identitetsdokumenter[10] og relaterede oplysninger, før kunden gives adgang til internetbetalingstjenesterne.[11]

6.2 Betalingstjenesteudbydere bør sikre, at de informationer[12], der gives til kunden på forhånd, indeholder specifikke detaljer vedrørende internetbetalingstjenesterne. Disse bør afhængigt af omstændighederne omfatte:

- tydelige informationer om krav vedrørende kundeudstyr, software eller andre nødvendige værktøjer (f.eks. antivirussoftware, firewalls)
- retningslinjer for korrekt og sikker anvendelse af personlige sikkerhedsoplysninger (personalised security credentials)
- en trinvis beskrivelse af den procedure, der gælder for en kundes udførelse og autorisation af en betalingstransaktion og/eller indhentning af oplysninger, herunder konsekvenserne af hver handling
- retningslinjer for korrekt og sikker anvendelse af al hardware og software, der stilles til rådighed for kunden
- de procedurer, der skal følges i tilfælde af tab eller tyveri af de personlige sikkerhedsoplysninger (personalised security credentials) eller kundens hardware eller software, der anvendes til at logge ind eller udføre transaktioner

[9] For eksempel Europa-Parlaments og Rådets direktiv 2005/60/EF af 26. oktober 2005 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvaskning af penge og finansiering af terrorisme. EUT L 309 af 25.11.2005, s. 15-36. Se også Kommissionens direktiv 2006/70/EF af 1. august 2006 om fastsættelse af gennemførelsesforanstaltninger for Europa-Parlamentets og Rådets direktiv 2005/60/EF, for så vidt angår definitionen af "politisk udsat person" og for lempede procedurer med hensyn til kundelegitimation og for undtagelse i tilfælde, hvor en finansiel aktivitet udøves lejlighedsvis eller i et meget begrænset omfang. EUT L 214 af 4.8.2006, s. 29-34.

[10] For eksempel pas, nationalt identitetskort eller avanceret elektronisk underskrift.

[11] Kundeidentifikationsprocessen gælder med forbehold af eventuelle undtagelser i eksisterende lovgivning om forebyggelse af hvidvask. Betalingstjenesteudbydere behøver ikke at udføre en særskilt kundeidentifikationsproces for internetbetalingstjenesterne, forudsat at en sådan kundeidentifikation allerede er udført, f.eks. for andre eksisterende betalingsrelaterede tjenester eller for åbning af en konto.

[12] Disse informationer supplerer artikel 42 i betalingstjenestedirektivet, der fastlægger de oplysninger, som betalingstjenesteudbyderen skal give betalingstjenestebrugeren, inden der indgås aftale om udbud af betalingstjenester.

- de procedurer, der skal følges, hvis der konstateres eller opstår mistanke om misbrug

- en beskrivelse af betalingstjenesteudbyderens og kundens ansvar og forpligtelser med hensyn til anvendelsen af internetbetalingstjenesten.

6.3 Betalingstjenesteudbydere bør sikre, at det i rammeaftalen med kunden er fastlagt, at betalingstjenesteudbyderen af sikkerhedshensyn kan blokere en specifik transaktion eller betalingsinstrumentet[13]. Aftalen bør fastlægge metoden til og vilkårene for underretning af kunden, og hvordan kunden kan kontakte betalingstjenesteudbyderen med henblik på at ophæve blokeringen af internetbetalingstransaktionen eller tjenesten i overensstemmelse med betalingstjenestedirektivet.

[13] Se artikel 55 i betalingstjenestedirektivet om grænser for brugen af betalingsinstrumentet.

Stærk kundeautentificering

7. Initieringen af internetbetalinger og adgang til følsomme betalingsdata bør beskyttes af stærk kundeautentificering. Betalingstjenesteudbydere bør have en procedure for stærk kundeautentificering, som er i overensstemmelse med den definition, der er angivet i disse retningslinjer.

7.1 [kontooverførsler/e-mandat/e-penge] Betalingstjenesteudbydere bør udføre stærk kundeautentificering for kundens autorisation af internetbetalingstransaktioner (herunder bundtede kontooverførsler) og for udstedelse eller ændring af mandater til direkte debitering. Betalingstjenesteudbydere bør imidlertid overveje at indføre alternative kundeautentificeringsmetoder for:

- udgående betalinger til pålidelige modtagere, der er anført på en tidligere oprettet hvidliste for den pågældende kunde
- transaktioner mellem to af den samme kundes konti hos samme betalingstjenesteudbyder
- overførsler inden for samme betalingstjenesteudbyder begrundet i en transaktionsrisikoanalyse
- betalinger af små beløb (mikrobetalingsinstrumenter), som nævnt i betalingstjenestedirektivet.[14]

7.2 Adgang til eller ændring af følsomme betalingsdata (herunder oprettelse og ændring af hvidlister) kræver stærk kundeautentificering. Hvis en betalingstjenesteudbyder udelukkende udbyder rådgivningstjenester, hvor der ikke videregives nogen følsomme kunde- eller betalingsoplysninger, såsom betalingskortdata, der nemt kan misbruges til svindel, kan betalingstjenesteudbyderen tilpasse sine autentificeringskrav på grundlag af sin risikovurdering.

7.3 [kort] For korttransaktioner bør alle betalingstjenesteudbydere, der udsteder kort, understøtte stærk autentificering af kortholderen. Alle udstedte kort skal teknisk være klar (registrerede) til at blive anvendt med stærk autentificering.

7.4 [kort] Betalingsindløsere bør understøtte teknologier, der gør det muligt for udstederen at udføre stærk autentificering af kortholderen for de kortbetalingsordninger, som indløseren deltager i.

7.5 [kort] Betalingsindløsere, bør kræve, at deres e-handelsforretninger understøtter løsninger, der gør det muligt for udstederen at udføre stærk autentificering af kortholderen for korttransaktioner via internettet. Det kan overvejes at anvende

[14] Se definitionen af betalingsinstrumenter for små betalinger (mikrobetalingsinstrumenter) i artikel 34, stk. 1, og artikel 53, stk. 1, i betalingstjenestedirektivet.

alternative autentificeringsmetoder for på forhånd identificerede kategorier af lavrisikotransaktioner, f.eks. på baggrund af en transaktionsrisikoanalyse, eller for transaktioner, der involverer betalinger af små beløb, som nævnt i betalingstjenestedirektivet.

7.6 [kort] For de betalingskort-schemes, der accepteres af tjenesten, bør udbydere af digitale tegnebøger kræve stærk autentificering af udstederen, første gang den retmæssige kortholder registrerer kortdataene.

7.7 Udbydere af digitale tegnebøger bør understøtte stærk kundeautentificering, når kunder logger ind på den digitale tegnebog eller udfører transaktioner ved hjælp af betalingskort via internettet. Det kan overvejes at anvende alternative autentificeringsmetoder for på forhånd identificerede kategorier af lavrisikotransaktioner, f.eks. på baggrund af en transaktionsrisikoanalyse, eller for transaktioner, der involverer betalinger af små beløb, som nævnt i betalingstjenestedirektivet.

7.8 [kort] For virtuelle kort bør den første registrering finde sted i et sikkert og pålideligt miljø.[15] Der bør kræves stærk kundeautentificering for datagenereringsprocessen for virtuelle kort, hvis kortet udstedes i internetmiljøet.

7.9 Betalingstjenesteudbydere bør sikre bilateral autentificering ved kommunikation med e-handelsforretninger med henblik på initiering af internetbetalinger og adgang til følsomme betalingsdata.

Tilmelding til og levering af autentificeringsværktøjer og/eller software leveret til kunden

8. Betalingstjenesteudbydere bør sikre, at kunders tilmelding til og den første levering af de autentificeringsværktøjer, der kræves for at anvende internetbetalingstjenesten, og/eller levering af betalingsrelateret software til kunder, sker på en sikker måde.

8.1 Tilmelding til og levering af autentificeringsværktøjer og/eller betalingsrelateret software leveret til kunden bør opfylde følgende krav:

- De relaterede procedurer bør udføres i et sikkert og pålideligt miljø, idet der tages højde for potentielle risici som følge af enheder, der ikke er under betalingstjenesteudbyderens kontrol.

[15] Miljøer, som hører ind under betalingstjenesteudbyderens ansvar, og hvor der er garanteret tilstrækkelig autentificering af kunden og af den betalingstjenesteudbyder, der udbyder tjenesten, og beskyttelse af fortrolige/følsomme oplysninger, omfatter: i) betalingstjenesteudbyderens lokaliteter, ii) netbanker eller andet sikkert websted, f.eks. hvor det selskab der administrerer betalingssystemet tilbyder tilsvarende sikkerhedsfeatures, blandt andet som defineret i retningslinje 4, eller iii) kontantautomater (ATM). (I forbindelse med kontantautomater kræves der stærk kundeautentificering. En sådan autentificering foregår sædvanligvis ved hjælp af chip og pinkode eller chip og biometriske oplysninger.)

- Der bør være indført effektive og sikre procedurer for leveringen af personlige sikkerhedsoplysninger (personalised security credentials), betalingsrelateret software og alle internetbetalingsrelaterede personaliserede enheder. Software leveret via internettet bør også underskrives digitalt af betalingstjenesteudbyderen, så kunden kan få bekræftet dens autenticitet, og at der ikke er manipuleret med den.

- [kort] For korttransaktioner bør kunden have mulighed for at tilmelde sig stærk autentificering uafhængigt af et specifikt internetkøb. Hvis aktivering i løbet af onlinekøb tilbydes, bør dette gøres ved at omdirigere kunden til et sikkert og pålideligt miljø.

8.2 [kort] Udstedere bør aktivt tilskynde til, at kortholdere tilmelder sig stærk autentificering, og kun give deres kortholdere mulighed for at undlade at tilmelde sig i særlige og begrænsede tilfælde, hvor det er begrundet i den risiko, der er forbundet med den specifikke korttransaktion.

Loginforsøg, sessionstimeout, gyldigheden af autentificering

9. Betalingstjenesteudbydere bør begrænse antallet af login- eller autentificeringsforsøg, definere regler for session-"timeouts" og fastlægge tidsbegrænsninger for gyldigheden af en autentificering.

9.1 Når der anvendes en engangsadgangskode til autentificering, bør betalingstjenesteudbydere sikre, at gyldighedsperioden for sådanne adgangskoder begrænses til et absolut nødvendigt minimum.

9.2 Betalingstjenesteudbydere bør fastlægge det maksimale antal mislykkede login- eller autentificeringsforsøg, hvorefter adgang til internetbetalingstjenesten blokeres (midlertidigt eller permanent). De bør have indført en sikker procedure til genaktivering af blokerede internetbetalingstjenester.

9.3 Betalingstjenesteudbydere bør fastlægge den maksimale periode, hvorefter inaktive sessioner automatisk afsluttes.

Overvågning af transaktioner

10. Transaktionsovervågningsmekanismer, der er udviklet med henblik på at forhindre, afsløre og blokere svigagtige betalingstransaktioner, bør anvendes før betalingstjenesteudbyderens endelige autorisation, og mistænkelige eller højrisikotransaktioner bør gennemgå en specifik screenings- og evalueringsprocedure. Der bør også være indført tilsvarende sikkerhedsovervågnings- og autorisationsmekanismer for udstedelsen af e-mandater.

10.1 Betalingstjenesteudbydere bør anvende systemer til afsløring og forebyggelse af svindel med henblik på at identificere mistænkelige transaktioner, inden betalingstjenesteudbyderen endeligt autoriserer transaktioner eller e-mandater. Sådanne systemer bør være baseret på f.eks. parametriserede regler (såsom sortlister for lækkede eller stjålne kortdata) og bør overvåge unormale adfærdsmønstre for kunden eller kundens adgangsenhed (såsom en ændring i IP-adressen[16] eller IP-rækkevidden i løbet af internetbetalingstjenestesessionen, undertiden betegnet som IP-geolokaliseringskontroller,[17] atypiske e-handlerkategorier for en specifik kunde eller unormale transaktionsdata osv.). Sådanne systemer bør også være i stand til at afsløre tegn på malwareinfektion i sessionen (f.eks. via script versus menneskelig validering) og kendte svindelscenarier. Løsningen, der anvendes til denne overvågning, bør i omfang, kompleksitet og tilpasningsevne stå mål med risikovurderingens resultat, og samtidig bør den overholde den relevante databeskyttelseslovgivning.

10.2 Betalingsindløsere bør have indført systemer til afsløring og forebyggelse af svindel med henblik på at overvåge e-handlernes aktiviteter.

10.3 Betalingstjenesteudbydere bør udføre eventuelle transaktionsscreenings- og evalueringsprocedurer inden for en passende tidsperiode for at undgå unødvendige forsinkelser i initieringen og/eller gennemførelsen af den pågældende betalingstjeneste.

10.4 Hvis betalingstjenesteudbyderen i henhold til sin risikopolitik beslutter sig for at blokere en betalingstransaktion, der er identificeret som potentielt svigagtig, bør betalingstjenesteudbyderen opretholde blokeringen i så kort tid som muligt, indtil sikkerhedsproblemerne er blevet løst.

Beskyttelse af følsomme betalingsdata

11. Følsomme betalingsdata bør beskyttes, når de lagres, behandles eller overføres.

11.1 Alle data, der anvendes til at identificere og autentificere kunder (f.eks. ved login, ved initiering af internetbetalinger og ved udstedelse, ændring eller annullering af e-mandater), og kundegrænsefladen (betalingstjenesteudbyderens eller e-handelsforretningens websted) bør på passende vis sikres mod tyveri og uautoriseret adgang eller ændring.

11.2 Betalingstjenesteudbydere bør sikre, at der ved udveksling af følsomme betalingsdata via internettet anvendes sikker end-to-end-kryptering[18] mellem de kommunikerende

[16] En IP-adresse er en unik numerisk kode, som identificerer hver enkelt computer, der er forbundet med internettet.

[17] En "Geo-IP"-kontrol bekræfter, om det udstedende land svarer til den IP-adresse, hvorfra brugeren initierer transaktionen.

[18] End-to-end-kryptering er kryptering i eller ved kildesystemet, hvor den tilsvarende kryptering kun forekommer i eller ved målsystemet. ETSI EN 302 109 V1.1.1. (2003-06).

parter i hele den pågældende kommunikationssession med henblik på at sikre dataenes fortrolighed og integritet. Dette bør ske ved anvendelse af stærke og bredt anerkendte krypteringsteknikker.

11.3 Betalingsindløsere, bør tilskynde til, at deres e-handelsforretninger ikke lagrer følsomme betalingsdata. I tilfælde af at e-handelsforretninger håndterer, dvs. lagrer, behandler eller overfører følsomme betalingsdata, bør disse betalingstjenesteudbydere ved kontrakt kræve, at e-handelsforretningerne har indført de nødvendige foranstaltninger til beskyttelse af disse data. Betalingstjenesteudbydere bør foretage regelmæssige kontroller, og hvis en betalingstjenesteudbyder bliver vidende om, at en e-handler, der håndterer følsomme betalingsdata, ikke har indført de nødvendige sikkerhedsforanstaltninger, bør udbyderen tage skridt til at håndhæve denne aftalemæssige forpligtelse eller opsige aftalen.

Kundeawareness, -uddannelse og -kommunikation

Kundeuddannelse og kundekommunikation

12. Betalingstjenesteudbydere bør, i det omfang det er nødvendigt, bistå og vejlede kunderne med hensyn til sikker brug af internetbetalingstjenesterne. Betalingstjenesteudbydere bør kommunikere med deres kunder på en sådan måde, at de forsikres om autenticiteten af de modtagne beskeder.

12.1 Betalingstjenesteudbydere bør stille mindst én sikker kommunikationskanal [19] til rådighed for løbende kommunikation med kunderne vedrørende korrekt og sikker brug af internetbetalingstjenesten. Betalingstjenesteudbydere bør informere kunderne om denne kanal og forklare, at beskeder på vegne af betalingstjenesteudbyderen via ethvert andet middel, såsom e-mail, vedrørende korrekt og sikker brug af internetbetalingstjenesten ikke er pålidelige. Betalingstjenesteudbyderen bør forklare:

- den procedure, kunderne skal anvende til at indberette (mistanke om) svigagtige betalinger, mistænkelige hændelser eller uregelmæssigheder i løbet af internetbetalingstjenestesessionen og/eller mulige forsøg på social manipulation (social engineering)[20] til betalingstjenesteudbyderen

- det videre forløb, dvs. hvordan betalingstjenesteudbyderen vil reagere i forhold til kunden

- hvordan betalingstjenesteudbyderen vil underrette kunden om (potentielle) svigagtige transaktioner eller manglende initiering af transaktioner samt advare kunden om forekomsten af angreb (f.eks. phishing e-mails).

12.2 Betalingstjenesteudbydere bør gennem den sikre kommunikationskanal holde kunderne informeret om opdateringer i sikkerhedsprocedurer vedrørende internetbetalingstjenester. Eventuelle varslinger om nye betydelige risici (f.eks. advarsler om social manipulation) bør også gives via den sikre kommunikationskanal.

12.3 Betalingstjenesteudbydere bør hjælpe kunderne i alle spørgsmål, klager, anmodninger om support og underretninger af uregelmæssigheder eller hændelser vedrørende internetbetalinger og relaterede tjenester, og kunderne bør behørigt informeres om, hvordan de kan få adgang til denne hjælp.

12.4 Betalingstjenesteudbydere bør iværksætte kundeuddannelses- og kundeawareness programmer, der er udformet med henblik på at sikre, at kunderne som minimum forstår behovet for at:

[19] Såsom en anvist postkasse på betalingstjenesteudbyderens websted eller et sikret websted.

[20] Social manipulering betyder i denne sammenhæng teknikker, der bruges til at manipulere mennesker med henblik på at indsamle oplysninger (f.eks. via e-mail eller telefonopkald) eller indhente oplysninger fra sociale netværk med henblik på svindel eller uautoriseret adgang til en computer eller et netværk.

- beskytte deres adgangskoder, sikkerhedstokens, personlige oplysninger og andre fortrolige data

- styre sikkerheden i den personlige enhed (f.eks. computer) ved at installere og opdatere sikkerhedskomponenter (antivirus, firewalls, sikkerhedspatches)

- tage højde for de betydelige trusler og risici, der er forbundet med download af software via internettet, hvis kunden ikke med rimelighed kan slå fast, at softwaren er ægte og ikke er manipuleret med

- anvende betalingstjenesteudbyderens ægte internetbetalingswebsted.

12.5 Betalingsindløsere bør kræve, at e-handelsforretninger tydeligt holder betalingsrelaterede processer adskilt fra netbutikken, så kunderne nemmere kan se, hvornår de kommunikerer med betalingstjenesteudbyderen og ikke med betalingsmodtageren (f.eks. ved at omdirigere kunden og åbne et særskilt vindue, så betalingsprocessen ikke vises inden for e-handelsforeningens rammer).

Underretninger, fastsættelse af grænser

13. Betalingstjenesteudbydere bør fastsætte begrænsninger for brugen af internetbetalingstjenester og kan give deres kunder mulighed for yderligere at fastsætte risikobegrænsning inden for disse grænser. De kan også udbyde tjenester vedrørende advarsler og kundeprofilstyring.

13.1 Inden en kunde tilbydes internetbetalingstjenester, bør betalingstjenesteudbydere fastsætte grænser[21] for de pågældende tjenester (f.eks. et maksimalt beløb for hver enkelt betaling eller et samlet beløb over en vis periode) og bør informere deres kunder herom. Betalingstjenesteudbydere bør gøre det muligt for kunderne at deaktivere internetbetalingsfunktionen.

Kundens adgang til information om status på initiering og gennemførelse af betalinger

14. Betalingstjenesteudbydere bør over for deres kunder bekræfte initieringen af betalingen og i behørig tid forsyne kunderne med de oplysninger, der er nødvendige for at kontrollere, om en betalingstransaktion er initieret og/eller gennemført korrekt.

14.1 [kontooverførsel/e-mandat] Betalingstjenesteudbydere bør stille en nær-realtidsfacilitet til rådighed for kunderne, hvor de når som helst kan kontrollere status på transaktionernes gennemførelse samt kontosaldi[22] i et sikkert og pålideligt miljø.

[21] Sådanne grænser kan enten gælde globalt (dvs. for alle betalingsinstrumenter, der giver mulighed for internetbetalinger) eller individuelt.

[22] Undtagen hvis faciliteten ekstraordinært er utilgængelig på grund af teknisk vedligeholdelse eller på grund af større hændelser.

14.2 Eventuelle detaljerede elektroniske opgørelser bør gøres tilgængelige i et sikkert og pålideligt miljø. Hvis betalingstjenesteudbydere informerer kunderne om tilgængeligheden af elektroniske opgørelser (f.eks. regelmæssigt, når der er udstedt en periodisk e-opgørelse, eller på ad hoc-basis efter gennemførelse af en transaktion) gennem en alternativ kanal, såsom SMS, e-mail eller brev, bør sådanne meddelelser ikke indeholde følsomme betalingsdata. Hvis meddelelserne indeholder følsomme betalingsdata, skal de krypteres.

Afsnit III – Afsluttende bestemmelser og gennemførelse

15. Disse retningslinjer finder anvendelse fra den 01.08.2015.

Bilag 1: Eksempler på bedste praksis

Ud over ovennævnte krav beskriver disse retningslinjer bedste praksis, som der tilskyndes til, men ikke kræves, at betalingstjenesteudbyderne og de relevante markedsdeltagere indfører. For overskuelighedens skyld er de kapitler, som denne bedste praksis gælder for, udtrykkeligt anført.

Generelt kontrol- og sikkerhedsmiljø

Ledelse

BP 1: Sikkerhedspolitikken kunne fastlægges i et særskilt dokument.

Risikostyring og -reduktion

BP 2: Betalingstjenesteudbydere kunne stille sikkerhedsværktøjer (f.eks. enheder og/eller brugertilpassede browsere, der er behørigt sikret,) til rådighed til beskyttelse af kundegrænsefladen mod uretmæssig brug eller angreb (f.eks. "man in the browser"-angreb).

Sporbarhed

BP 3: Betalingsindløsere kunne ved aftale kræve, at e-handelsforretninger, som lagrer betalingsoplysninger, har indført passende processer til understøttelse af sporbarhed.

Specifikke kontrol- og sikkerhedsforanstaltninger vedrørende internetbetalinger

Indledende identificering af kunder, oplysninger

BP4: Kunden kunne underskrive en tjenestekontrakt vedrørende udførelse af internetbetalingstransaktioner, frem for at vilkårene indgår i en bredere generel kontrakt med betalingstjenesteudbyderen.

BP5: Betalingstjenesteudbydere kunne også sikre, at kunderne løbende eller, i det omfang det er relevant, på ad hoc-basis og via passende midler (f.eks. foldere, websteder) gives tydelige og enkle anvisninger, der forklarer deres ansvar med hensyn til sikker brug af tjenesten.

Stærk kundeautentificering

BP6: [kort] E-handelsforretninger kunne understøtte stærk autentificering fra udstederens side af kortholderen i korttransaktioner via internettet.

BP7: For at lette processen for kunderne kunne betalingstjenesteudbydere overveje at anvende et enkelt værktøj til stærk kundeautentificering for alle internetbetalingstjenester. Dette kunne øge kundernes accept af løsningen og gøre det nemmere at anvende den korrekt.

BP8: Stærk kundeautentificering kunne omfatte elementer, der forbinder autentificeringen til et specifikt beløb eller en specifik modtager. Dette kunne give kunderne øget vished i forbindelse med autorisation af betalinger. Den teknologiløsning, der gør det muligt at forbinde de data, der er underlagt stærk autentificering, og transaktionsdataene, bør være sikret mod manipulering.

Beskyttelse af følsomme betalingsdata

BP 9: Det er ønskeligt, at e-handelsforretninger, der håndterer følsomme betalingsdata, giver personale med ansvar for afsløring af svindel passende undervisning og ajourfører denne uddannelse regelmæssigt med henblik på at sikre, at indholdet altid er relevant i forhold til et dynamisk sikkerhedsmiljø.

Kundeuddannelse og kundekommunikation

BP 10: Det er ønskeligt, at betalingsindløsere tilrettelægger uddannelsesprogrammer for deres e-handelsforretninger vedrørende forebyggelse af svindel.

Underretninger, fastsættelse af grænser

BP 11: Betalingstjenesteudbydere kunne inden for de fastsatte begrænsninger for brugen give deres kunder mulighed for at styre grænser for internetbetalingstjenester i et sikkert og pålideligt miljø.

BP 12: Betalingstjenesteudbydere kunne indføre varsling til kunder, såsom via telefonopkald eller SMS, om mistænkelige transaktioner eller højrisikotransaktioner på baggrund af deres risikostyringspolitikker.

BP 13: Betalingstjenesteudbydere kunne gøre det muligt for kunder at fastlægge generelle, personaliserede regler som parametre for deres adfærd i forbindelse med internetbetalinger og relaterede tjenester, f.eks. at de kun vil initiere betalinger fra bestemte lande, og at betalinger, der initieres fra andre steder, bør blokeres, eller at de kan anføre specifikke modtagere på hvid- eller sortlister.