EVROPSKA CENTRALNA BANKA

EUROSISTEM

PRIPOROČILA ZA VARNOST SPLETNIH PLAČIL

KONČNA RAZLIČICA PO JAVNEM POSVETOVANJU

1 SPLOŠNO

Poročilo vsebuje niz priporočil za izboljšanje varnosti spletnih plačil. Oblikoval jih je evropski forum za varnost plačil malih vrednosti, SecuRe Pay (v nadaljevanju: forum). Forum je bil ustanovljen leta 2011 kot pobuda za prostovoljno sodelovanje med organi. Njegov namen je zlasti med nadzorniki ponudnikov plačilnih storitev (PSP) in pregledniki zagotoviti splošno poznavanje in razumevanje zadev, povezanih z varnostjo elektronskih plačilnih storitev malih vrednosti in z instrumenti, ki jih zagotavljajo države članice Evropske unije (EU)/Evropskega gospodarskega prostora (EGP). Delo foruma se osredotoča na celotno verigo obdelave elektronskih plačilnih storitev malih vrednosti (brez čekov in gotovine) ne glede na plačilni kanal. Forum obravnava tista področja, na katerih se pokažejo večje šibke in ranljive točke, in, kjer je primerno, oblikuje priporočila. Končni cilj je spodbujati k temu, da se vzpostavi usklajena minimalna stopnja varnosti na ravni celotne EU/EGP. Organi, ki sodelujejo v prizadevanjih foruma, so našteti v prilogi.

Glede na trenutne izkušnje regulatornih organov, zakonodajalcev, PSP in širše javnosti, da je za spletna plačila značilna višja stopnja goljufij kot za tradicionalne načine plačevanja,[1] je forum sklenil oblikovati priporočila za varnost spletnih plačil. Iz teh so razvidne izkušnje preglednikov in nadzornikov v njihovih državah, upoštevajo pa povratne informacije, pridobljene v javni razpravi.[2]

Namen oblikovanja usklajenih evropskih priporočil za varnost spletnih plačil je prispevati k boju proti goljufijam pri plačilih in povečanju zaupanja strank v spletna plačila. Poročilo vsebuje tudi nekaj najboljših praks (NP) in spodbuja PSP, upravljavce plačilnih shem in druge udeležence na trgu, kot so spletni trgovci, naj jih privzamejo. Te najboljše prakse so pomembne, saj je varnost spletnih plačil odvisna od odgovornega vedenja vseh udeležencev.

PODROČJE UPORABE IN NASLOVNIKI

Če ni drugače navedeno, priporočila, ključni vidiki (KV) in najboljše prakse (NP) v tem poročilu veljajo za vse PSP, kot je opredeljeno v Direktivi o plačilnih storitvah,[3] ki zagotavljajo spletne plačilne storitve, in tudi za upravljavce plačilnih shem[4] (vključno s kartičnimi plačilnimi shemami, shemami kreditnih plačil, shemami direktnih obremenitev itd.). Namen tega poročila je opredeliti skupne minimalne zahteve za spodaj naštete spletne plačilne storitve ne glede na uporabljeno dostopno napravo:

---

[1] Javno dostopni podatki o goljufijah na ravni EU so trenutno omejeni, vendar pa so prevladujoča oblika goljufij pri plačilih po poročanju britanskega organa za spodbujanje sektorja finančnih storitev, zveze Financial Fraud Action UK in francoskega foruma za varnost plačilnih kartic *(Observatoire de la sécurité des cartes de paiement)* goljufije pri kartičnem poslovanju brez fizične prisotnosti kartice. Glej tudi poročilo Evropske centralne banke (2012), Poročilo o kartičnih goljufijah *(Report on card fraud), julij*.

[2] Javna razprava o osnutku priporočil je potekala od sredine aprila do junija 2012.

[3] Direktiva 2007/64/ES Evropskega parlamenta in Sveta z dne 13. novembra 2007 o plačilnih storitvah na notranjem trgu, ki spreminja direktive 97/7/ES, 2002/65/ES, 2005/60/ES in 2006/48/ES ter razveljavlja Direktivo 97/5/ES, UL L 319, 5.12.2007, str. 1.

[4] Upravljavec plačilne sheme je odgovoren za splošno delovanje sheme, ki podpira zadevni plačilni instrument, in zagotavlja, da vsi sodelujoči akterji upoštevajo pravila sheme. Poleg tega je odgovoren za zagotavljanje skladnosti sheme s standardi na področju pregleda. Evropska centralna banka (2009), Usklajen pristop in standardi za pregled plačilnih instrumentov *(Harmonised oversight approach and oversight standards for payment instruments)*, februar.

- [kartice] izvrševanje spletnih kartičnih plačil, vključno z virtualnimi kartičnimi plačili, in registracija podatkov o kartičnih plačilih za uporabo v storitvah »elektronske denarnice«;

- [kreditna plačila] izvrševanje spletnih kreditnih plačil;

- [e-pooblastilo] izdaja in sprememba elektronskih pooblastil za direktne obremenitve;

- [e-denar] prenosi elektronskega denarja med dvema računoma elektronskega denarja preko spleta.

Integratorji plačil[5], ki ponujajo storitve odrejanja plačil, se (lahko) obravnavajo kot pridobitelji spletnih plačilnih storitev (in s tem PSP) ali zunanji ponudniki tehničnih storitev za zadevne sheme. V zadnjem primeru bi morali biti integratorji plačil pogodbeno zavezani za izpolnjevanje priporočil.

S področja uporabe priporočil, ključnih vidikov in najboljših praks so izključeni:[6]

- druge spletne storitve, ki jih zagotavlja PSP prek svoje spletne strani za plačevanje (npr. e-borzno posredovanje, pogodbe, sklenjene prek spleta);

- plačila, pri katerih se navodila pošljejo po pošti, s telefonskim nalogom, glasovno pošto ali z uporabo tehnologije kratkih sporočil;

- mobilna plačila, ki ne temeljijo na brskalnikih;[7]

- kreditna plačila, pri katerih tretja stranka dostopa do plačilnega računa stranke;

- plačilne transakcije, izvedene s strani podjetij prek namenskih omrežij;

- kartična plačila z uporabo anonimnih fizičnih ali virtualnih predplačniških kartic, ki jih ni mogoče ponovno polniti, kadar ni trajnega sodelovanja med izdajateljem in imetnikom kartice;

- kliring in poravnava plačilnih transakcij.

VODILNA NAČELA

Priporočila temeljijo na štirih vodilnih načelih.

Prvič, PSP in upravljavci plačilnih shem bi morali izvesti posebne ocene tveganj, povezanih z zagotavljanjem spletnih plačilnih storitev, kar bi bilo treba redno posodabljati v skladu z razvojem groženj varnosti na spletu in mehanizmov goljufij. Nekatera tveganja na tem področju so odkrili že v preteklosti, na primer Banka za mednarodne poravnave leta 2003[8] ali Zvezni preiskovalni svet za finančne institucije (Federal Financial Institutions Examination Council) v letih 2005 in 2011.[9] Vendar je zaradi hitrega tehnološkega napredka in uvedbe novih načinov izvajanja spletnih plačil skupaj z dejstvom, da so postali goljufi bolj organizirani, njihovi napadi pa bolj izpopolnjeni, nadvse pomembno redno ocenjevanje zadevnih tveganj.

Drugič, veljati bi moralo splošno načelo, da morata biti odrejanje spletnih plačil in tudi dostop do občutljivih podatkov o plačilih zaščitena z močno avtentikacijo strank. Za namene tega poročila so občutljivi podatki o plačilih opredeljeni kot podatki, ki se lahko zlorabijo za goljufijo. Mednje spadajo podatki, ki omogočajo odreditev naloga za plačilo, podatki, ki se uporabljajo za avtentikacijo, podatki, ki se uporabljajo za naročanje plačilnih instrumentov, ali orodja za avtentikacijo, ki se pošljejo strankam, ter podatki, parametri in programska oprema, ki lahko, če jih spreminjamo, vplivajo na možnost legitimne stranke, da preveri plačilne transakcije,

[5] Integratorji plačil zagotavljajo prejemniku plačila (tj. spletnemu trgovcu) standardiziran vmesnik do storitev odreditve plačil, ki jih ponujajo PSP.

[6] Nekatere od teh zadev bodo lahko vključene v naknadno posebno poročilo.

[7] Posebna priporočila, namenjena izdaji in vzdrževanju programske opreme, bodo oblikovana v okviru ločene delovne skupine na področju mobilnih plačil.

[8] Banka za mednarodne poravnave (2003), Načela upravljanja tveganj za elektronsko bančništvo (*Risk Management Principles for Electronic Banking),* julij.

[9] Zvezni preiskovalni svet za finančne institucije (Federal Financial Institutions Examination Council) (2005), Preverjanje pristnosti v okolju internetnega bančništva (*Authentication in an Internet Banking Environment),* oktober. Glej tudi Dodatek k navodilom za leto 2005 *(Supplement to the 2005 guidance),* junij 2011.

odobri e-pooblastila ali nadzoruje račun, kot so »črne« in »bele« liste, omejitve, ki jih določi stranka, itd.

Močna avtentikacija stranke je postopek, ki temelji na uporabi dveh ali več naslednjih elementov – označeni so kot poznavanje, lastništvo in neločljiva povezava: i) nekaj, kar ve samo uporabnik, npr. statično geslo, koda, osebna identifikacijska številka; ii) nekaj, kar je v izključni lasti uporabnika, npr. žeton, pametna kartica, mobilni telefon; iii) nekaj, kar uporabnik je, npr. biometrična značilnost, kot je prstni odtis. Poleg tega morajo biti izbrani elementi vzajemno neodvisni, tj. kršitev enega ne vpliva na drugega oziroma druge. Najmanj en element bi moral biti tak, da ga ni mogoče ponovno uporabiti in reproducirati (z izjemo neločljive povezave) ter neopazno ukrasti prek spleta. Postopek močne avtentikacije bi moral biti zasnovan tako, da varuje zaupnost podatkov za avtentikacijo.

Forum meni, da PSP, ki nimajo postopkov avtentikacije ali imajo šibke postopke avtentikacije, pri sporni transakciji ne morejo dokazati, da je stranka odobrila transakcijo.

Tretjič, PSP bi morali izvajati učinkovite postopke za odobritev transakcij ter prav tako za spremljanje transakcij in sistemov, da bi lahko prepoznali neobičajne vzorce plačevanja pri strankah in preprečili goljufije.

In za konec, PSP in upravljavci plačilnih shem bi morali sodelovati v programih za ozaveščanje in izobraževanje strank o varnostnih vprašanjih v zvezi z uporabo spletnih plačilnih storitev, da bi strankam omogočili[10] varno in učinkovito uporabo tovrstnih storitev.

Priporočila so napisana čim bolj splošno, da bi veljala tudi v primeru stalnih tehnoloških inovacij, ob tem pa se forum zaveda, da se lahko kadar koli pojavijo nove grožnje, zato bo redno pregledoval ta priporočila.

Namen tega poročila ni, da se opredelijo posebne varnostne ali tehnične rešitve. Prav tako ne poskuša na novo opredeliti ali predlagati sprememb obstoječih industrijskih tehničnih standardov ali pričakovanj organov na področjih varstva podatkov in neprekinjenega poslovanja. Organi lahko pri ocenjevanju skladnosti z varnostnimi priporočili upoštevajo skladnost z ustreznimi mednarodnimi standardi. Kadar so v priporočilih navedene rešitve, se lahko enak rezultat doseže z drugimi sredstvi.

Priporočila v tem poročilu predstavljajo minimalna pričakovanja. Ne posegajo v odgovornost PSP, upravljavcev plačilnih shem in drugih udeležencev na trgu, da spremljajo in ocenjujejo tveganja, ki so povezana z njihovo dejavnostjo plačil, razvijajo lastne podrobne varnostne politike ter izvajajo ustrezne varnostne in izredne ukrepe ter ukrepe upravljanja z incidenti in ukrepe za neprekinjeno poslovanje, ki so sorazmerni s tveganji, neločljivo povezanimi z zagotovljenimi plačilnimi storitvami.

IZVAJANJE

Poročilo vsebuje 14 priporočil za večjo varnost spletnih plačil. Vsako priporočilo podrobno opišejo ključni vidiki (KV). Slednje je treba brati skupaj s priporočili, da bi tako v celoti razumeli, kakšna so najmanjša pričakovanja za izpolnjevanje varnostnih priporočil. S strani naslovnikov se pričakuje upoštevanje priporočil in KV, oziroma morajo biti na zahtevo ustreznega pristojnega organa zmožni pojasniti in utemeljiti morebitna odstopanja od njih (**načelo »upoštevaj ali pojasni«**). Poročilo opisuje tudi nekaj najboljših praks ter spodbuja PSP, upravljavce plačilnih shem in relevantne udeležence na trgu, naj jih privzamejo.

Pravno podlago za nacionalne organe za izvajanje priporočil zagotavljata domača zakonodaja, v katero je prenesena Direktiva o plačilnih storitvah, in/ali obstoječa pristojnost zadevnih organov za pregled in nadzor. Člani foruma so dolžni podpreti izvajanje priporočil v svojih jurisdikcijah in jih bodo vključili v obstoječe okvire za nadzor/pregled. Forum si bo tudi prizadeval, da zagotovi učinkovito in dosledno izvajanje v vseh jurisdikcijah, ter v ta namen lahko sodeluje z drugimi pristojnimi organi.

PSP in upravljavci plačilnih shem bi morali priporočila izvesti do 1. februarja 2015. Nacionalni organi lahko po potrebi določijo krajše prehodno obdobje.

[10] Med stranke spadajo potrošniki in podjetja, za katera se zagotavlja plačilna storitev.

KRATEK PREGLED POROČILA

Priporočila so urejena v tri skupine.

1. **Splošno kontrolno in varnostno okolje** platforme za podporo spletnih plačilnih storitev. PSP bi morali kot del svojih postopkov za upravljanje tveganj oceniti primernost svojih notranjih varnostnih ukrepov za primere notranjih in zunanjih scenarijev tveganj. Priporočila v prvem sklopu obravnavajo vprašanja v zvezi z upravljanjem, prepoznavanjem in ocenjevanjem tveganj, spremljanjem in poročanjem, nadzorom in zmanjševanjem tveganj ter sledljivostjo.

2. **Posebni kontrolni in varnostni ukrepi za spletna plačila.** Priporočila v drugem sklopu vsebujejo vse korake obdelave plačilne transakcije, od dostopa do storitve (podatki o stranki, prijava, možnosti avtentikacije) do odreditve plačila, nadzora in odobritve ter zaščite občutljivih podatkov o plačilu.

3. **Ozaveščanje, izobraževanje in obveščanje strank.** Priporočila v tretjem sklopu vključujejo zaščito strank, kaj morajo stranke storiti v primeru neželene zahteve po personaliziranih varnostnih poverilnicah, kako varno uporabljati spletne plačilne storitve, in nazadnje, kako lahko stranke preverijo, da se je transakcija začela izvajati in je bila izvršena.

Poročilo vsebuje tudi slovar nekaterih ključnih opredelitev. V prilogi so našteti člani foruma.

2 PRIPOROČILA

SPLOŠNO KONTROLNO IN VARNOSTNO OKOLJE

Priporočilo št. 1: Upravljanje

PSP in plačilne sheme bi morali izvajati in redno preverjati formalno varnostno politiko za spletne plačilne storitve.

1.1 KV Varnostna politika bi morala biti ustrezno dokumentirana, višje vodstvo pa bi jo moralo redno preverjati (v skladu s KV 2.4) in odobriti. V njej bi morali biti opredeljeni cilji v zvezi z varnostjo in dovzetnost za tveganje.

1.2 KV Varnostna politika bi morala opredeliti vloge in odgovornosti, vključno s funkcijo upravljanja tveganj, ki poroča neposredno ravni uprave, in linije poročanja za zadevne spletne plačilne storitve, vključno z upravljanjem občutljivih podatkov o plačilih, kar zadeva oceno, nadzor in zmanjševanje tveganj.

1.1 NP Varnostna politika bi lahko bila zapisana v posebnem dokumentu.

Priporočilo št. 2: Ocena tveganja

PSP in plačilne sheme bi morali izvajati in dokumentirati temeljita ocenjevanja tveganj v zvezi z varnostjo spletnih plačil in s tem povezanih storitev, in sicer pred samo uvedbo storitve oziroma storitev in naknadno na redni podlagi.

2.1 KV PSP in plačilne sheme bi morali prek svoje funkcije za upravljanje tveganj izvajati in dokumentirati podrobna ocenjevanja tveganj za spletna plačila in podobne storitve. PSP in plačilne sheme bi morali preučiti rezultate stalnega spremljanja groženj za varnost v zvezi s spletnimi plačilnimi storitvami, ki jih ponujajo ali nameravajo ponujati, ob upoštevanju: i) tehnoloških rešitev, ki jih uporabljajo; ii) storitev, ki jih zanje opravljajo zunanji ponudniki; in iii) tehničnega okolja strank. PSP in plačilne sheme bi morali preučiti tveganja, ki so povezana z izbranimi tehnološkimi platformami, arhitekturo aplikacij, programskimi tehnikami in rednimi

postopki, ki jih uporabljajo sami[11] in njihove stranke,[12] ter rezultate procesa spremljanja varnostnih incidentov (glej Priporočilo št. 3).

2.2 KV Na podlagi tega bi morali PSP in plačilne sheme določiti, ali in v kolikšni meri so morda potrebne spremembe obstoječih varnostnih ukrepov, tehnologij, ki se uporabljajo, ter razpoložljivih postopkov ali storitev. PSP in plačilne sheme bi morali upoštevati čas, ki je potreben za izvajanje sprememb (vključno z uvajanjem strank), in sprejeti ustrezne vmesne ukrepe za čim večje zmanjšanje varnostnih incidentov ter goljufij in morebitnih motečih učinkov.

2.3 KV Ocenjevanje tveganj bi moralo obravnavati potrebo po zaščiti in varstvu občutljivih podatkov o plačilih.

2.4 KV PSP in plačilne sheme bi morali preučiti scenarije tveganja in obstoječe varnostne ukrepe po večjih incidentih, ki vplivajo na njihove storitve, pred večjo spremembo infrastrukture ali postopkov, in kadar se v okviru spremljanja tveganj odkrijejo nove grožnje. Poleg tega bi bilo treba najmanj enkrat letno izvesti splošen pregled ocenjevanja tveganj.

Rezultate ocenjevanj tveganj in pregledov bi bilo treba predložiti višjemu vodstvu v odobritev.

Priporočilo št. 3: Spremljanje incidentov in poročanje o njih

PSP in plačilne sheme bi morali zagotavljati dosledno in celostno spremljanje in obravnavanje varnostnih incidentov ter nadaljnje ukrepe, vključno s pritožbami strank glede varnosti. PSP in plačilne sheme bi morali vzpostaviti postopek za poročanje o tovrstnih incidentih upravi, pri večjih varnostnih incidentih pa pristojnim organom.

3.1 KV PSP in plačilne sheme bi morali zagotoviti postopek za spremljanje in obravnavanje incidentov in pritožb strank v zvezi z varnostjo in tudi za nadaljnje ukrepe v teh primerih ter o tovrstnih incidentih poročati upravi.

3.2 KV PSP in plačilne sheme bi morali zagotoviti postopek za takojšnje obveščanje pristojnih organov (tj. nadzornikov in preglednikov ter organov za varstvo podatkov), kjer ti obstajajo, in sicer v primeru večjih varnostnih incidentov iz naslova plačilnih storitev, ki jih zagotavljajo.

3.3 KV PSP in plačilne sheme bi morali vzpostaviti postopek za sodelovanje z ustreznimi organi pregona pri večjih varnostnih incidentih iz naslova plačil, ki vključujejo tudi kršitve varnosti podatkov.

3.4 KV PSP pridobitelji bi morali na podlagi pogodbe zahtevati, da spletni trgovci, ki shranjujejo, obdelujejo ali posredujejo občutljive podatke o plačilih, sodelujejo z njimi in tudi z ustreznimi organi pregona v primeru varnostnih incidentov iz naslova plačil, vključno s kršitvami varnosti podatkov. Če PSP odkrije, da spletni trgovec ne sodeluje, kot zahteva pogodba, bi moral ukrepati, da uveljavi to pogodbeno obveznost, ali pogodbo prekiniti.

Priporočilo št. 4: Nadzor in zmanjševanje tveganj

PSP in plačilne sheme bi morali izvajati varnostne ukrepe v skladu s svojo varnostno politiko, da bi zmanjšali identificirana tveganja. Ti ukrepi bi morali vključevati večplastno varnostno zaščito, ki omogoča, da se ob neuspehu ene ravni zaščite aktivira druga raven zaščite (»globinska zaščita«).

4.1 KV Pri oblikovanju, razvijanju in vzdrževanju spletnih plačilnih storitev bi morali PSP in plačilne sheme posebej upoštevati ustrezno razdelitev nalog v okoljih informacijske tehnologije (IT) (npr. razvojno, testno in produkcijsko okolje) ter ustrezno izvajanje načela »najmanjšega privilegija«[13] kot osnovo za zanesljivo

[11] Na primer občutljivost sistema na vdor v postopek izvajanja plačila, injekcija SQL, skriptno izvajanje na več mestih, prekoračitve medpomnilnika.

[12] Na primer tveganja, ki so povezana z uporabo večpredstavnostnih aplikacij, vtičnikov v brskalnikih, okvirov, zunanjih povezav.

[13] »Vsak program in vsak privilegirani uporabnik sistema bi moral delovati tako, da bi koristil najmanjšo mogočo mero potrebnih privilegijev za dokončanje dela.« Glej Saltzer, J. H. (1974), »Zaščita in nadzor izmenjave informacij v sistemu Multics« *(Protection and the Control of Information Sharing in Multics)*,

upravljanje identitete in dostopa.

4.2 KV PSP in plačilne sheme bi morali imeti na voljo ustrezne varnostne rešitve za zaščito omrežij, spletnih strani, strežnikov in komunikacijskih povezav pred zlorabo ali napadi. PSP in plačilne sheme bi morali razbremeniti strežnike vseh odvečnih funkcij, da bi jih zaščitili (okrepili), ter odpraviti ali zmanjšati ranljivosti ogroženih aplikacij. Dostop različnih aplikacij do potrebnih podatkov in virov bi moral biti strogo omejen na najnižjo raven po načelu »najmanjšega privilegija«. Za omejitev uporabe »lažnih« spletnih strani (ki oponašajo legitimne strani PSP) bi bilo treba transakcijske spletne strani, ki ponujajo spletne plačilne storitve, označiti z razširjenimi potrdili o veljavnosti, sestavljenimi v imenu PSP, ali z drugimi podobnimi načini za avtentikacijo.

4.3 KV PSP in plačilne sheme bi morali imeti na voljo ustrezne postopke za spremljanje, sledenje in omejevanje dostopa do: i) občutljivih podatkov o plačilih ter ii) logičnih in fizičnih kritičnih virov, kot so omrežja, sistemi, zbirke podatkov, varnostni moduli, itd. PSP bi morali ustvarjati, shranjevati in analizirati ustrezne dnevnike in revizijske sledi.

4.4 KV Pri oblikovanju,[14] razvijanju in vzdrževanju spletnih plačilnih storitev bi PSP morali zagotoviti, da je zmanjšanje količine podatkov[15] nujna sestavina osrednje funkcije: zbiranje, preusmerjanje, obdelava, shranjevanje in/ali arhiviranje ter vizualizacija občutljivih podatkov o plačilih bi morali ostati na absolutno minimalni ravni.

4.5 KV Varnostne ukrepe za spletne plačilne storitve bi bilo treba preizkusiti pod nadzorom funkcije upravljanja tveganj, da bi tako zagotovili njihovo zanesljivost in učinkovitost. Vse spremembe bi morale biti predmet formalnega postopka uvajanja sprememb, ki zagotavlja, da so spremembe ustrezno načrtovane, preizkušene, dokumentirane in odobrene. Na podlagi uvedenih sprememb in opaženih groženj za varnost bi bilo treba testiranja redno ponavljati, vključno s scenariji zadevnih in znanih potencialnih napadov.

4.6 KV Varnostne ukrepe PSP za spletne plačilne storitve bi bilo treba redno revidirati, da bi zagotovili njihovo zanesljivost in učinkovitost. Revidirati bi bilo treba tudi izvajanje in delovanje spletnih plačilnih storitev. Pogostost in osredotočenost takih revizij bi morala upoštevati s tem povezana varnostna tveganja ter biti z njimi sorazmerna. Revizije bi morali izvajati zanesljivi in neodvisni (notranji ali zunanji) strokovnjaki. Ti nikakor ne bi smeli biti povezani z razvojem, izvajanjem ali operativnim upravljanjem zagotovljenih spletnih plačilnih storitev.

4.7 KV Kadar koli PSP in plačilne sheme funkcije, ki so povezane z varnostjo spletnih plačilnih storitev, prenesejo na zunanje izvajalce, bi pogodba morala vključevati določbe, ki zahtevajo skladnost z načeli in priporočili iz tega poročila.

4.8 KV PSP, ki ponujajo storitve pridobivanja, bi morali od spletnih trgovcev, ki obravnavajo (tj. shranjujejo, obdelujejo ali posredujejo) občutljive podatke o plačilih, na podlagi pogodbe zahtevati, da izvajajo varnostne ukrepe v svoji infrastrukturi IT, v skladu s KV 4.1 do 4.7, da se prepreči kraja teh občutljivih podatkov o plačilih iz njihovih sistemov. Če PSP odkrije, da spletni trgovec ne zagotavlja zahtevanih varnostnih ukrepov, bi moral ukrepati, da uveljavi to pogodbeno obveznost, ali pogodbo prekiniti.

4.1 NP PSP bi morali zagotoviti varnostna orodja (npr. ustrezno zavarovane naprave in/ali prirejene brskalnike), da bi zaščitili strankin vmesnik pred nezakonito rabo ali napadi (npr. napadi »prestrezanja v brskalniku«).

Priporočilo št. 5: Sledljivost

PSP bi morali imeti na voljo postopke, ki zagotavljajo, da se lahko ustrezno sledi vsem transakcijam in tudi poteku postopka e-pooblastila.

Sporočilo ACM, knjiga 17, št. 7, str. 388.

[14] Zasebnost že pri načrtovanju.

[15] Zmanjšanje količine podatkov se nanaša na politiko zbiranja čim manjše količine osebnih podatkov, potrebnih za izpeljavo dane funkcije.

5.1 KV PSP bi morali zagotoviti, da njihova storitev vključuje varnostne mehanizme za podrobno beleženje podatkov o transakciji in e-pooblastilu, vključno z zaporedno številko transakcije, časovnim žigom za podatke o transakciji, spremembami parametrizacije ter tudi dostopa do podatkov o transakciji in e-pooblastilu.

5.2 KV PSP bi morali uporabljati dnevniške datoteke, ki omogočajo sledenje morebitnim dodatkom, spremembam ali brisanjem podatkov o transakciji in e-pooblastilu.

5.3 KV PSP bi morali preverjati in analizirati podatke o transakciji in e-pooblastilu ter zagotoviti orodja za presojo dnevniških datotek. Zadevne aplikacije bi morale biti na voljo samo pooblaščenemu osebju.

5.1 NP PSP, ki ponujajo storitve pridobivanja, bi lahko na podlagi pogodbe zahtevali, da morajo spletni trgovci, ki shranjujejo podatke o plačilih, uvesti ustrezne postopke, ki podpirajo sledljivost.

POSEBNI KONTROLNI IN VARNOSTNI UKREPI ZA SPLETNA PLAČILA

Priporočilo št. 6: Začetna identifikacija stranke, podatki

Stranke bi bilo treba ustrezno identificirati v skladu z evropsko zakonodajo na področju preprečevanja pranja denarja[16] in potrditi bi morale, da so pripravljene izvesti spletna plačila z uporabo teh storitev, preden se jim zanje odobri dostop. PSP bi morali zagotoviti stranki ustrezne »predhodne«, »redne« ali, kjer to velja, »ad hoc« informacije o potrebnih zahtevah (npr. oprema, postopki) za izvajanje varnih spletnih plačilnih transakcij in o tveganjih, ki so neločljivo povezana s tem.

6.1 KV PSP bi morali zagotoviti, da je stranka izvedla postopke v zvezi s skrbnim preverjanjem stranke ter zagotovila ustrezne osebne dokumente[17] in s tem povezane podatke, preden se ji odobri dostop do spletnih plačilnih storitev.[18]

6.2 KV PSP bi morali zagotoviti, da predhodne informacije,[19] ki se zagotovijo stranki, vsebujejo vse podrobnosti v zvezi s spletnimi plačilnimi storitvami. Kjer pride v poštev, bi morale vključevati:

- točne informacije o vseh zahtevah, ki zadevajo opremo, programsko opremo ali druga potrebna orodja stranke (npr. protivirusna programska oprema, požarni zidovi);
- navodila za pravilno in varno uporabo personaliziranih varnostnih poverilnic;
- postopni opis postopka za stranko, ki želi predložiti in odobriti plačilno transakcijo in/ali pridobiti informacije, vključno s posledicami vsakega ukrepa;
- navodila za pravilno in varno uporabo vse strojne in programske opreme, ki se zagotovi stranki;
- postopke, ki jih je treba izvesti ob izgubi ali kraji personaliziranih varnostnih poverilnic ali strojne ali programske opreme stranke za prijavo v sistem ali izvajanje transakcij;
- postopke, ki jih je treba izvesti ob odkritju ali sumu zlorabe;
- opis odgovornosti in obveznosti PSP oziroma stranke v zvezi z uporabo spletne plačilne storitve.

---

16 Na primer, Direktiva 2005/60/ES Evropskega parlamenta in Sveta z dne 26. oktobra 2005 o preprečevanju uporabe finančnega sistema za pranje denarja in financiranje terorizma. UL L 309, 25.11.2005, str. 15–36. Glej tudi Direktivo Komisije 2006/70/ES z dne 1. avgusta 2006 o določitvi izvedbenih ukrepov za Direktivo 2005/60/ES Evropskega parlamenta in Sveta glede opredelitve »politično izpostavljene osebe« in tehničnih meril za postopke poenostavljene dolžnosti skrbnosti pri ugotavljanju identitete stranke ter izjeme na podlagi finančne dejavnosti, ki poteka le občasno ali v omejenem obsegu. UL L 214, 4.8.2006, str. 29–34.

17 Na primer potni list, osebno izkaznico ali napredni elektronski podpis.

18 Postopek identifikacije stranke ne posega v odstopanja, ki jih zagotavlja veljavna zakonodaja na področju preprečevanja pranja denarja. PSP ni treba izvajati ločenega postopka identifikacije stranke za spletne plačilne storitve, če je bila taka identifikacija stranke že izvedena, na primer za druge obstoječe storitve, povezane s plačili, ali za odprtje računa.

19 Ti podatki dopolnjujejo člen 42 Direktive o plačilnih storitvah, ki določa, katere informacije morajo PSP zagotoviti uporabniku plačilne storitve, preden sklenejo pogodbo za zagotavljanje plačilnih storitev.

6.3 KV PSP bi morali zagotoviti, da okvirna pogodba s stranko določa, da PSP lahko blokira določeno transakcijo ali plačilni instrument[20] zaradi varnostnih zadržkov. Določati bi moral način in pogoje obveščanja strank ter kako lahko stranka vzpostavi stik s PSP, da bi spletno plačilno transakcijo ali storitev »deblokirali«, kar je v skladu z Direktivo o plačilnih storitvah.

6.4 KV PSP bi morali tudi zagotoviti, da imajo stranke stalno ali ad hoc, kjer je to primerno, in po ustreznih kanalih (npr. letakih, spletnih straneh) na voljo točna in preprosta navodila z obrazložitvijo njihovih odgovornosti v zvezi z varno uporabo storitve.

6.1 NP Stranka bi lahko podpisala posebno pogodbo za storitev za izvajanje spletnih plačilnih transakcij, namesto da bi bili pogoji vključeni v širšo splošno pogodbo o storitvah s PSP.

Priporočilo št. 7: Močna avtentikacija strank

Začetek odreditve spletnih plačil in tudi dostop do občutljivih podatkov o plačilih bi morala biti zaščitena z močno avtentikacijo strank.

7.1 KV [kreditna plačila/e-pooblastilo/e-denar] PSP bi morali izvajati močno avtentikacijo strank za odobritev strankinih spletnih plačilnih transakcij (vključno z množičnimi kreditnimi plačili) ter izdajo ali spremembo elektronskih pooblastil za direktno obremenitev. Ob tem bi PSP lahko preučili sprejetje alternativnih ukrepov za avtentikacijo strank za:

- izplačila zanesljivim upravičencem, ki so že na predhodnih belih seznamih za dano stranko;
- transakcije med dvema računoma iste stranke pri istem PSP;
- prenose pri istem PSP, utemeljene na podlagi analize tveganosti transakcije;
- plačila malih vrednosti, kot jih opredeljuje Direktiva o plačilnih storitvah.[21]

7.2 KV Za pridobitev dostopa do občutljivih podatkov o plačilih ali za njihovo spremembo (vključno z oblikovanjem in spreminjanjem belih seznamov) je potrebna močna avtentikacija. Kadar PSP ponuja izključno svetovalne storitve in ne razkriva občutljivih podatkov o strankah ali plačilih, na primer podatkov o plačilnih karticah, ki jih je mogoče zlahka zlorabiti za goljufije, PSP lahko prilagodi svoje zahteve v zvezi z avtentikacijo na podlagi ocene tveganj.

7.3 KV [kartice] Pri kartičnih transakcijah bi morali vsi PSP, ki izdajajo kartice, podpirati močno avtentikacijo imetnika kartice. Vse izdane kartice morajo biti tehnično pripravljene (registrirane) za uporabo z močno avtentikacijo.

7.4 KV [kartice] PSP, ki ponujajo storitve pridobivanja, bi morali podpirati tehnologije, ki omogočajo izdajatelju močno avtentikacijo imetnika kartice za kartične plačilne sheme, v katerih sodeluje pridobitelj.

7.5 KV [kartice] PSP, ki ponujajo storitve pridobivanja, bi morali od svojega spletnega trgovca zahtevati, da podpira rešitve, ki izdajatelju omogoča močno avtentikacijo imetnika kartice za spletne kartične transakcije. Uporaba alternativnih ukrepov avtentikacije bi lahko bila primerna za vnaprej določene skupine transakcij z nizko stopnjo tveganja, na primer na podlagi analize tveganosti transakcije ali za plačila malih vrednosti, kot jih opredeljuje Direktiva o plačilnih storitvah.

7.6 KV Vse plačilne sheme bi morale podpreti izvajanje močne avtentikacije strank z uvedbo ureditve odgovornosti [22] za sodelujoče PSP na vseh evropskih trgih.

---

[20] Glej člen 55 Direktive o plačilnih storitvah o omejitvi uporabe plačilnega instrumenta.

[21] Glej opredelitev plačilnih instrumentov male vrednosti v členih 34(1) in 53(1) Direktive o plačilnih storitvah.

[22] Ureditev odgovornosti bi morala zagotoviti, da mora PSP izvesti povračilo drugim PSP vsako goljufijo, ki bi bila posledica šibke avtentikacije strank.

7.7 KV [kartice] Za sheme kartičnih plačil, ki jih storitev podpira, bi morali ponudniki storitev elektronske denarnice od izdajatelja zahtevati močno avtentikacijo, ko zakoniti imetnik prvič vnaša podatke o kartici.

7.8 KV Ponudniki storitev elektronske denarnice bi morali podpirati močno avtentikacijo strank, ko se te prijavijo v plačilne storitve elektronske denarnice ali izvajajo spletne kartične transakcije. Uporaba alternativnih ukrepov avtentikacije bi lahko bila primerna za vnaprej določene skupine transakcij z nizko stopnjo tveganja, na primer na podlagi analize tveganosti transakcije ali za plačila malih vrednosti, kot jih opredeljuje Direktiva o plačilnih storitvah.

7.9 KV [kartice] Pri virtualnih karticah bi morala prva registracija potekati v varnem in zanesljivem okolju[23]. Močna avtentikacija stranke bi morala biti obvezna za postopek ustvarjanja podatkov virtualne kartice, če se kartica izdaja v internetnem okolju.

7.10 KV PSP bi morali zagotavljati ustrezno dvostransko avtentikacijo, ko komunicirajo s spletnimi trgovci za namene odrejanja spletnih plačil in dostopa do občutljivih podatkov o plačilih.

7.1 NP [kartice] Spletni trgovci bi lahko podprli močno avtentikacijo imetnikov kartice, ki bi jo izvajal izdajatelj pri spletnih kartičnih transakcijah.

7.2 NP PSP bi lahko zaradi strank razmislili o uporabi enotnega orodja za avtentikacijo strank za vse plačilne storitve. To bi lahko povečalo sprejetost te rešitve med strankami in olajšalo pravilno uporabo.

7.3 NP Močna avtentikacija stranke bi lahko vključevala elemente, ki povezujejo avtentikacijo z določenim zneskom in prejemnikom plačila. To bi strankam lahko zagotovilo večjo gotovost pri odobravanju plačil. Tehnološka rešitev, ki omogoča povezavo med podatki za močno avtentikacijo in podatki o transakciji, bi morala biti odporna proti nedovoljenemu spreminjanju.

Priporočilo št. 8: Registracija in zagotavljanje orodij za avtentikacijo in/ali programske opreme, ki jo dobi stranka

PSP bi morali zagotoviti, da registracija in začetna zagotovitev orodij za avtentikacijo, potrebnih za uporabo spletne plačilne storitve, in/ali dostava programske opreme, povezane s plačilom, strankam, potekajo varno.

8.1 KV Registracija in zagotavljanje orodij za avtentikacijo in/ali programske opreme, povezane s plačilom, ki jo dobi stranka, bi morali izpolnjevati naslednje zahteve.

- Postopke, povezane s tem, bi bilo treba izvajati v varnem in zanesljivem okolju ob upoštevanju morebitnih tveganj, ki izhajajo iz naprav, nad katerimi PSP nima nadzora.

- Vzpostavljeni bi morali biti učinkoviti in varni postopki za dostavo personaliziranih varnostnih poverilnic, programske opreme za izvajanje plačil in vseh personaliziranih naprav, povezanih s spletnimi plačili. Programska oprema, dostavljena prek spleta, bi morala imeti tudi digitalni podpis PSP, da stranka lahko preveri njeno pristnost in da ni bila nedovoljeno spremenjena.

- [kartice] Pri kartičnih transakcijah bi stranka morala imeti možnost, da se prijavi v močno avtentikacijo neodvisno od določenega spletnega nakupa. Kadar obstaja možnost aktivacije med spletnim nakupovanjem, bi bilo treba stranko preusmeriti v varno in zanesljivo okolje.

8.2 KV [kartice] Izdajatelji bi morali aktivno spodbujati imetnike kartic k prijavi v močno avtentikacijo ter svojim imetnikom kartic omogočiti, da prijavo obidejo samo izjemoma in v omejenem številu primerov, kadar to upravičuje tveganje, povezano z določeno kartično transakcijo.

[23] Okolja v okviru odgovornosti PSP, ki zagotavljajo ustrezno avtentikacijo stranke in PSP, ki ponuja storitev, ter zaščito zaupnih/občutljivih informacij, so: i) prostori PSP; ii) spletna stran internetnega bančništva ali druga varna spletna stran, npr. kadar upravljavec plačilne sheme ponuja primerljive varnostne funkcije med drugim, kot je opredeljeno v priporočilu št. 4; ali iii) storitve bankomatov. (Pri bankomatih je obvezna močna avtentikacija stranke. Tako avtentikacijo navadno zagotavljata čip in PIN ali čip in biometrični podatki.)

Priporočilo št. 9: Poskusi prijave, iztek postopka, veljavnost avtentikacije

PSP bi morali omejiti število poskusov prijave ali avtentikacije, opredeliti pravila za »iztek« postopka spletne plačilne storitve in nastaviti omejitev časa za veljavnost avtentikacije.

9.1 KV Kadar se za avtentikacijo uporablja enkratno geslo, bi morali PSP zagotoviti, da je obdobje veljavnosti takih gesel omejeno na najkrajši potrebni čas.

9.2 KV PSP bi morali določiti največje število neuspelih poskusov prijave ali avtentikacije, po katerih se dostop do spletne plačilne storitve (začasno ali trajno) blokira. Zagotoviti bi morali varen postopek za ponovno aktivacijo blokiranih spletnih plačilnih storitev.

9.3 KV PSP bi morali določiti najdaljše obdobje, po katerem se neaktivni postopki spletnih plačilnih storitev samodejno prekinejo.

Priporočilo št. 10: Spremljanje transakcije

Mehanizme za spremljanje transakcije, zasnovane za preprečevanje, odkrivanje in blokiranje goljufivih plačilnih transakcij, bi bilo treba vklopiti pred zadnjo odobritvijo PSP; za sumljive ali zelo tvegane transakcije bi bilo treba izvesti poseben postopek preverjanja in presoje. Enakovredni varnostni mehanizmi za spremljanje in odobritev bi morali biti vzpostavljeni tudi za izdajo e-pooblastil.

10.1 KV PSP bi morali uporabljati sisteme za odkrivanje in preprečevanje goljufij, da bi prepoznali sumljive transakcije, preden PSP dokončno odobri transakcije ali e-pooblastila. Taki sistemi bi morali temeljiti na primer na pravilih na podlagi parametrov (kot so črne liste kompromitiranih ali ukradenih podatkov o karticah) in spremljati vzorce nenavadnega vedenja stranke ali strankine dostopne naprave (kot je sprememba naslova IP (Internet Protocol)[24] ali razpon IP med postopkom spletne plačilne storitve, kar je včasih mogoče odkriti s preverjanjem geolokacije naslova IP,[25] netipične skupine spletnih trgovcev za določeno stranko ali podatki o nenormalnih transakcijah itd.). Taki sistemi bi morali biti zmožni odkriti tudi znake okužbe programske opreme v postopku (npr. z avtomatiziranim proti ročnemu preverjanju) in znane scenarije goljufij. Obseg, kompleksnost in prilagodljivost rešitev za spremljanje bi morali biti ob upoštevanju ustrezne zakonodaje o varstvu podatkov sorazmerni z rezultati ocenjevanja tveganj.

10.2 KV Kartične plačilne sheme bi morale v sodelovanju s pridobitelji zagotoviti usklajeno opredelitev kategorij spletnih trgovcev in od pridobiteljev zahtevati, da jo temu primerno uporabljajo v sporočilu PSP o odobritvi, ki se pošlje izdajatelju.[26]

10.3 KV PSP pridobitelji bi morali imeti vzpostavljene sisteme za odkrivanje in preprečevanje goljufij, da bi lahko spremljali dejavnosti spletnih trgovcev.

10.4 KV PSP bi morali izvesti vse postopke preverjanja in presoje transakcije v ustreznem časovnem obdobju, da ne bi neupravičeno zavlačevali začetka odreditve in/ali izvršitve zadevne plačilne storitve.

10.5 KV Kadar se PSP v skladu s svojo politiko obvladovanja tveganj odloči za blokado plačilne transakcije, za katero je bilo ugotovljeno, da gre morda za goljufijo, bi moral ohraniti blokado čim krajši čas, dokler se ne razrešijo vprašanja glede varnosti.

Priporočilo št. 11: Zaščita občutljivih podatkov o plačilih

Občutljive podatke o plačilih bi bilo treba zaščititi med hrambo, obdelavo ali posredovanjem.

---

[24] Naslov IP je edinstvena številčna koda, ki omogoča prepoznavanje vsakega računalnika, povezanega z internetom.

[25] S preverjanjem »geolokacije naslova IP« preverimo, ali se država izdajatelja ujema z naslovom IP, s katerega uporabnik izvaja transakcijo.

[26] Skupine spletnih trgovcev se nanašajo na razvrstitev trgovcev glede na sektor poslovnih dejavnosti. Kategorije spletnih trgovcev trenutno še niso standardizirane po kartičnih plačilnih shemah in se ne pošljejo vedno v sporočilu o odobritvi. Usklajena razvrstitev skupin spletnih trgovcev (npr. na podlagi evropske razvrstitve NACE) bi pomagala PSP, da bi lažje analizirali tveganje goljufije pri določeni transakciji.

11.1 KV Vsi podatki, ki se uporabljajo za identifikacijo in avtentikacijo strank (npr. ob prijavi, na začetku odreditve spletnih plačil ter ob izdaji, spremembi ali preklicu e-pooblastil) in tudi vmesnika stranke (spletne strani PSP ali trgovca), bi morali biti ustrezno zavarovani pred krajo in nepooblaščenim dostopom ali spreminjanjem.

11.2 KV PSP bi morali zagotoviti, da se pri izmenjavi občutljivih podatkov o spletnih plačilih uporablja varno šifriranje od začetka od konca[27] med strankama, ki sta v stiku med zadevnim postopkom komuniciranja, da bi zaščitili zaupnost in celovitost podatkov z uporabo močnih in splošno priznanih tehnik šifriranja.

11.3 KV PSP, ki ponujajo storitve pridobivanja, bi morali spodbujati svoje spletne trgovce, naj občutljivih podatkov o plačilih ne shranjujejo. Če spletni trgovci obravnavajo, tj. shranjujejo, obdelujejo ali posredujejo občutljive podatke o plačilih, bi morali taki PSP od spletnih trgovcev na podlagi pogodbe zahtevati, da zagotovijo potrebne ukrepe za zaščito teh podatkov. PSP bi morali izvajati redne kontrole. Če PSP odkrije, da spletni trgovec, ki obravnava občutljive podatke o plačilih, ne zagotavlja potrebnih varnostnih ukrepov, bi moral ukrepati, da uveljavi to pogodbeno obveznost, ali pogodbo prekiniti.

11.1 NP Zaželeno je, da spletni trgovci, ki obravnavajo občutljive podatke o plačilih, ustrezno usposobijo svoje osebje, kiupravlja z goljufijami in to usposabljanje redno posodabljajo, da je vsebina vedno usklajena z dinamičnim varnostnim okoljem.

OZAVEŠČANJE, IZOBRAŽEVANJE IN OBVEŠČANJE STRANK

Priporočilo št. 12: Izobraževanje in obveščanje strank

PSP bi morali zagotoviti pomoč in navodila za stranke, kjer je to potrebno, v zvezi z varno uporabo spletnih plačilnih storitev. PSP bi morali komunicirati s svojimi strankami tako, da bi jim potrdili pristnost prejetega sporočila.

12.1 KV PSP bi morali zagotoviti najmanj en zavarovan kanal[28] za stalno komunikacijo s strankami v zvezi s pravilno in varno uporabo spletne plačilne storitve. PSP bi morali stranke obvestiti o tem kanalu in pojasniti, da sporočila v imenu PSP, poslana po drugih poteh, na primer po elektronski pošti, ki se nanašajo na pravilno in varno uporabo spletne plačilne storitve, niso zanesljiva. PSP bi moral pojasniti:

- postopek, po katerem lahko stranke poročajo PSP o (osumljenih) nepravih plačilih, sumljivih incidentih ali nepravilnostih med postopkom spletne plačilne storitve in/ali morebitnih poskusih socialnega inženiringa[29];
- naslednje korake, tj. kako bo PSP odgovoril stranki;
- kako bo PSP obvestil stranko o (potencialnih) nepravih transakcijah ali o tem, da se niso začele izvajati, ali opozoril stranko o pojavu napadov (npr. e-pošta z lažnim predstavljanjem).

12.2 KV PSP bi morali po zavarovanem kanalu obveščati stranke o posodobitvah varnostnih postopkov v zvezi s spletnimi plačilnimi storitvami. Tudi vsa opozorila o večjih porajajočih se tveganjih (npr. opozorila o socialnem inženiringu) bi bilo treba poslati po zavarovanem kanalu.

12.3 KV PSP bi morali strankam zagotoviti pomoč za vsa vprašanja, pritožbe, zahtevke za podporo in obvestila o nepravilnostih ali incidentih v zvezi s spletnimi plačili in podobnimi storitvami, stranke pa bi bilo treba ustrezno obvestiti o tem, kako se taka pomoč lahko pridobi.

---

[27] Šifriranje od začetka do konca se nanaša na šifriranje v ali pri izvornem končnem sistemu z ustreznim šifriranjem samo v ali pri ciljnem končnem sistemu. ETSI EN 302 109 V1.1.1. (2003-06).

[28] Na primer temu namenjen poštni predal na spletni strani PSP ali zavarovani spletni strani.

[29] Socialni inženiring v tem smislu pomeni tehnike manipulacije z ljudmi za pridobivanje informacij (npr. po e-pošti ali s telefonskimi klici) ali priklic informacij s socialnih omrežij za namene goljufije ali pridobivanje nepooblaščenega dostopa do računalnika ali omrežja.

12.4 KV PSP in, kjer je primerno, plačilne sheme bi morali uvesti programe za izobraževanje in ozaveščanje strank, katerih namen bi bil zagotoviti, da bi stranke razumele vsaj to, da je treba:

- zaščititi njihova gesla, varnostne žetone, osebne podatke in druge zaupne podatke;
- ustrezno nadzorovati varnost osebnih naprav (npr. računalnika) z namestitvijo in nadgradnjo varnostnih komponent (protivirusna zaščita, požarni zidovi, varnostni popravki);
- upoštevati večje grožnje in tveganja, ki so povezani s prenašanjem programske opreme z interneta, če stranka ne more biti zares prepričana, da je programska oprema pristna in ni bila nedovoljeno spremenjena;
- uporabljati pravo spletno stran PSP za spletna plačila.

12.5 KV PSP pridobitelji bi morali od spletnih trgovcev zahtevati, naj bodo postopki, povezani s plačili, jasno ločeni od spletne trgovine, da bodo stranke lažje ugotovile, kdaj komunicirajo s PSP in ne s prejemnikom plačila (npr. s preusmerjanjem stranke in odprtjem novega okna, zato da se postopek plačevanja ne pokaže v okviru spletnega trgovca).

12.1 NP Zaželeno je, da PSP, ki ponujajo storitve pridobivanja, pripravijo izobraževalne programe za svoje spletne trgovce o preprečevanju goljufij.

Priporočilo št. 13: Obvestila, določanje omejitev

PSP bi morali določiti omejitve za spletne plačilne storitve in svojim strankam v okviru teh omejitev zagotoviti možnosti za nadaljnje zmanjšanje tveganj. Prav tako lahko poskrbijo tudi za storitve opozarjanja in storitve upravljanja profilov strank.

13.1 KV PSP bi morali, preden stranki zagotovijo spletne plačilne storitve, določiti omejitve[30], ki veljajo za te storitve (npr. najvišji znesek za vsako posamezno plačilo ali kumulativni znesek za določeno obdobje), in o tem bi morali obvestiti svoje stranke. PSP bi morali strankam omogočiti, da izklopijo funkcijo spletnega plačila.

13.1 NP PSP bi lahko v okviru določenih omejitev zagotovili svojim strankam možnost upravljanja omejitev za spletne plačilne storitve v varnem in zanesljivem okolju.

13.2 NP PSP bi lahko strankam poslali opozorila, na primer prek telefonskih klicev ali kratkih sporočil, pri sumljivih ali zelo tveganih plačilnih transakcijah na podlagi svojih politik upravljanja tveganj.

13.3 NP PSP bi lahko strankam omogočili, da določijo splošna, personalizirana pravila kot parametre za svoje ravnanje v zvezi s spletnimi plačili in podobnimi storitvami, npr. odrejanje plačil samo iz določenih držav in blokiranje plačil, ki bi se izvajala od drugod, ali možnost vnašanja določenih prejemnikov na bele ali črne liste.

Priporočilo št. 14: Dostop strank do informacij o statusu postopka odreditve in izvršitve plačila

PSP bi morali svojim strankam potrditi, da je bilo plačilo odrejeno, in jim pravočasno zagotoviti vse potrebne informacije, s katerimi lahko preverijo, da se je plačilna transakcija začela izvajati in/ali je bila izvršena pravilno.

14.1 KV [kreditna plačila/e-pooblastilo] PSP bi morali strankam zagotoviti možnost, da skoraj v realnem času preverijo status izvrševanja transakcij ter v vsakem trenutku tudi saldo računov[31] v varnem in zanesljivem okolju.

14.2 KV Vsi podrobni elektronski izpiski bi morali biti na voljo v varnem in zanesljivem okolju. Kadar PSP obveščajo stranke o razpoložljivosti elektronskih izpiskov (npr. redno ob izdaji rednega e-izpiska ali ad hoc po izvršitvi transakcije) po alternativnem kanalu, kot so kratka sporočila, e-pošta ali pismo, ta sporočila ne bi smela vsebovati občutljivih podatkov o plačilih, če pa jih vsebujejo, bi morali biti prikriti.

---

[30] Take omejitve se lahko uporabljajo na splošno (tj. za vse plačilne instrumente, ki omogočajo spletna plačila) ali v posamičnih primerih.

[31] Razen v primeru izjemne nerazpoložljivosti te možnosti zaradi tehničnega vzdrževanja ali zaradi večjih incidentov.

SLOVAR IZRAZOV

Izrazi v nadaljevanju so opredeljeni za namene tega poročila.

Izraz	Opredelitev
Avtentikacija	Postopek, ki PSP omogoča preverjanje strankine identitete.
Odobritev	Postopek, s katerim se preverja, ali ima stranka ali PSP pravico izvesti določeno dejanje, na primer pravico do prenosa sredstev ali dostopa do občutljivih podatkov.
Pooblastila	Informacije – običajno zaupne –, ki jih zagotovi stranka ali PSP za avtentikacijo. Pooblastila lahko pomenijo tudi fizično orodje, ki vsebuje informacije (npr. generator enkratnega gesla, pametna kartica), ali nekaj, kar si uporabnik zapomni ali ga predstavlja (kot so biometrične značilnosti).
Večji varnostni incident iz naslova plačil	Incident, ki pomembno vpliva ali lahko vpliva na varnost, celovitost ali kontinuiteto sistemov PSP, povezanih s plačevanjem, in/ali varnost občutljivih podatkov o plačilih ali sredstev. Ocena pomembnosti bi morala upoštevati število potencialno oškodovanih strank, tvegani znesek in vpliv na druge PSP ali druge plačilne infrastrukture.
Analiza tveganosti transakcije	Ocena tveganja, povezanega z določeno transakcijo, ki upošteva merila, kot so na primer strankini vzorci plačevanja (vedenje), vrednost zadevne transakcije, vrsta proizvoda in profil prejemnika.
Virtualne kartice	Možnost plačevanja s kartico, za katero se ustvari alternativna, začasna številka kartice s krajšim obdobjem veljavnosti, omejeno uporabo in vnaprej določenim limitom porabe, ki se lahko uporablja za spletne nakupe.
Storitve elektronske denarnice	Rešitve, s katerimi stranka lahko prijavi podatke, ki se nanašajo na enega ali več plačilnih instrumentov, za izvrševanje plačil z več spletnimi trgovci.

PRILOGA: SEZNAM ORGANOV, KI SODELUJEJO V EVROPSKEM FORUMU ZA VARNOST PLAČIL MALIH VREDNOSTI

	Člani
BE	Nationale Bank van België/Banque Nationale de Belgique (belgijska centralna banka)
BG	Българска народна банка (bolgarska centralna banka)
CZ	Česká národní banka (češka centralna banka)
DK	Danmarks Nationalbank (danska centralna banka) Finanstilsynet
DE	Deutsche Bundesbank (nemška centralna banka) Bundesanstalt für Finanzdienstleistungsaufsicht
EE	Eesti Pank (estonska centralna banka) Finantsinspektsioon
IE	Central Bank of Ireland (irska centralna banka)
GR	Bank of Greece (grška centralna banka)
ES	Banco de España (španska centralna banka)
FR	Banque de France (francoska centralna banka) Autorité de Contrôle Prudentiel
IT	Banca d'Italia (italijanska centralna banka)
CY	Central Bank of Cyprus (ciprska centralna banka)
LV	Latvijas Banka (latvijska centralna banka) Finanšu un kapitāla tirgus komisija
LT	Lietuvos bankas (litovska centralna banka)
LU	Banque centrale du Luxembourg (luksemburška centralna banka) Commission de Surveillance du Secteur Financier
HU	Magyar Nemzeti Bank (madžarska centralna banka) Pénzügyi Szervezetek Állami Felügyelete

	Člani
MT	Central Bank of Malta (centralna banka Malte)
NL	De Nederlandsche Bank (nizozemska centralna banka)
AT	Oesterreichische Nationalbank (avstrijska centralna banka) Österreichische Finanzmarktaufsicht
PL	Narodowy Bank Polski (poljska centralna banka) Komisja Nadzoru Finansowego
PT	Banco de Portugal (portugalska centralna banka)
RO	Banca Națională a României (romunska centralna banka)
SI	Banka Slovenije
SK	Národná banka Slovenska (slovaška centralna banka)
FI	Suomen Pankki-Finlands Bank (finska centralna banka) Finanssivalvonta
SE	Sveriges Riksbank (švedska centralna banka) Finansinspektionen
UK	Financial Services Authority
	European Banking Authority (Evropski bančni organ) European Central Bank (Evropska centralna banka)
	Opazovalci
IPI	Central bank of Iceland (centralna banka Islandije) Fjármálaeftirlitið
LI	Liechtensteinische Landesbank 1861 (centralna banka Lihtenštajna) Finanzmarktaufsicht Liechtenstein (nadzor finančnega trga)
NO	Norges Bank (norveška centralna banka) Finanstilsvnet (norveški organ za finančni nadzor)
	Evropska komisija Europol

Naslov: Kaiserstrasse 29, 60311 Frankfurt na Majni, Nemčija

Poštni naslov: poštni predal 16 03 19, 60066 Frankfurt na Majni, Nemčija

Telefon: +49 69 1344 0; spletna stran: http://www.ecb.europa.eu; faks: +49 69 1344 6000

ISSN 978-92-899-0866-5 (elektronska izdaja)
kataloška številka EU QB-30-13-188-EN-N (elektronska izdaja)