EBA/GL/2017/17

12/01/2018

Smjernice

o sigurnosnim mjerama za operativne i sigurnosne rizike povezane s platnim uslugama na temelju Direktive (EU) 2015/2366 (Direktiva PSD2)

1. Obveze usklađivanja i izvješćivanja

Status ovih smjernica

1. Ovaj dokument sadrži smjernice izdane na temelju članka 16. Uredbe (EU) br. 1093/2010[1]. U skladu s člankom 16. stavkom 3. Uredbe (EU) br. 1093/2010 nadležna tijela i financijske institucije moraju ulagati napore da se usklade s ovim smjernicama.

2. Smjernice iznose EBA-ino stajalište o odgovarajućim nadzornim praksama unutar Europskog sustava financijskog nadzora ili o tome kako bi se pravo Unije trebalo primjenjivati u određenom području. Nadležna tijela određena člankom 4. stavkom 2. Uredbe (EU) br. 1093/2010 na koja se smjernice primjenjuju trebala bi se s njima uskladiti tako da ih na odgovarajući način uključe u svoje prakse (npr. izmjenama svojeg pravnog okvira ili nadzornih postupaka), uključujući i u slučajevima kada su smjernice prvenstveno upućene institucijama.

Zahtjevi za izvješćivanje

3. U skladu s člankom 16. stavkom 3. Uredbe (EU) 1093/2010 nadležna tijela moraju obavijestiti EBA-u o tome jesu li usklađena ili se namjeravaju uskladiti s ovim smjernicama, odnosno o razlozima neusklađenosti do 12.03.2018. U slučaju izostanka takve obavijesti unutar ovog roka EBA će smatrati da nadležna tijela nisu usklađena. Obavijesti se dostavljaju slanjem ispunjenog obrasca koji se nalazi na internetskoj stranici EBA-e na adresu compliance@eba.europa.eu s uputom „EBA/GL/2017/17“ . Obavijesti bi trebale slati osobe s odgovarajućom nadležnošću za izvješćivanje o usklađenosti u ime svojih nadležnih tijela. Svaka se promjena statusa usklađenosti također mora prijaviti EBA-i.

4. Obavijesti će biti objavljene na EBA-inoj internetskoj stranici u skladu s člankom 16. stavkom 3.

[1] Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ, (SL L 331, 15.12.2010., str. 12.).

2. Predmet, područje primjene i definicije

Predmet i područje primjene

5. Smjernice su pripremljene na temelju obveze EBA-e iz članka 95. stavka 3. Direktive (EU) 2015/2366[2] (Direktiva PSD2).

6. Ovim se smjernicama određuju zahtjevi za utvrđivanje, provedbu i praćenje sigurnosnih mjera koje pružatelji platnih usluga moraju poduzeti, u skladu s člankom 95. stavkom 1. Direktive (EU) 2015/2366, radi upravljanja operativnim i sigurnosnim rizicima povezanima s platnim uslugama koje pružaju.

Adresati

7. Ove su smjernice upućene pružateljima platnih usluga kako je definirano u članku 4. stavku 11. Direktive (EU) 2015/2366 i kako je navedeno u definiciji „financijskih institucija" u članku 4. stavku 1. Uredbe (EU) br. 1093/2010 te nadležnim tijelima kako je definirano u članku 4. stavku 2. točki i. te Uredbe upućivanjem na Direktivu 2007/64/EZ stavljenu izvan snage [3] (sadašnja Direktiva (EU) 2015/2366[4]).

Definicije

8. Osim ako je drugačije navedeno, pojmovi upotrijebljeni i utvrđeni u Direktivi (EU) 2015/2366 imaju isto značenje u ovim smjernicama. Osim toga, za potrebe ovih smjernica primjenjuju se sljedeće definicije:

Upravljačko tijelo	–	za pružatelje platnih usluga koji su kreditne institucije ovaj pojam ima isto značenje kao i iz definicije iz članka 3. stavka 1. točke 7. Direktive 2013/36/EU[5],

[2] Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ (SL L 337, 23. 12. 2015., str. 35.).

[3] Direktiva 2007/64/EZ Europskog parlamenta i Vijeća od 13. studenoga 2007. o platnim uslugama na unutarnjem tržištu i o izmjeni direktiva 97/7/EZ, 2002/65/EZ, 2005/60/EZ i 2006/48/EZ te stavljanju izvan snage Direktive 97/5/EZ (SL L 319, 5. 12. 2007., str. 1.).

[4] U skladu s drugim podstavkom članka 114. Direktive (EU) 2015/2366, sva upućivanja na Direktivu 2007/64/EZ stavljenu izvan snage smatraju se upućivanjima na Direktivu (EU) 2015/2366 i čitaju se u skladu s korelacijskom tablicom iz Priloga II. Direktivi (EU) 2015/2366.

[5] Direktiva 2013/36/EU Europskog parlamenta i Vijeća o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicijskim društvima, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ (SL L 176, 27. 6. 2013., str. 338.).

	– za pružatelje platnih usluga koji su institucije za platni promet ili institucije za elektronički novac ovaj pojam znači direktore ili osobe odgovorne za upravljanje pružateljem platnih usluga i, gdje je to primjenjivo, osobe odgovorne za upravljanje aktivnostima platnih usluga pružatelja platnih usluga, – za pružatelje platnih usluga navedene u članku 1. stavku 1. točkama (c), (e) i (f) Direktive (EU) 2015/2366 ovaj pojam ima značenje koje mu je dodijeljeno primjenjivim pravom EU-a ili nacionalnim pravom.
Operativni ili sigurnosni incident	Jedan događaj ili niz povezanih događaja koje pružatelj platnih usluga nije planirao, a koji imaju ili će vjerojatno imati negativan učinak na cjelovitost, dostupnost, povjerljivost, autentičnost ili kontinuitet usluga povezanih s plaćanjem.
Više rukovodstvo	(a) za pružatelje platnih usluga koji su kreditne institucije ovaj pojam ima isto značenje kao i iz definicije iz članka 3. stavka 1. točke 9. Direktive 2013/36/EU; (b) za pružatelje platnih usluga koji su institucije za platni promet ili institucije za elektronički novac ovaj pojam znači fizičke osobe koje obavljaju izvršne funkcije unutar institucije, a koje su odgovorne i odgovaraju upravljačkom tijelu za svakodnevno upravljanje pružateljem platnih usluga; (c) za pružatelje platnih usluga navedene u članku 1. stavku 1. točkama (c), (e) i (f) Direktive (EU) 2015/2366 ovaj pojam ima značenje koje mu je dodijeljeno primjenjivim pravom EU-a ili nacionalnim pravom.
Sigurnosni rizik	Rizik koji proizlazi iz neprikladnih ili neuspjelih unutarnjih procesa ili vanjskih događaja koji imaju ili mogu imati negativan učinak na dostupnost, cjelovitost ili povjerljivost sustava informacijskih i komunikacijskih tehnologija (IKT) ili informacija koje se upotrebljavaju za pružanje platnih usluga. To uključuje rizik od kibernapada ili rizik koji proizlazi iz neprikladne fizičke sigurnosti.
Sklonost preuzimanju rizika	Ukupna razina i vrste rizika koje je institucija spremna preuzeti u sklopu svoje sposobnosti podnošenja rizika, u skladu sa svojim poslovnim modelom, kako bi ostvarila svoje strateške ciljeve.

3. Provedba

Datum primjene

9. Ove smjernice primjenjuju se od 13. siječnja 2018.

4. Smjernice

Smjernica 1: Opća načela

1.1 Svi pružatelji platnih usluga trebali bi se uskladiti sa svim odredbama utvrđenima u ovim smjernicama. Razina detalja trebala bi biti razmjerna veličini pružatelja platnih usluga te prirodi, opsegu, složenosti i rizičnosti pojedinih usluga koje pružatelj platnih usluga pruža ili namjerava pružati.

Smjernica 2: Upravljanje

Okvir za upravljanje operativnim i sigurnosnim rizicima

2.1 Pružatelji platnih usluga trebali bi utvrditi učinkovit okvir za upravljanje operativnim i sigurnosnim rizicima (dalje u tekstu: „okvir za upravljanje rizicima”) koji bi upravljačko tijelo, a prema potrebi i više rukovodstvo, trebalo odobriti i preispitati barem jednom godišnje. Taj bi okvir trebao biti usmjeren na sigurnosne mjere za smanjivanje operativnih i sigurnosnih rizika te bi u potpunosti trebao biti ugrađen u cjelokupne procese upravljanja rizicima pružatelja platnih usluga.

2.2 Okvir za upravljanje rizicima trebao bi:

a) sadržavati sveobuhvatan dokument o sigurnosnoj politici kako je navedeno u članku 5. stavku 1. točki (j) Direktive (EU) 2015/2366;

b) biti dosljedan u preuzimanju rizika pružatelja platnih usluga;

c) utvrditi i dodijeliti ključne uloge i odgovornosti kao i odgovarajuće linije izvješćivanja potrebne za provođenje sigurnosnih mjera i upravljanje sigurnosnim i operativnim rizicima;

d) uspostaviti neophodne postupke i sustave za utvrđivanje, mjerenje, praćenje i upravljanje nizom rizika koji proizlaze iz aktivnosti pružatelja platnih usluga povezanih s plaćanjem, a kojima je pružatelj platnih usluga izložen, uključujući mehanizme kontinuiteta poslovanja.

2.3 Pružatelji platnih usluga trebali bi osigurati da okvir za upravljanje rizicima bude ispravno dokumentiran te da ga se tijekom njegove provedbe i praćenja ažurira na temelju dokumentiranih „stečenih iskustava”.

2.4 Pružatelji platnih usluga trebali bi osigurati da prije velike promjene infrastrukture, procesa ili postupaka te nakon svakog značajnog operativnog ili sigurnosnog incidenta koji utječe na sigurnost platnih usluga koje pružaju bez nepotrebne odgode preispitaju postoji li potreba za promjenama ili poboljšanjima unutar okvira za upravljanje rizicima.

Modeli za upravljanje rizicima i kontrolu

2.5 Pružatelji platnih usluga trebali bi uspostaviti tri učinkovite linije obrane ili odgovarajući unutarnji model upravljanja rizicima i kontrolu, radi utvrđivanja operativnih i sigurnosnih rizika te upravljanja njima. Pružatelji platnih usluga trebali bi osigurati da prethodno navedeni model za unutarnju kontrolu ima dostatne ovlasti, neovisnost, resurse i izravne linije izvješćivanja prema upravljačkom tijelu i, prema potrebi, višem rukovodstvu.

2.6 Revizije sigurnosnih mjera utvrđenih ovim smjernicama trebali bi obavljati revizori sa stručnim znanjem u području informatičke sigurnosti i plaćanja koji su operativno neovisni unutar pružatelja platnih usluga ili od njega. Pri određivanju učestalosti i usmjerenja tih revizija u obzir bi se trebali uzeti odgovarajući sigurnosni rizici.

Eksternalizacija poslova

2.7 Pružatelji platnih usluga trebali bi osigurati učinkovitost sigurnosnih mjera utvrđenih ovim smjernicama u slučaju eksternalizacije operativnih funkcija platnih usluga, uključujući eksternalizaciju informatičkih sustava.

2.8 Pružatelji platnih usluga trebali bi osigurati da su u ugovore i sporazume o razini usluga s pružateljima usluga kojima su eksternalizirali te funkcije ugrađeni primjereni i razmjerni sigurnosni ciljevi, mjere i željene karakteristike izvedbe. Pružatelji platnih usluga trebali bi pratiti razinu usklađenosti tih pružatelja usluga sa sigurnosnim ciljevima, mjerama i željenim karakteristikama izvedbe te tražiti jamstva u pogledu te usklađenosti.

Smjernica 3: Procjena rizika

Utvrđivanje funkcija, procesa i sredstava

3.1 Pružatelji platnih usluga trebali bi utvrditi, uspostaviti i redovito ažurirati popis svojih poslovnih funkcija, ključnih uloga i procesa za podršku kako bi izradili pregled važnosti svake funkcije, uloge i procesa za podršku te njihovih međuovisnosti povezanih s operativnim i sigurnosnim rizicima.

3.2 Pružatelji platnih usluga trebali bi utvrditi, uspostaviti i redovito ažurirati popis informacijskih sredstava kao što su sustavi IKT-a, njihove konfiguracije i ostale infrastrukture, a i međusobne povezanosti s drugim unutarnjim i vanjskim sustavima, kako bi mogli upravljati sredstvima koja podržavaju njihove ključne poslovne funkcije i procese.

Klasifikacija funkcija, procesa i sredstava

3.3 Pružatelji platnih usluga trebali bi klasificirati utvrđene poslovne funkcije, procese za podršku i informacijska sredstva prema njihovoj kritičnosti.

Procjena rizika u pogledu funkcija, procesa i sredstava

3.4 Pružatelji platnih usluga trebali bi osigurati stalno praćenje prijetnji i ranjivosti te redovito preispitivati scenarije rizika koji utječu na njihove poslovne funkcije, kritične procese i informacijska sredstva. Kao dio obveze da provode i dostavljaju nadležnim tijelima ažurirane i sveobuhvatne procjene operativnih i sigurnosnih rizika povezanih s platnim uslugama koje pružaju i o primjerenosti mjera za smanjenje rizika i kontrolnim mehanizmima koji se provode kao odgovor na te rizike, kako je propisano u članku 95. stavku 2. Direktive (EU) 2015/2366, pružatelji platnih usluga trebali bi jednom godišnje ili u kraćim vremenskim razmacima koje utvrdi nadležno tijelo provesti i dokumentirati procjene rizika povezanih s funkcijama, procesima i informacijskim sredstvima koje su utvrdili i klasificirali kako bi se utvrdili i procijenili ključni operativni i sigurnosni rizici. Takve procjene rizika trebale bi se provesti i prije uvođenja bilo kakve velike promjene u infrastrukturi, procesu ili postupcima koji utječu na sigurnost platnih usluga.

3.5 Na temelju tih procjena rizika pružatelji platnih usluga trebali bi utvrditi jesu li, i u kojoj mjeri, potrebne promjene u pogledu postojećih sigurnosnih mjera, tehnologija koje se upotrebljavaju i postupaka ili platnih usluga koje se nude. Pružatelji platnih usluga trebali bi u obzir uzeti vrijeme potrebno za provođenje tih promjena i vrijeme potrebno za poduzimanje primjerenih privremenih sigurnosnih mjera kako bi se pojave operativnih ili sigurnosnih incidenata, prijevara i potencijalnih negativnih učinaka u pružanju platnih usluga svele na najmanju moguću mjeru.

Smjernica 4: Zaštita

4.1 Pružatelji platnih usluga trebali bi uspostaviti i provesti preventivne sigurnosne mjere za zaštitu od utvrđenih operativnih i sigurnosnih rizika. Tim bi se mjerama trebala osigurati primjerena razina sigurnosti u skladu s utvrđenim rizicima.

4.2 Pružatelji platnih usluga trebali bi uspostaviti i provesti pristup „dubinske obrane" uvođenjem višeslojnih kontrola kojima se obuhvaćaju osobe, procesi i tehnologija pri čemu svaki pojedini sloj služi kao sigurnosna zaštita za prethodne slojeve. Dubinsku obranu trebalo bi shvatiti tako da se njome utvrđuje više od jedne kontrole kojom se obuhvaća isti rizik, kao što su načelo „četiri oka", autentifikacija na temelju dvaju elemenata, segmentacija mreže i višestruki vatrozidi.

4.3 Pružatelji platnih usluga trebali bi osigurati povjerljivost, cjelovitost i dostupnost svojih kritičnih logičkih i fizičkih sredstava, resursa i osjetljivih podataka o plaćanju svojih korisnika platnih usluga bez obzira na to jesu li oni u mirovanju, prijenosu ili upotrebi. Ako ti podatci sadržavaju osobne podatke, te bi se mjere trebale provoditi u skladu s Uredbom (EU) br. 2016/679[6] ili, ako je primjenjivo, Uredbom (EZ) br. 45/2001[7]

[6] Uredba (EU) Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4. 5. 2016., str. 1.).

[7] Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka (SL L 8, 12. 1. 2001., str. 1.).

4.4 Pružatelji platnih usluga trebali bi kontinuirano utvrđivati utječu li promjene u postojećem operativnom okruženju na postojeće sigurnosne mjere i je li potrebno donošenje daljnjih mjera kako bi se smanjio povezani rizik. Te promjene trebale bi biti dio formalnog procesa upravljanja promjenama pružatelja platnih usluga kojim bi se trebalo osigurati da se promjene propisno planiraju, testiraju i dokumentiraju te da za njih postoji propisno ovlaštenje. Na temelju uočenih sigurnosnih prijetnji i uvedenih promjena trebalo bi provesti testiranje koje uključuje scenarije relevantnih i poznatih potencijalnih napada.

4.5 Pružatelji platnih usluga trebali bi pri izradi, razvoju i pružanju platnih usluga osigurati primjenu načela razdvajanja dužnosti i „najmanjih ovlasti". Pružatelji platnih usluga trebali bi posvećivati posebnu pozornost razdvajanju informatičkih okruženja, osobito okruženja za razvoj, testiranje i produkciju.

Cjelovitost i povjerljivost podataka i sustavā

4.6 Pružatelji platnih usluga trebali bi, pri izradi, razvoju i pružanju platnih usluga, osigurati da prikupljanje, usmjeravanje, obrada, pohranjivanje ili arhiviranje i vizualizacija osjetljivih podataka o plaćanju korisnika platnih usluga budu primjereni, relevantni i ograničeni na ono što je nužno za pružanje njihovih platnih usluga.

4.7 Pružatelji platnih usluga trebali bi redovito provjeravati da je softver koji se upotrebljava za pružanje platnih usluga, uključujući korisnički softver povezan s plaćanjem, ažuriran te da se primjenjuju kritične sigurnosne ispravke. Pružatelji platnih usluga trebali bi osigurati da postoje mehanizmi za provjeru cjelovitosti kako bi se verificirala cjelovitost softvera, ugrađenih programa i informacija u pogledu njihovih platnih usluga.

Fizička sigurnost

4.8 Pružatelji platnih usluga trebali bi provoditi primjerene mjere za fizičku sigurnost, osobito kako bi zaštitili osjetljive podatke o plaćanju korisnikā platnih usluga te sustave IKT-a koji se upotrebljavaju za pružanje platnih usluga.

Kontrola pristupa

4.9 Fizički i logički pristup sustavima IKT-a trebao bi biti dozvoljen samo ovlaštenim osobama. Ovlaštenja bi trebalo dodjeljivati u skladu sa zadatcima i odgovornostima zaposlenika te bi ona trebala biti ograničena na osobe koje su primjereno osposobljene i koje se primjereno nadzire. Pružatelji platnih usluga trebali bi uvesti kontrole kojima se takav pristup sustavima IKT-a pouzdano ograničava na osobe s opravdanim poslovnim potrebama. Elektronički pristup podatcima i sustavima preko aplikacija trebao bi biti ograničen na najmanju moguću mjeru koja je potrebna za pružanje odgovarajuće usluge.

4.10 Pružatelji platnih usluga trebali bi uvesti jake kontrole u pogledu povlaštenog pristupa sustavu tako da strogo ograničavaju i pomno nadziru zaposlenike s pravom povlaštenog pristupa sustavu. Trebalo bi uvesti kontrole kao što su pristup temeljen na ulogama, bilježenje i pregled aktivnosti

povlaštenih korisnika u sustavima, pouzdana autentifikacija i praćenje neuobičajenih pojava. Pružatelji platnih usluga trebali bi upravljati pravima pristupa informacijskim sredstvima i njihovim sustavima za podršku na temelju načela „nužnosti uvida”. Prava pristupa trebalo bi povremeno preispitivati.

4.11 Evidencije pristupa trebalo bi čuvati tijekom razdoblja koje je razmjerno kritičnosti utvrđenih poslovnih funkcija, procesa za podršku i informacijskih sredstava, u skladu sa smjernicama 3.1. i 3.2. i ne dovodeći u pitanje zahtjeve u pogledu čuvanja podataka utvrđene pravom EU-a i nacionalnim pravom. Pružatelji platnih usluga te bi informacije trebali upotrebljavati radi olakšavanja utvrđivanja i istraživanja neuobičajenih aktivnosti koje su otkrivene tijekom pružanja platnih usluga.

4.12 Kako bi se osigurala sigurna komunikacija i smanjili rizici, administrativni pristup na daljinu kritičnim dijelovima IKT-a trebalo bi odobravati samo na temelju načela nužnosti uvida i uz uvjet primjene rješenja koja koriste pouzdanu autentifikaciju.

4.13 Funkcioniranje proizvoda, alata i postupaka povezanih s procesima kontrole pristupa trebalo bi štititi procese kontrole pristupa od njihova ugrožavanja ili zaobilaženja. To uključuje uvrštavanje, isporuku, opoziv i povlačenje odgovarajućih proizvoda, alata i postupaka.

Smjernica 5: Otkrivanje

Stalno praćenje i otkrivanje

5.1 Pružatelji platnih usluga trebali bi uspostaviti i provesti procese i mogućnosti za stalno praćenje poslovnih funkcija, procesa za podršku i informacijskih sredstava radi otkrivanja neuobičajenih aktivnosti tijekom pružanja platnih usluga. Kao dio tog stalnog praćenja, pružatelji platnih usluga trebali bi imati uspostavljene primjerene i učinkovite mogućnosti za otkrivanje fizičkih ili logičkih narušavanja sigurnosti te povreda povjerljivosti, cjelovitosti i dostupnosti informacijskih sredstava koja se upotrebljavaju u pružanju platnih usluga.

5.2 Procesima stalnog praćenja i otkrivanja trebalo bi obuhvatiti:

a) relevantne unutarnje i vanjske čimbenike, uključujući poslovne funkcije i administrativne funkcije IKT-a;

b) transakcije radi otkrivanja zlouporaba pristupa koje su počinili pružatelji usluga ili drugi subjekti i

c) potencijalne unutarnje i vanjske prijetnje.

5.3 Pružatelji platnih usluga trebali bi provesti mjere za otkrivanje mogućeg curenja informacija, zlonamjernog softvera i drugih sigurnosnih prijetnji te javno poznatih ranjivosti softvera i hardvera te provjeravati odgovarajuća nova sigurnosna ažuriranja softvera.

Praćenje i izvješćivanje s obzirom na operativne ili sigurnosne incidente

5.4 Pružatelji platnih usluga trebali bi odrediti primjerene kriterije i pragove za klasifikaciju događaja kao operativnog ili sigurnosnog incidenta, kako je navedeno u odjeljku „Definicije" ovih smjernica, te rane pokazatelje opasnosti koji bi trebali služiti kao upozorenje pružatelju platnih usluga kako bi se omogućilo rano otkrivanje operativnih ili sigurnosnih incidenata.

5.5 Pružatelji platnih usluga trebali bi uspostaviti primjerene procese i organizacijske strukture radi osiguravanja dosljednog i cjelovitog praćenja operativnih ili sigurnosnih incidenata, postupanja s njima te njihova daljnjeg praćenja.

5.6 Pružatelji platnih usluga trebali bi uspostaviti postupak za prijavljivanje takvih operativnih ili sigurnosnih incidenata te pritužbi korisnika povezanih sa sigurnošću svojem višem rukovodstvu.

Smjernica 6: Kontinuitet poslovanja

6.1 Pružatelji platnih usluga trebali bi uspostaviti dobro upravljanje kontinuitetom poslovanja kako bi u najvećoj mogućoj mjeri osigurali sposobnost neprekidnog pružanja platnih usluga i kako bi ograničili gubitke u slučaju znatnijeg prekida poslovanja.

6.2 Kako bi uspostavili dobro upravljanje kontinuitetom poslovanja, pružatelji platnih usluga trebali bi pažljivo analizirati svoju izloženost znatnijim prekidima poslovanja i procijeniti, kvantitativno i kvalitativno, njihov potencijalni učinak primjenom unutarnje ili vanjske analize podataka i scenarija. Na temelju utvrđenih i klasificiranih kritičnih funkcija, procesa, sustava, transakcija i međuovisnosti u skladu sa smjernicama 3.1. – 3.3. pružatelji platnih usluga trebali bi dati prednost aktivnostima kontinuiteta poslovanja uz primjenu pristupa koji se temelji na riziku, a koje se mogu temeljiti na procjenama rizika provedenima na temelju smjernice 3. Time se, ovisno o poslovnom modelu pružatelja platnih usluga, može, primjerice, olakšati daljnja obrada kritičnih transakcija uz istodobno provođenje korektivnih mjera.

6.3 Na osnovi analize provedene na temelju smjernice 6.2., pružatelj platnih usluga trebao bi uspostaviti:

a) planove kontinuiteta poslovanja kako bi osigurao da može primjereno reagirati u izvanrednim situacijama i da može održavati svoje kritične poslovne aktivnosti i

b) mjere ublažavanja koje će donijeti u slučaju prestanka pružanja svojih platnih usluga i otkaza postojećih ugovora, a kako bi izbjegao negativne učinke na platne sustave i na korisnike platnih usluga te osigurao izvršenje platnih transakcija koje su u tijeku.

Planiranje kontinuiteta poslovanja na temelju scenarija

6.4 Pružatelj platnih usluga trebao bi razmotriti niz različitih scenarija, uključujući ekstremne, ali moguće, scenarije, kojima bi mogao biti izložen te procijeniti potencijalni učinak koji bi ti scenariji mogli imati.

6.5 Na osnovi analize provedene na temelju smjernice 6.2. i mogućih scenarija utvrđenih na temelju smjernice 6.4., pružatelj platnih usluga trebao bi razviti planove za odgovor i oporavak koji bi trebali:

a) biti usmjereni na učinak na funkcioniranje kritičnih funkcija, procesa, sustava, transakcija i međuovisnosti;

b) biti dokumentirani i stavljeni na raspolaganje poslovnim jedinicama i jedinicama za podršku te lako dostupni u izvanrednim situacijama i

c) biti ažurirani u skladu s iskustvima stečenima na temelju testiranja, novih utvrđenih rizika i prijetnji te promijenjenih ciljeva i prioriteta oporavka.

Testiranje planova kontinuiteta poslovanja

6.6 Pružatelji platnih usluga trebali bi testirati svoje planove kontinuiteta poslovanja i osigurati da se funkcioniranje njihovih kritičnih funkcija, procesa, sustava, transakcija i međuovisnosti testira barem jednom godišnje. Tim planovima trebali bi se podržavati ciljevi za zaštitu i, prema potrebi, ponovnu uspostavu cjelovitosti i dostupnosti njihova poslovanja te povjerljivosti njihovih informacijskih sredstava.

6.7 Planovi bi se trebali ažurirati barem jednom godišnje, na temelju rezultata testiranja, postojećih informacija o prijetnjama, razmjene informacija i iskustva stečenog tijekom prijašnjih događaja te promjenjivih ciljeva oporavka kao i na temelju analize operativno i tehnički mogućih scenarija koji se još nisu dogodili te, ako je to relevantno, nakon promjena u sustavima i procesima. Pružatelji platnih usluga trebali bi se tijekom izrade svojih planova kontinuiteta poslovanja savjetovati s relevantnim unutarnjim i vanjskim dionicima te s njima koordinirati svoje djelovanje.

6.8 Testiranje planova kontinuiteta poslovanja pružateljā platnih usluga trebalo bi:

a) uključivati primjeren skup scenarija kako je navedeno u smjernici 6.4.;

b) biti osmišljeno tako da se njime preispituju pretpostavke na kojima se temelje planovi kontinuiteta poslovanja, uključujući sustave upravljanja i planove za komuniciranje u kriznim situacijama i

c) uključivati postupke za provjeru sposobnosti njihovih zaposlenika i procesa za primjeren odgovor na prethodno navedene scenarije.

6.9 Pružatelji platnih usluga trebali bi povremeno pratiti učinkovitost svojih planova kontinuiteta poslovanja te dokumentirati i analizirati sve probleme ili neuspjehe utvrđene na temelju tih testiranja.

Komuniciranje u kriznim situacijama

6.10 U slučaju prekida poslovanja ili izvanredne situacije, a tijekom provedbe planova kontinuiteta poslovanja, pružatelji platnih usluga trebali bi osigurati postojanje učinkovitih mjera za

komuniciranje u kriznim situacijama tako da svi relevantni unutarnji i vanjski dionici, uključujući vanjske pružatelje usluga, budu pravodobno i primjereno informirani.

Smjernica 7:Testiranje sigurnosnih mjera

7.1 Pružatelji platnih usluga trebali bi uspostaviti i provesti okvir za testiranje kojim se potvrđuje pouzdanost i učinkovitost sigurnosnih mjera te osigurati da je okvir za testiranje prilagođen tako da se njime mogu razmatrati nove prijetnje i ranjivosti utvrđene na temelju aktivnosti praćenja rizika.

7.2 Pružatelji platnih usluga trebali bi osigurati provođenje testiranja u slučaju promjena u infrastrukturi, procesima ili postupcima te u slučaju promjena koje su provedene kao posljedica značajnih operativnih ili sigurnosnih incidenata.

7.3 Okvirom za testiranje trebale bi se obuhvatiti i sigurnosne mjere relevantne za i. platne terminale i uređaje koji se upotrebljavaju za pružanje platnih usluga; ii. platne terminale i uređaje koji se upotrebljavaju za autentifikaciju korisnika platnih usluga; i iii. uređaje i softver koje korisnicima platnih usluga pruža pružatelj platnih usluga za izradu/primanje autentifikacijskog koda.

7.4 Okvirom za testiranje trebalo bi se osigurati:

a) da se testiranja provode kao dio formalnog procesa upravljanja promjenama pružatelja platnih usluga kako bi se osigurala njihova pouzdanost i učinkovitost;

b) da testiranja provode neovisni ispitivači s dostatnim znanjem, vještinama i stručnošću u testiranju sigurnosnih mjera za platne usluge, koji nisu uključeni u razvoj sigurnosnih mjera za odgovarajuće platne usluge ili sustave koje će se testirati, barem u pogledu konačnih testiranja prije početka primjene sigurnosnih mjera i

c) da testiranja uključuju ispitivanja ranjivosti i penetracijska testiranja koja su primjerena razini rizika utvrđenoj u pogledu platnih usluga.

7.5 Pružatelji platnih usluga trebali bi provoditi stalna i ponovljena testiranja sigurnosnih mjera za svoje platne usluge. Za sustave koji su kritični za pružanje njihovih platnih usluga (kako je opisano u smjernici 3.2.) ta testiranja provode se barem jednom godišnje. Sustavi koji nisu kritični trebali bi se redovito testirati primjenom pristupa koji se temelji na riziku barem jednom svake tri godine.

7.6 Pružatelji platnih usluga trebali bi pratiti i procjenjivati rezultate provedenih testiranja i u skladu s njima ažurirati svoje sigurnosne mjere, a u slučaju kritičnih sustava trebali bi to činiti bez neopravdane odgode.

Smjernica 8: Svijest o situaciji i kontinuirano učenje

Pregled prijetnji i svijest o situaciji

8.1 Pružatelji platnih usluga trebali bi uspostaviti i provesti procese i organizacijske strukture za utvrđivanje i stalno praćenje sigurnosnih i operativnih prijetnji koje bi mogle bitno utjecati na njihovu sposobnost pružanja platnih usluga.

8.2 Pružatelji platnih usluga trebali bi analizirati operativne ili sigurnosne incidente koji su utvrđeni ili su se dogodili unutar ili izvan organizacije. Pružatelji platnih usluga trebali bi razmotriti ključna iskustva stečena tim analizama i u skladu s njima ažurirati sigurnosne mjere.

8.3 Pružatelji platnih usluga trebali bi aktivno pratiti tehnološki razvoj kako bi osigurali da su svjesni sigurnosnih rizika.

Programi za osposobljavanje i podizanje svijesti o sigurnosti

8.4 Pružatelji platnih usluga trebali bi uspostaviti programe za osposobljavanje za sve zaposlenike kako bi osigurali da su osposobljeni za izvršavanje svojih dužnosti i odgovornosti u skladu s relevantnom sigurnosnom politikom i postupcima u cilju smanjenja ljudskih pogrešaka, krađa, prijevara, zlouporaba ili gubitaka. Pružatelji platnih usluga trebali bi osigurati da se programom za osposobljavanje osigurava osposobljavanje zaposlenika barem jednom godišnje, te češće ako je to potrebno.

8.5 Pružatelji platnih usluga trebali bi osigurati da se zaposlenicima koji obavljaju ključne uloge utvrđene na temelju smjernice 3.1. pruži ciljano osposobljavanje o informacijskoj sigurnosti jednom godišnje ili češće ako je to potrebno.

8.6 Pružatelji platnih usluga trebali bi uspostaviti i provoditi povremene programe podizanja svijesti o sigurnosti kako bi obrazovali svoje zaposlenike i razmotrili rizike povezane s informacijskom sigurnošću. Tim programima trebalo bi se zahtijevati da zaposlenici pružatelja platnih usluga prijave svaku neobičnu aktivnost i incidente.

Smjernica 9: Upravljanje odnosima s korisnicima platnih usluga

Podizanje svijesti korisnika platnih usluga o sigurnosnim rizicima i mjerama za smanjenje rizika

9.1 Pružatelji platnih usluga trebali bi uspostaviti i provoditi procese za jačanje svijesti korisnika platnih usluga o sigurnosnim rizicima povezanima s platnim uslugama osiguravanjem pomoći i smjernica korisnicima platnih usluga.

9.2 Pomoć i smjernice koje se nude korisnicima platnih usluga trebale bi se ažurirati s obzirom na nove prijetnje i ranjivosti, a o promjenama bi trebalo obavještavati korisnike platnih usluga.

9.3 Ako je to dopušteno u okviru funkcionalnosti proizvoda, pružatelji platnih usluga trebali bi dopustiti korisnicima platnih usluga da onemoguće određene platne funkcionalnosti povezane s platnim uslugama koje pružatelj platnih usluga pruža korisniku platnih usluga.

9.4 Ako je pružatelj platnih usluga u skladu s člankom 68. stavkom 1. Direktive (EU) 2015/2366, dogovorio s platiteljem ograničenje potrošnje za platne transakcije izvršene putem određenog platnog instrumenta, pružatelj platnih usluga trebao bi platitelju omogućiti da prilagođava ta ograničenja do iznosa najvišeg dogovorenog ograničenja.

9.5 Pružatelji platnih usluga trebali bi omogućiti da korisnici platnih usluga primaju upozorenja o iniciranju ili neuspjelim pokušajima iniciranja platnih transakcija čime im se omogućuje da otkriju prijevarno ili zlonamjerno korištenje njihovim računom.

9.6 Pružatelji platnih usluga trebali bi informirati korisnike platnih usluga o ažuriranjima sigurnosnih postupaka koji utječu na korisnike platnih usluga s obzirom na pružanje platnih usluga.

9.7 Pružatelji platnih usluga trebali bi korisnicima platnih usluga pružiti pomoć s obzirom na sva pitanja, zahtjeve za podršku i obavijesti o neuobičajenim pojavama ili problemima u pogledu sigurnosnih pitanja povezanih s platnim uslugama. Korisnici platnih usluga trebali bi biti primjereno informirani o tome kako je moguće dobiti tu pomoć.