EBA/GL/2017/17

12/01/2018

Smernice

o varnostnih ukrepih za operativna in varnostna tveganja pri plačilnih storitvah na podlagi Direktive (EU) 2015/2366 (PSD2)

1. Obveznosti glede skladnosti in poročanja

Vloga teh smernic

1. Dokument vsebuje smernice, izdane v skladu s členom 16 Uredbe (EU) št. 1093/2010[1]. V skladu s členom 16(3) Uredbe (EU) št. 1093/2010 si morajo pristojni organi in finančne institucije na vsak način prizadevati za upoštevanje smernic.

2. V smernicah je predstavljeno stališče organa EBA o ustreznih nadzorniških praksah v Evropskem sistemu finančnega nadzora in o tem, kako bi bilo treba zakonodajo Unije uporabljati na določenem področju. Pristojni organi iz člena 4(2) Uredbe (EU) št. 1093/2010, za katere smernice veljajo, bi jih morali upoštevali tako, da jih ustrezno vključijo v svoje prakse (npr. s spremembo svojega pravnega okvira ali nadzorniških postopkov), tudi če so smernice namenjene predvsem institucijam.

Dolžnost poročanja

3. Pristojni organi morajo v skladu s členom 16(3) Uredbe (EU) št. 1093/2010 do 12.03.2018 organ EBA uradno obvestiti, ali ravnajo oziroma ali nameravajo ravnati v skladu s temi smernicami, ali pa mu sporočiti razloge za njihovo neupoštevanje. Če pristojni organi do tega roka ne bodo poslali uradnega obvestila, bo organ EBA štel, da jih ne upoštevajo. Uradna obvestila je treba poslati na obrazcu, ki je na voljo na spletni strani organa EBA, na elektronski naslov compliance@eba.europa.eu z navedbo sklica „EBA/GL/2017/17“. Predložiti jih morajo osebe, ki so pooblaščene za poročanje o skladnosti v imenu svojih pristojnih organov. Organu EBA je treba sporočiti tudi vsako spremembo stanja glede upoštevanja smernic.

4. Uradna obvestila bodo v skladu s členom 16(3) objavljena na spletni strani organa EBA.

[1] Uredba (EU) št. 1093/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski bančni organ) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/78/ES (UL L 331, 15.12.2010, str. 12).

2. Vsebina, področje uporabe in opredelitve pojmov

Vsebina in področje uporabe

5. Te smernice temeljijo na pooblastilu, dodeljenemu Evropskemu bančnemu organu (EBA) na podlagi člena 95(3) Direktive (EU) 2015/2366[2] (PSD2).

6. Smernice določajo zahteve za vzpostavljanje, izvajanje in spremljanje varnostnih ukrepov, ki jih morajo sprejeti ponudniki plačilnih storitev v skladu s členom 95(1) Direktive (EU) 2015/2366 za obvladovanje operativnih in varnostnih tveganj, povezanih s plačilnimi storitvami, ki jih opravljajo.

Naslovniki

7. Te smernice so namenjene ponudnikom plačilnih storitev, kakor so opredeljeni v členu 4(11) Direktive (EU) 2015/2366 in kakor je navedeno v opredelitvi pojma „finančne institucije“ v členu 4(1) Uredbe (EU) 1093/2010, in pristojnim organom, kakor so opredeljeni v točki (i) člena 4(2) te uredbe, s sklicevanjem na razveljavljeno Direktivo 2007/64/ES[3] (sedaj Direktiva (EU) 2015/2366[4]).

Opredelitve

8. Če ni določeno drugače, imajo izrazi v teh smernicah enak pomen kot izrazi, ki se uporabljajo in so opredeljeni v Direktivi (EU) 2015/2366. Poleg tega se v teh smernicah uporabljajo naslednje opredelitve:

Upravljalni organ	– Za ponudnike plačilnih storitev, ki so kreditne institucije, ima ta izraz enak pomen kot opredelitev v točki (7) člena 3(1) Direktive 2013/36/EU[5]. – Za ponudnike plačilnih storitev, ki so plačilne institucije ali institucije za izdajo elektronskega denarja, pomeni ta izraz

[2] Direktiva (EU) 2015/2366 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o plačilnih storitvah na notranjem trgu, spremembah direktiv 2002/65/ES, 2009/110/ES ter 2013/36/EU in Uredbe (EU) št. 1093/2010 ter razveljavitvi Direktive 2007/64/ES (UL L 337, 23.12.2015, str. 35).

[3] Direktiva 2007/64/ES Evropskega parlamenta in Sveta z dne 13. novembra 2007 o plačilnih storitvah na notranjem trgu in o spremembah direktiv 97/7/ES, 2002/65/ES, 2005/60/ES in 2006/48/ES ter o razveljavitvi Direktive 97/5/ES (UL L 319, 5.12.2007, str. 1).

[4] V skladu z drugim pododstavkom člena 114 Direktive (EU) 2015/2366 se šteje vsako sklicevanje na razveljavljeno Direktivo 2007/64/ES za sklicevanje na Direktivo (EU) 2015/2366 in se bere v skladu s korelacijsko tabelo v Prilogi II k Direktivi (EU) 2015/2366.

[5] Direktiva 2013/36/EU Evropskega parlamenta in Sveta o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij in investicijskih podjetij, spremembi Direktive 2002/87/ES in razveljavitvi direktiv 2006/48/ES in 2006/49/ES (UL L 176, 27.6.2013, str. 338).

	direktorje in osebe, odgovorne za upravljanje ponudnika plačilnih storitev, in po potrebi osebe, odgovorne za upravljanje dejavnosti plačilnih storitev ponudnika plačilnih storitev. – Za ponudnike plačilnih storitev iz točk (c), (e) in (f) člena 1(1) Direktive (EU) 2015/2366 ima ta izraz pomen, ki mu ga je dodelila veljavna zakonodaja EU ali veljavna nacionalna zakonodaja.
Operativni ali varnostni incident	Enkratni dogodek ali niz povezanih dogodkov, ki jih ponudnik plačilnih storitev ne načrtuje in ki ima ali bo verjetno imel negativen učinek na celovitost, razpoložljivost, zaupnost, avtentičnost in/ali neprekinjenost s plačilom povezanih storitev.
Višje vodstvo	(a) Za ponudnike plačilnih storitev, ki so kreditne institucije, ima ta izraz enak pomen kot opredelitev v točki (9) člena 3(1) Direktive 2013/36/EU. (b) Za ponudnike plačilnih storitev, ki so plačilne institucije in institucije za izdajo elektronskega denarja, pomeni ta izraz fizične osebe, ki v instituciji opravljajo izvršilne funkcije in so odgovorne upravljalnemu organu za vsakodnevno upravljanje ponudnika plačilnih storitev. (c) Za ponudnike plačilnih storitev iz točk (c), (e) in (f) člena 1(1) Direktive (EU) 2015/2366 ima ta izraz pomen, ki mu ga je dodelila veljavna zakonodaja EU ali veljavna nacionalna zakonodaja.
Varnostno tveganje	Tveganje, ki izhaja iz neustreznih ali neuspelih notranjih postopkov ali zunanjih dogodkov, ki imajo ali bi lahko imeli negativni učinek na razpoložljivost, celovitost, zaupnost sistemov informacijske in komunikacijske tehnologije (IKT) in/ali informacij, ki se uporabljajo za opravljanje plačilnih storitev. To vključuje tveganje zaradi kibernetskih napadov ali neustrezne fizične varnosti.
Nagnjenost k prevzemanju tveganja	Skupna stopnja in vrste tveganj, ki jih je institucija pripravljena prevzeti v okviru svoje sposobnosti prevzemanja tveganj, v skladu s svojim poslovnim modelom, da doseže strateške cilje.

3. Izvajanje

Datum začetka uporabe

9. Te smernice se začnejo uporabljati 13. januarja 2018.

4. Smernice

Smernica 1: Splošna načela

1.1 Vsi ponudniki plačilnih storitev bi morali upoštevati vse določbe iz teh smernic. Raven podrobnosti mora biti sorazmerna z velikostjo ponudnika plačilnih storitev ter z naravo, obsegom, kompleksnostjo in tveganostjo posameznih storitev, ki jih ponudnik plačilnih storitev opravlja ali namerava opravljati.

Smernica 2: Upravljanje

Okvir upravljanja operativnih in varnostnih tveganj

2.1 Ponudniki plačilnih storitev bi morali vzpostaviti učinkovit okvir upravljanja operativnih in varnostnih tveganj (v nadaljevanju: okvir upravljanja tveganj), ki bi ga moral upravljalni organ in, kadar je primerno, višje vodstvo, odobriti in pregledati vsaj enkrat na leto. Ta okvir bi moral biti osredotočen na varnostne ukrepe za zmanjšanje operativnih in varnostnih tveganj ter bi moral biti v celoti vključen v vse postopke ponudnika plačilnih storitev za upravljanje tveganj.

2.2 Okvir upravljanja tveganj mora:

a) vključevati izčrpen dokument o varnostni strategiji, kot je navedeno v členu 5(1)(j) Direktive (EU) 2015/2366;

b) biti skladen z nagnjenostjo ponudnika plačilnih storitev k prevzemanju tveganj;

c) opredeliti in določiti ključne vloge in odgovornosti ter ustrezni sistem poročanja, ki je potreben za krepitev varnostnih ukrepov ter upravljanje varnostnih in operativnih tveganj;

d) vzpostaviti potrebne postopke in sisteme za ugotavljanje, merjenje, spremljanje in upravljanje številnih tveganj, ki izhajajo iz dejavnosti ponudnika plačilnih storitev v zvezi s plačili in ki jim je ponudnik plačilnih storitev izpostavljen, vključno z ureditvami za zagotavljanje neprekinjenega poslovanja.

2.3 Ponudniki plačilnih storitev bi morali zagotoviti, da je okvir upravljanja tveganj ustrezno dokumentiran ter med njegovim izvajanjem in spremljanjem redno posodobljen z dokumentiranimi „pridobljenimi novimi spoznanji“.

2.4 Ponudniki plačilnih storitev bi morali zagotoviti, da pred vsako večjo spremembo infrastrukture, procesov ali postopkov in po vsakem večjem operativnem ali varnostnem incidentu, ki vpliva na varnost plačilnih storitev, ki jih opravljajo, pregledajo, ali je treba nemudoma izvesti spremembe ali izboljšave okvira upravljanja tveganj.

Upravljanje tveganj in modeli za nadzor

2.5 Ponudniki plačilnih storitev bi morali zaradi prepoznavanja ter upravljanja operativnih in varnostnih tveganj vzpostaviti tri učinkovite nivoje obrambe ali enakovreden model notranjega upravljanja tveganj in kontrol. Ponudniki plačilnih storitev bi morali zagotoviti, da ima omenjeni model notranje kontrole ustrezna pooblastila, neodvisnost, sredstva in neposredne linije poročanja upravljalnemu organu ter, kadar je primerno, višjemu vodstvu.

2.6 Varnostne ukrepe iz teh smernic bi morali revidirati revizorji s strokovnim znanjem na področju varnosti informacijskih tehnologij in plačil, ki so operativno neodvisni znotraj ponudnikov plačilnih storitev ali od njih. V zvezi s pogostostjo in usmerjenostjo takšnih revizij bi bilo treba upoštevati ustrezna varnostna tveganja.

Zunanje izvajanje

2.7 Kadar se izvajanje operativnih nalog, povezanih z opravljanjem plačilnih storitev, vključno s sistemi IT, uporabijo zunanji izvajalci, bi morali ponudniki plačilnih storitev zagotoviti učinkovitost varnostnih ukrepov iz teh smernic.

2.8 Ponudniki plačilnih storitev bi morali zagotoviti, da so ustrezni in sorazmerni varnostni cilji, ukrepi in ciljne zmogljivosti vključeni v pogodbe in sporazume o ravni storitev, sklenjene s ponudniki, ki so zunanji izvajalci takšnih funkcij. Ponudniki plačilnih storitev bi morali spremljati in dobiti zagotovilo glede ravni skladnosti takšnih ponudnikov z varnostnimi cilji, ukrepi in ciljnimi zmogljivostmi.

Smernica 3: Ocena tveganja

Opredelitev funkcij, postopkov in sredstev

3.1 Ponudniki plačilnih storitev bi morali opredeliti, vzpostaviti in redno posodabljati popis svojih poslovnih funkcij, ključnih vlog in podpornih postopkov, da bi določili pomen vsake funkcije, vloge in podpornega postopka ter njihovo medsebojno odvisnost v povezavi z operativnimi in varnostnimi tveganji.

3.2 Ponudniki plačilnih storitev bi morali opredeliti, vzpostaviti in redno posodabljati inventar informacijskih sredstev, kot so sistemi IKT, njihove konfiguracije, druge infrastrukture, pa tudi medsebojne povezave z drugimi notranjimi in zunanjimi sistemi, da bi lahko upravljali s sredstvi, ki podpirajo njihove ključne poslovne funkcije in postopke.

Razvrščanje funkcij, postopkov in podatkov

3.3 Ponudniki plačilnih storitev bi morali razvrstiti ugotovljene poslovne funkcije, podporne postopke in informacijska sredstva glede na kritičnost.

Ocena tveganja funkcij, postopkov in podatkov

3.4 Ponudniki plačilnih storitev bi morali zagotoviti, da nenehno spremljajo grožnje in ranljivosti ter redno pregledujejo scenarije tveganj, ki vplivajo na njihove poslovne funkcije, ključne postopke in informacijska sredstva. Ponudniki plačilnih storitev bi morali v okviru obveznosti, da izvajajo ter pristojnim organom posredujejo posodobljeno in celovito oceno tveganja za operativna in varnostna tveganja, povezana s plačilnimi storitvami, ki jih opravljajo, ter ustreznosti omilitvenih ukrepov in nadzornih mehanizmov, ki jih izvajajo kot odgovor na ta tveganja, kot je določeno v členu 95(2) Direktive (EU) 2015/2366, vsaj enkrat na leto ali pogosteje, kot to določi pristojni organ, izvajati in dokumentirati ocene tveganja funkcij, postopkov in informacijskih sredstev, ki so jih ugotovili in razvrstili, da bi odkrili in ocenili ključna operativna in varnostna tveganja. Takšne ocene tveganja bi bilo treba opraviti tudi pred vsako večjo spremembo infrastrukture, procesov ali postopkov, ki vplivajo na varnost plačilnih storitev.

3.5 Na podlagi ocen tveganja bi morali ponudniki plačilnih storitev določiti, ali so potrebne spremembe obstoječih varnostnih ukrepov, uporabljenih tehnologij in postopkov ali plačilnih storitev, ki jih ponujajo, in obseg takšnih sprememb. Ponudniki plačilnih storitev bi morali upoštevati čas, ki je potreben za izvajanje sprememb, in čas za izvajanje ustreznih notranjih varnostnih ukrepov za zmanjšanje operativnih ali varnostnih incidentov, goljufije in morebitnih motečih učinkov pri izvajanju plačilnih storitev.

Smernica 4: Zaščita

4.1 Ponudniki plačilnih storitev bi morali vzpostaviti in izvajati preventivne varnostne ukrepe v odziv na ugotovljena operativna in varnostna tveganja. Ti ukrepi bi morali zagotavljati primerno raven zaščite v skladu z ugotovljenimi tveganji.

4.2 Ponudniki plačilnih storitev bi morali vzpostaviti in izvajati pristop „večplastne obrambe“ z uvedbo večravninskih kontrol, ki bi zajemale ljudi, procese in tehnologijo, pri čemer bi vsaka raven služila kot varnostna mreža za prejšnje ravni. Večplastno obrambo je treba razumeti tako, da je za isto tveganje določena več kot samo ena kontrola, kot je npr. načelo štirih oči, dvojno preverjanje pristnosti, mrežna delitev in več požarnih zidov.

4.3 Ponudniki plačilnih storitev bi morali zagotoviti zaupnost, celovitost in razpoložljivost svojih ključnih logičnih in fizičnih sredstev, virov in občutljivih plačilnih podatkov svojih uporabnikov plačilnih storitev, ki so lahko v mirovanju, prehodu ali v uporabi. Če podatki vključujejo osebne podatke, bi bilo treba te ukrepe izvajati v skladu z Uredbo (EU) 2016/679[6], ali če je primerno, Uredbo (ES) 45/2001.[7]

[6] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

[7] Uredba (ES) št. 45/2001 evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1).

4.4 Ponudniki plačilnih storitev bi morali redno ugotavljati, ali spremembe v obstoječem operativnem okolju vplivajo na obstoječe varnostne ukrepe oziroma zahtevajo, da se sprejmejo nadaljnji ukrepi za ublažitev s tem povezanega tveganja. Te spremembe bi morale predstavljati del formalnega postopka za upravljanje sprememb, ki bi moral zagotavljati, da so spremembe ustrezno načrtovane, preskušene, dokumentirane in odobrene. Na podlagi opaženih groženj za varnost in izvedenih sprememb bi bilo treba opraviti testiranje, da bi se vključili scenariji ustreznih in znanih morebitnih napadov.

4.5 Pri oblikovanju, razvijanju in opravljanju plačilnih storitev bi morali ponudniki plačilnih storitev zagotoviti, da se uporabita načeli ločevanja nalog in „minimalnih pravic“. Ponudniki plačilnih storitev bi morali nameniti posebno pozornost ločevanju okolij informacijske tehnologije, zlasti okolja razvoja, testiranja in proizvodnje.

Celovitost in zaupnost podatkov in sistemov

4.6 Pri oblikovanju, razvijanju in opravljanju plačilnih storitev bi morali ponudniki plačilnih storitev zagotoviti, da so postopki zbiranja, usmerjanja, obdelave, shranjevanja in/ali arhiviranja ter vizualizacije občutljivih plačilnih podatkov uporabnikov plačilnih storitev ustrezni, relevantni in omejeni le na to, kar je potrebno za opravljanje njihovih plačilnih storitev.

4.7 Ponudniki plačilnih storitev bi morali redno preverjati, ali je programska oprema, ki se uporablja za opravljanje plačilnih storitev, vključno s plačili povezano programsko opremo uporabnikov, posodobljena in da se uporabljajo kritični varnostni programski popravki. Ponudniki plačilnih storitev bi morali zagotoviti, da so na voljo mehanizmi za preverjanje celovitosti, s katerimi se preveri celovitost programske opreme, požarni zid in informacije o njihovih plačilnih storitvah.

Fizična varnost

4.8 Ponudniki plačilnih storitev bi morali imeti vzpostavljene primerne fizične varnostne ukrepe, zlasti da se zavarujejo občutljivi podatki o plačilih uporabnikov plačilnih storitev ter sistemi IKT, ki se uporabljajo za opravljanje plačilnih storitev.

Kontrola dostopa

4.9 Fizičen in logičen dostop do sistemov IKT bi moral biti dovoljen samo pooblaščenim posameznikom. Pooblastilo se podeli v skladu z nalogami in odgovornostmi zaposlenih ter se omeji na posameznike, ki so ustrezno usposobljeni in nadzorovani. Ponudniki plačilnih storitev bi morali vzpostaviti kontrole, ki takšen dostop do sistemov IKT zanesljivo omejijo na osebe z zakonitimi poslovnimi zahtevami. Elektronski dostop do podatkov in sistemov s pomočjo aplikacij bi moral biti omejen na minimum, ki je potreben za opravljanje ustrezne storitve.

4.10 Ponudniki plačilnih storitev bi morali vzpostaviti stroge kontrole privilegiranega dostopa do sistema s strogim omejevanjem in nadzorovanjem osebja, ki ima obširnejše pravice za dostop do sistema. Izvajati bi bilo treba kontrole, kot so dostop na podlagi vloge (role-based access), vodenje evidence in pregledovanje sistemskih dejavnosti privilegiranih uporabnikov, strogo preverjanje

pristnosti in spremljanje nepravilnosti. Ponudniki plačilnih storitev bi morali upravljati pravice dostopa do informacijskih sredstev in njihove podporne sisteme na podlagi „potrebe po seznanjenosti z informacijami“ (need-to-know basis). Pravice dostopa bi bilo treba redno pregledovati.

4.11 Evidence o dostopu je treba hraniti takšno obdobje, ki je sorazmerno kritičnosti ugotovljenih poslovnih funkcij, podpornih procesov in informacijskih sredstev, v skladu s smernicama 3.1 in 3.2, brez poseganja v zahteve o hrambi, ki jih določa zakonodaja EU in nacionalna zakonodaja. Ponudniki plačilnih storitev bi morali te informacije uporabljati za lažje ugotavljanje in preiskovanje nepravilnih dejavnosti, ki so bile ugotovljene pri opravljanju plačilnih storitev.

4.12 Zaradi zagotavljanja varne komunikacije in zmanjšanja tveganja se odobri oddaljeni administrativni dostop do kritičnih elementov IKT le na podlagi „potrebe po seznanjenosti z informacijami“ in kadar se uporabljajo rešitve na podlagi strogega preverjanja pristnosti.

4.13 Delovanje produktov, orodij in postopkov v zvezi s postopki kontrole dostopa bi moralo varovati procese kontrole dostopa pred zlorabami ali zaobitvijo predpisov. To vključuje registracijo, dostavo, preklic in umik ustreznih produktov, orodij in postopkov.

Smernica 5: Odkrivanje

Stalno spremljanje in odkrivanje

5.1 Ponudniki plačilnih storitev bi morali vzpostaviti in izvajati postopke in zmožnosti za stalno spremljanje poslovnih funkcij, podpornih procesov in informacijskih sredstev z namenom odkrivanja nepravilnih dejavnosti pri opravljanju plačilnih storitev. V okviru takšnega stalnega spremljanja bi morali imeti ponudniki plačilnih storitev na voljo učinkovite zmogljivosti za odkrivanje fizičnih ali logičnih vdorov in kršitev zaupnosti, celovitosti in razpoložljivosti informacijskih sredstev, uporabljenih pri opravljanju plačilnih storitev.

5.2 Stalno spremljanje in procesi odkrivanja bi morali zajemati naslednje:

a) ustrezne notranje in zunanje dejavnike, vključno s poslovnimi funkcijami in upravnimi funkcijami za IKT;

b) transakcije za odkrivanje zlorabe dostopa s strani ponudnikov storitev ali drugih subjektov; in

c) morebitne notranje in zunanje grožnje.

5.3 Ponudniki plačilnih storitev bi morali izvajati ukrepe za odkrivanje morebitnih uhajanj informacij, zlonamernih kod in drugih groženj za varnost ter javno znanih ranljivosti programske in strojne opreme, ter iskati ustrezne nove varnostne posodobitve.

Spremljanje in poročanje o operativnih ali varnostnih incidentih

5.4 Ponudniki plačilnih storitev bi morali določiti ustrezna merila in prage za razvrstitev dogodka med operativne ali varnostne incidente, kot je določeno v oddelku „Opredelitve pojmov“ teh smernic, ter zgodnje opozorilne znake, ki ponudnika plačilnih storitev opozorijo, naj omogoči zgodnje odkrivanje operativnih ali varnostnih incidentov.

5.5 Ponudniki plačilnih storitev bi morali vzpostaviti ustrezne procese in organizacijske strukture, da bi zagotovili skladno in celostno spremljanje, obdelavo in sledenje operativnih ali varnostnih incidentov.

5.6 Ponudniki plačilnih storitev bi morali vzpostaviti postopek za sporočanje takšnih operativnih ali varnostnih incidentov in pritožb strank v zvezi z varnostjo svojemu višjemu vodstvu.

Smernica 6: Neprekinjeno poslovanje

6.1 Ponudniki plačilnih storitev bi morali vzpostaviti smotrno upravljanje neprekinjenega poslovanja, da bi kar najbolj povečali svoje zmožnosti neprekinjenega opravljanja plačilnih storitev in omejili izgube v primeru resne motnje poslovanja.

6.2 Ponudniki plačilnih storitev bi morali za vzpostavitev smotrnega upravljanja neprekinjenega poslovanja skrbno analizirati svojo izpostavljenost resnim motnjam poslovanja in (kvantitativno in kvalitativno) oceniti njihov potencialni vpliv, pri čemer bi morali uporabiti notranje in/ali zunanje podatke ter analizo scenarija. Na podlagi ugotovljenih in razvrščenih ključnih funkcij, procesov, sistemov, transakcij in medsebojnih odvisnosti v skladu s smernicami 3.1 do 3.3 bi morali ponudniki plačilnih storitev dati prednost ukrepom za zagotovitev neprekinjenega poslovanja z uporabo tveganju prilagojenega pristopa, ki lahko temelji na ocenah tveganja, ki se izvajajo v okviru smernice 3. Glede na poslovni model ponudnika plačilnih storitev lahko ta na primer olajša nadaljnjo obdelavo ključnih transakcij, medtem ko se napori za rešitev nadaljujejo.

6.3 Na podlagi analiz, ki se izvajajo v skladu s smernico 6.2, bi moral ponudnik plačilnih storitev uvesti:

a) načrt neprekinjenega poslovanja, da zagotovi, da se lahko ustrezno odzove na izredne razmere in da je sposoben vzdrževati svoje ključne poslovne dejavnosti; in

b) ukrepe za zmanjšanje tveganj, ki jih mora sprejeti v primeru prenehanja izvajanja plačilnih storitev in prekinitve obstoječih pogodb, da se izogne škodljivim vplivom na plačilne sisteme in na uporabnike plačilnih storitev ter zagotovi nemoteno izvajanje potekajočih plačilnih transakcij.

Načrt neprekinjenega poslovanja na temelju scenarija

6.4 Ponudniki plačilnih storitev bi morali upoštevati vrsto različnih scenarijev, vključno z ekstremnimi, a verjetnimi scenariji, ki bi jim bili lahko izpostavljeni, in oceniti morebitni vpliv takšnih scenarijev.

6.5 Na podlagi analize, opravljene v skladu s smernico 6.2 in verjetnimi scenariji, ugotovljenimi v skladu s smernico 6.4, bi moral ponudnik plačilnih storitev pripraviti načrte odzivanja in sanacije, ki bi morali:

a) biti osredotočeni na vpliv na delovanje ključnih funkcij, procesov, sistemov, transakcij in medsebojnih odvisnosti;

b) biti dokumentirani in dani na razpolago poslovnim in podpornim enotam ter lahko dostopni v nujnih primerih; in

c) biti posodobljeni v skladu s pridobljenimi spoznanji iz testiranj, novimi ugotovljenimi tveganji in grožnjami ter spremenjenimi cilji in prednostnimi nalogami sanacije.

Testiranje načrtov neprekinjenega poslovanja

6.6 Ponudniki plačilnih storitev bi morali testirati svoje načrte neprekinjenega poslovanja in vsaj enkrat letno opraviti testiranje delovanja svojih ključnih funkcij, procesov, sistemov, transakcij in medsebojnih odvisnosti. Načrti bi morali podpreti zaščito, in če je treba, tudi ponovno vzpostavitev celovitosti in razpoložljivosti dejavnosti, ter zaupnost informacijskih sredstev.

6.7 Načrte je treba posodobiti vsaj enkrat letno na podlagi rezultatov testiranja, trenutnih obveščevalnih podatkov o nevarnosti, skupne rabe informacij in pridobljenih spoznanj iz prejšnjih dogodkov ter spremenjenih ciljev sanacije, prav tako pa tudi analize operativno in tehnično verjetnih scenarijev, ki se še niso zgodili in, če je primerno, po spremembah sistemov in procesov. Ponudniki plačilnih storitev bi se morali med vzpostavitvijo načrta neprekinjenega poslovanja posvetovati in uskladiti z ustreznimi notranjimi in zunanjimi deležniki.

6.8 Testiranje načrta neprekinjenega poslovanja bi moralo:

a) vključevati ustrezen sklop scenarijev, kot je navedeno v smernici 6.4;

b) biti zasnovano tako, da preveri predpostavke, na katerih temeljijo načrti neprekinjenega poslovanja, vključno z ureditvami upravljanja in načrti kriznega obveščanja; in

c) vključevati postopke za preverjanje zmožnosti zaposlenega osebja in procesov, da se ustrezno odzovejo na zgoraj navedene scenarije.

6.9 Ponudniki plačilnih storitev bi morali redno spremljati učinkovitost svojih načrtov neprekinjenega poslovanja ter dokumentirati in analizirati vse izzive ali napake, ki nastanejo na podlagi testiranj.

Krizno obveščanje

6.10 V primeru motnje ali izrednih razmer in med izvajanjem načrtov neprekinjenega poslovanja bi morali ponudniki plačilnih storitev zagotoviti, da imajo na voljo učinkovite ukrepe za krizno obveščanje, tako da so vse ustrezne zainteresirane strani, vključno z zunanjimi ponudniki storitev, pravočasno in ustrezno obveščeni.

Smernica 7: Testiranje varnostnih ukrepov

7.1 Ponudniki plačilnih storitev bi morali vzpostaviti in izvajati okvir za testiranje, ki ocenjuje stabilnost in učinkovitost varnostnih ukrepov, ter zagotoviti, da je okvir za testiranje prilagojen tako, da upošteva nove grožnje in ranljivosti, ugotovljene na podlagi dejavnosti spremljanja tveganj.

7.2 Ponudniki plačilnih storitev bi morali zagotoviti, da se testi izvajajo v primeru sprememb infrastrukture, procesov ali postopkov in kadar so spremembe posledica večjih operativnih ali varnostnih incidentov.

7.3 Okvir testiranja bi moral zajeti tudi varnostne ukrepe, ki so povezani s (i) plačilnimi terminali in napravami, ki se uporabljajo za opravljanje plačilnih storitev, (ii) plačilnimi terminali in napravami, ki se uporabljajo za preverjanje pristnosti uporabnika plačilnih storitev in (iii) napravami in programsko opremo, ki jo ponudnik plačilnih storitev zagotovi uporabniku plačilnih storitev zaradi generiranja/prejema kode za preverjanje pristnosti.

7.4 Okvir testiranja bi moral zagotoviti naslednje:

a) da se testi izvajajo v okviru formalnega postopka za upravljanje sprememb ponudnika plačilnih storitev, ki bi moral zagotavljati njihovo temeljitost in učinkovitost;

b) da teste izvajajo neodvisni izvajalci testiranja, ki imajo ustrezno znanje, veščine in izkušnje za testiranje varnostnih ukrepov za plačilne storitve in ne sodelujejo pri razvoju varnostnih ukrepov za ustrezne plačilne storitve ali sisteme, ki naj se testirajo, in sicer vsaj za končne teste pred začetkom izvajanja varnostnih ukrepov; in

c) da testi vključujejo preverjanje ranljivosti in preskuse vdora, ki ustrezajo stopnji tveganja, povezani s plačilnimi storitvami.

7.5 Ponudniki plačilnih storitev bi morali za svoje plačilne storitve opravljati stalne in ponavljajoče se teste varnostnih ukrepov. Za sisteme, ki so ključnega pomena za opravljanje plačilnih storitev (kot je opisano v smernici 3.2), bi bilo treba testiranje opraviti vsaj enkrat letno. Manj pomembne sisteme bi bilo treba redno testirati na podlagi tveganju prilagojenega pristopa, vendar vsaj vsaka tri leta.

7.6 Ponudniki plačilnih storitev bi morali spremljati in ovrednotiti rezultate opravljenih testiranj ter v primeru ključnih sistemov ustrezno in nemudoma posodobiti svoje varnostne ukrepe.

Smernica 8: Zavedanje o razmerah in stalno izobraževanje

Razsežnost grožnje in zavedanje o razmerah

8.1 Ponudniki plačilnih storitev bi morali vzpostaviti organizacijsko strukturo in vzpostaviti ter izvajati procese za ugotavljanje in stalno spremljanje varnostnih in operativnih groženj, ki bi lahko pomembno vplivale na njihovo zmožnost opravljanja plačilnih storitev.

8.2 Ponudniki plačilnih storitev bi morali analizirati vse operativne ali varnostne incidente, ki so bili ugotovljeni ali so se pojavili v organizaciji in/ali zunaj nje. Ponudniki plačilnih storitev bi morali upoštevati ključne izkušnje, pridobljene na podlagi teh analiz, in varnostne ukrepe ustrezno posodobiti.

8.3 Ponudniki plačilnih storitev bi morali aktivno spremljati tehnološki razvoj za zagotovitev, da upošteva varnostna tveganja.

Programi usposabljanja in osveščanje glede varnosti

8.4 Ponudniki plačilnih storitev bi morali vzpostaviti program usposabljanja za vse zaposlene, da bi zagotovili, da so usposobljeni za izvajanje svojih nalog in odgovornosti v skladu z ustreznimi varnostnimi politikami in postopki, z namenom zmanjšati človeške napake, kraje, goljufije, nepravilno uporabo ali izgubo. Ponudniki plačilnih storitev bi morali zagotoviti, da je program usposabljanja članom osebja na voljo vsaj enkrat letno in po potrebi pogosteje.

8.5 Ponudniki plačilnih storitev bi morali zagotoviti, da je članom osebja, ki izvajajo ključne vloge, opredeljene v smernici 3.1, zagotovljeno ciljno usposabljanje na področju varnosti informacij na letni osnovi in po potrebi pogosteje.

8.6 Ponudniki plačilnih storitev bi morali vzpostaviti in izvajati redne programe osveščanja glede varnosti z namenom izobraževanja osebja in odzivanja na tveganja, povezana z varnostjo informacij. Ti programi bi morali od osebja ponudnika plačilnih storitev zahtevati, da sporočajo vse neobičajne dejavnosti in incidente.

Smernica 9: Upravljanje odnosov z uporabniki plačilnih storitev

Zavedanje uporabnika plačilnih storitev o varnostnih tveganjih in ukrepih za ublažitev tveganja

9.1 Ponudniki plačilnih storitev bi morali vzpostaviti in izvajati procese za povečanje zavedanja uporabnikov plačilnih storitev o varnostnih tveganjih v povezavi s plačilnimi storitvami in sicer tako, da jim zagotovijo pomoč in smernice.

9.2 Pomoč in smernice, ki so na voljo uporabnikom plačilnih storitev, bi bilo treba posodabljati glede na nove pojavljajoče se grožnje in ranljivosti, spremembe pa sporočati uporabnikom plačilnih storitev.

9.3 Ponudniki plačilnih storitev bi morali, če to dovoljuje funkcionalnost produkta, uporabnikom plačilnih storitev dovoliti, da onemogočijo nekatere plačilne funkcionalnosti, povezane s plačilnimi storitvami, ki jih ponudnik plačilnih storitev ponuja uporabnikom plačilnih storitev.

9.4 Če se je ponudnik plačilnih storitev v skladu s členom 68(1) Direktive (EU) 2015/2366 s plačnikom dogovoril o omejitvah porabe za plačilne transakcije, izvršene prek določenih plačilnih instrumentov, bi moral ponudnik plačilnih storitev plačniku zagotoviti možnost, da prilagodi te omejitve do najvišje dogovorjene omejitve.

9.5 Ponudniki plačilnih storitev bi morali uporabnikom plačilnih storitev zagotoviti možnost, da prejmejo opozorilo o začetih in/ali neuspelih poskusih izvedbe plačilnih transakcij ter jim omogočiti, da lahko sami zaznajo goljufivo ali škodljivo uporabo njihovih računov.

9.6 Ponudniki plačilnih storitev bi morali uporabnike plačilnih storitev obveščati o posodobitvah in varnostnih postopkih, ki vplivajo na uporabnike plačilnih storitev v smislu zagotavljanja plačilnih storitev.

9.7 Ponudniki plačilnih storitev bi morali uporabnikom plačilnih storitev zagotoviti pomoč v zvezi z vsemi vprašanji, zahtevami za podporo in obvestili o nepravilnostih ali zadevami, ki se nanašajo na

varnost v zvezi s plačilnimi storitvami. Uporabniki plačilnih storitev bi morali biti ustrezno obveščeni o tem, kako lahko pridobijo takšno pomoč.