EBI/PN/2014/12_Rev1

2014. gada 19. decembris

Galīgās pamatnostādnes

par interneta maksājumu drošību

Saturs

Pamatnostādnes par interneta maksājumu drošību

Pamatnostādņu statuss

Šajā dokumentā ietvertas pamatnostādnes saskaņā ar 16. pantu Eiropas Parlamenta un Padomes 2010. gada 24. novembra Regulā (ES) Nr. 1093/2010, ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Banku iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/78/EK („EBI regula"). Kompetentajām iestādēm un finanšu iestādēm saskaņā ar EBI regulas 16. panta 3. punktu jādara viss iespējamais, lai ievērotu pamatnostādnes.

Pamatnostādnēs izklāstīts EBI viedoklis par atbilstošām uzraudzības praksēm Eiropas Finanšu uzraudzības sistēmā jeb par to, kā Savienības tiesību akti jāpiemēro konkrētā jomā. Tādēļ EBI sagaida, ka pamatnostādnes ievēros visas tās kompetentās iestādes un finanšu iestādes, kurām tās ir adresētas. Kompetentajām iestādēm, uz kurām attiecas pamatnostādnes, tās jāievēro, attiecīgā veidā iekļaujot savās uzraudzības praksēs (piemēram, grozot savu tiesisko regulējumu vai veicot izmaiņas savos uzraudzības procesos), arī tad, ja pamatnostādnes galvenokārt paredzētas iestādēm.

Ziņojumu sniegšanas prasības

Saskaņā ar EBI regulas 16. panta 3. punktu kompetentajām iestādēm līdz 2015. gada 5. maijam jāpaziņo EBI, vai tās ievēro vai paredz ievērot šīs pamatnostādnes, vai jānorāda to neievērošanas iemesli. Ja līdz minētajam termiņam nebūs saņemts nekāds paziņojums, EBI uzskatīs, ka attiecīgās kompetentās iestādes nav izpildījušas minētās prasības. Paziņojumi jāiesniedz, nosūtot 5. nodaļā iekļauto veidlapu uz e-pasta adresi compliance@eba.europa.eu ar norādi „EBA/GL/2014/12". Paziņojumi jāiesniedz personām, kurām ir atbilstošas pilnvaras sniegt ziņojumus par atbilstību attiecīgo kompetento iestāžu vārdā.

Paziņojumus publicēs EBI tīmekļa vietnē saskaņā ar 16. panta 3. punktu.

I sadaļa. Darbības joma un definīcijas

Darbības joma

1. Šīs pamatnostādnes nosaka obligātās prasības interneta maksājumu drošības jomā. Pamatnostādnes balstās uz noteikumiem Direktīvā 2007/64/EK[1] ("Maksājumu pakalpojumu direktīva") attiecībā uz informācijas prasībām par maksājumu pakalpojumiem, un maksājumu pakalpojumu sniedzēju saistībām attiecībā uz maksājumu pakalpojumu sniegšanu. Turklāt direktīvas 10. panta 4. punkts liek maksājumu iestādēm ieviest stingrus pārvaldības pasākumus un atbilstīgus iekšējās kontroles mehānismus.

2. Pamatnostādnes attiecas uz maksājumu pakalpojumu sniegšanu, ko piedāvā maksājumu pakalpojumu sniedzēji ar interneta starpniecību, kā definēts minētās direktīvas 1. pantā.

3. Pamatnostādnes ir adresētas finanšu iestādēm, kā noteikts Regulas (ES) Nr. 1093/2010 4. panta 1. punktā, un kompetentajām iestādēm, kā noteikts Regulas (ES) Nr. 1093/2010 4. panta 2. punktā. Kompetentās iestādes no 28 Eiropas Savienības dalībvalstīm nodrošina un uzrauga šo pamatnostādņu piemērošanu maksājumu pakalpojumu sniedzējiem, kā noteikts Maksājumu pakalpojumu direktīvas 1. pantā.

4. Turklāt kompetentās iestādes var nolemt pieprasīt maksājumu pakalpojumu sniedzējiem sniegt ziņojumus kompetentajai iestādei par atbilstību pamatnostādnēm.

5. Šīs pamatnostādnes neietekmē Eiropas Centrālās bankas "Ieteikumi par interneta maksājumu drošību" ("Ziņojums") spēkā esamību.[2] Ziņojums joprojām ir tas dokuments saskaņā, ar kuru centrālās bankas savā maksājumu sistēmas un instrumentu pārraudzībā novērtē interneta maksājumu drošības atbilstību.

6. Pamatnostādnes nosaka obligātās prasības. Pamatnostādnes neskar maksājumu pakalpojumu sniedzēju atbildību par maksājumu darījumu riska uzraudzību un novērtēšanu, tās izstrādā savu drošības politiku un īsteno atbilstošus drošības, ārkārtas gadījumu, negadījumu pārvaldības un darbības nepārtrauktības pasākumus, kas ir samērojami ar sniegto maksājumu pakalpojumu saistīto risku.

7. Pamatnostādņu mērķis ir noteikt kopējas obligātās prasības sekojošiem interneta maksājumu pakalpojumiem neatkarīgi no izmantotās piekļuves ierīces:

    - [kartes] maksājumiem ar karti internetā, tostarp maksājumiem ar virtuālo karti, kā arī maksājumu kartes datu reģistrācijai, lai izmantotu pakalpojumu "virtuālais maciņš";

[1] Eiropas Parlamenta un Padomes Direktīva 2007/64/EK (2007. gada 13. novembris) par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 97/7/EK, 2002/65/EK, 2005/60/EK un 2006/48/EK un atceļ Direktīvu 97/5/EK, OV L 319, 05.12.2007.

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

- [kredīta pārvedumi] kredīta pārvedumiem internetā;

- [e-mandāts] tiešā debeta elektroniskā mandāta izsniegšanai un grozījumiem;

- [e-nauda] elektroniskās naudas pārvedumiem starp diviem elektroniskās naudas kontiem, izmantojot internetu.

8. Ja pamatnostādnes nosaka kādu rezultātu, šo rezultātu var sasniegt ar dažādiem līdzekļiem. Šajās pamatnostādnēs, papildus noteiktajām prasībām, ir sniegti labas prakses piemēri (1. pielikums), kurus maksājumu pakalpojumu sniedzējiem ieteicams, bet nav obligāti ievērot.

9. Ja maksājumu pakalpojumu sniegšana un instrumenti tiek piedāvāti, izmantojot maksājumu shēmas (piem., karšu maksājumu shēmas kredīta pārvedumu un tiešā debeta maksājumu shēmas u. c.), kompetentās iestādes sadarbojas ar attiecīgo centrālo banku, kas veic maksājumu instrumentu pārraudzības funkciju, lai par shēmu darbību atbildīgie izpildītāji spētu nodrošināt konsekventu pamatnostādņu piemērošanu.

10. Maksājumu integratori,[3] kas piedāvā maksājumu uzsākšanas pakalpojumus, tiek uzskatīti vai nu par interneta maksājumu pakalpojumu saņēmējiem (un tādējādi par maksājumu pakalpojumu sniedzējiem) vai par attiecīgo atbalsta shēmu ārējo tehnisko pakalpojumu sniedzējiem vai par maksājumu pakalpojumu sniedzējiem. Pēdējā gadījumā līgumā nosaka, ka maksājumu integratori atbilst pamatnostādnēm.

11. Pamatnostādņu darbības jomā nav iekļauti:

- citi interneta pakalpojumi, ko piedāvā maksājumu pakalpojumu sniedzējs, izmantojot savu maksājumu tīmekļa vietni (piemēram, e-starpniecības maksa, tiešsaistes līgumi);

- maksājumi, ja instruktāža tiek veikta pa pastu, tālruni, balss pastu, vai izmantojot uz SMS tehnoloģijas;

- mobilie maksājumi, izņemot pārlūkprogrammās bāzētos maksājumus;

- kredīta pārvedumi, ja trešā persona piekļūst klienta maksājumu kontam;

- maksājumu darījumi, ko veic uzņēmums, izmantojot speciālu tīklu;

- karšu maksājumi, izmantojot anonīmas un neuzpildāmas fiziskas vai virtuālas priekšapmaksas kartes, ja nav pastāvīgu saistību starp emitentu un kartes turētāju;

- maksājumu darījumu norēķini un tīrvērte.

[3] Maksājumu integratori nodrošina maksājuma saņēmēju (t.i. e-komersantu) ar standartizētu interfeisu maksājumu pakalpojumiem, ko sniedz maksājumu pakalpojumu sniedzēji.

Definīcijas

12. Šajās pamatnostādnēs, papildus definīcijām, kas minētas Maksājumu pakalpojumu direktīvā, piemēro šādas definīcijas:

- *Autentifikācija* ir procedūra, kas ļauj maksājumu pakalpojumu sniedzējam pārbaudīt klienta identitāti.

- *Droša klienta autentifikācija*, šajās pamatnostādnēs, procedūra, kas balstās uz divu vai vairāku šādu elementu izmantošanu, kas kvalificēti kā zināšanas, īpašumtiesības un raksturlielumi: i) kaut kas, ko zina tikai lietotājs, piemēram, statiskā parole, kods, personas identifikācijas numurs; ii) kaut kas, kas pieder tikai lietotājam, piemēram, kodu kalkulators, viedkarte, mobilais tālrunis; iii) kaut kas, kas ir raksturīgs tikai lietotājam, piemēram, pirkstu nospiedumi. Turklāt izvēlētajiem elementiem jābūt savstarpēji neatkarīgiem, t.i., kompromitējot vienu netiek apdraudēts cits(i) Vismaz vienam no elementiem jābūt unikālam un atkārtoti neizmantojamam (izņemot raksturīgi piemītošam, piemēram viedkartei), un tādam, ko nav iespējams slepeni iegūt, izmantojot internetu. Drošas autentifikācijas procedūra ir tāda, kas aizsargā autentifikācijas datu konfidencialitāti.

- *Autorizācija* ir procedūra, kas pārbauda, vai klientam vai arī maksājumu pakalpojumu sniedzējam ir tiesības veikt konkrētu darbību, piemēram, tiesības pārskaitīt līdzekļus, vai piekļūt slepeniem datiem.

- *Autentifikācijas* dati parasti ir konfidenciāla informācija, ko iesniedz klients vai maksājumu pakalpojumu sniedzējs autentifikācijas mērķiem. Autentifikācijas dati var nozīmēt arī iekārtas piederēšanu, kas satur informāciju (piemēram, kodu kalkulators, viedkarte), vai kaut kas, ko lietotājs atceras vai pārstāv (piemēram, biometriskie parametri).

- *Nozīmīgs maksājumu drošības incidents* ir incidents, kuram ir vai var būt būtiska ietekme uz drošību, integritāti vai maksājumu pakalpojumu sniedzēja izmantoto sistēmu darbības nepārtrauktību un/vai uz slepenu maksājumu datu vai līdzekļu drošību. Būtiskuma novērtējumā ņem vērā iespējami skarto klientu skaitu un riska ietekmi uz citiem maksājumu pakalpojumu sniedzējiem vai citām maksājumu infrastruktūrām.

- *Darījuma riska analīze* ir riska novērtējums, kas saistīts ar konkrētu darījumu, ņemot vērā tādus kritērijus kā, piemēram, klientu maksājumu veidu (raksturu), saistīto darījumu vērtību, produkta veidu un saņēmēja profilu.

- *Virtuālās kartes* ir risinājums maksājumiem ar karti, tām ir alternatīvs, pagaidu kartes numurs ar samazinātu derīguma termiņu, ierobežota lietošana, iepriekš noteikti maksājumu ierobežojumi, un tās var izmantot pirkumiem internetā.

- *Virtuālais maciņš* ir risinājums, kas ļauj klientam reģistrēt datus, kas attiecas uz vienu vai vairākiem maksājumu instrumentiem, lai veiktu maksājumus vairākiem e-komersantiem.

II sadaļa. Pamatnostādnes par interneta maksājumu drošību

Vispārējā kontrole un drošības vide

Vadība

1. Maksājumu pakalpojumu sniedzēji ievieš un regulāri pārskata drošības politiku interneta maksājumu pakalpojumiem.

    1.1 Drošības politikai jābūt pienācīgi dokumentētai un tā tiek regulāri pārskatīta (saskaņā ar 2.4. punktu) un to apstiprina augstākā vadība. Tā nosaka drošības mērķus un pieļaujamo riska līmeni.

    1.2 Drošības politika nosaka lomas un atbildību, tostarp informācijas drošības riska pārvaldības funkciju ar tiesībām sniegt tiešu ziņojumu augstākās vadības līmenī, un pienākumu gatavot regulārus drošības pārskatus par interneta maksājumu pakalpojumiem, tostarp par slepenu maksājumu datu pārvaldību, ņemot vērā riska novērtējumu, kontroli un mazināšanu.

Riska novērtējums

2. Maksājumu pakalpojumu sniedzēji veic un dokumentē detalizētu riska novērtējumu attiecībā uz interneta maksājumu drošību un ar to saistītiem pakalpojumiem, gan pirms pakalpojuma(u) izveidošanas, gan regulāri pēc tam.

    2.1 Maksājumu pakalpojumu sniedzēji, īstenojot riska pārvaldības funkciju, veic un dokumentē detalizētu riska izvērtēšanu interneta maksājumiem un ar to saistītajiem pakalpojumiem. Maksājumu pakalpojumu sniedzēji apsver pastāvīgas uzraudzības rezultātus attiecībā uz drošības draudiem saistībā ar interneta maksājumu pakalpojumiem, ko tie piedāvā vai plāno piedāvāt, ņemot vērā: i) izmantoto tehnoloģisko risinājumu, ii) no ārējo pakalpojumu sniedzējiem saņemtos pakalpojumus un, iii) klientu tehnisko vidi. Maksājumu pakalpojumu sniedzēji izvērtē risku, kas saistīts ar izvēlēto tehnoloģiju platformām, to uzbūvi un arhitektūru, programmēšanas metodēm un kārtību, gan viņu pusē,[4] gan klientu pusē,[5] kā arī drošības incidentu uzraudzības procesu (skatīt 3. punktu).

    2.2 Pamatojoties uz šo, maksājumu pakalpojumu sniedzēji nosaka, vai un cik lielā mērā esošajiem drošības pasākumiem, izmantotajām tehnoloģijām un piedāvātajiem pakalpojumiem vai procedūrām ir nepieciešamas izmaiņas. Maksājumu pakalpojumu sniedzēji ņem vērā laiku, kas nepieciešams izmaiņu ieviešanai (tostarp ieviešanai

[4] Piemēram, sistēmas jutību, lai novērstu maksājumu sesiju nolaupīšanu, *SQL* injekciju, starpvietņu skriptošanu, bufera pārpildi utt.

[5] Piemēram, riski, kas saistīti ar multivides aplikāciju, pārlūkprogrammu spraudņu, rāmju, ārējo saišu utt. izmantošanu.

klienta pusē) un pieņemt nepieciešamos pagaidu pasākumus, lai mazinātu drošības incidentus un krāpšanu.

2.3 Risku novērtēšana pievēršas arī nepieciešamībai aizsargāt slepenus maksājumu datus.

2.4 Maksājumu pakalpojumu sniedzēji pārskata riska scenārijus un esošos drošības pasākumus pēc nozīmīgiem incidentiem, kas ietekmē pakalpojumus, pirms nozīmīgām infrastruktūras vai procedūras izmaiņām, un ja tiek identificēti jauni draudi. Turklāt riska novērtējuma vispārēju pārskatīšanu veic vismaz reizi gadā. Riska novērtējuma un pārskatīšanas rezultātus iesniedz apstiprināšanai augstākajai vadībai.

Incidentu uzraudzība un ziņojumu sniegšana

3. Maksājumu pakalpojumu sniedzēji nodrošina konsekventu un integrētu uzraudzību, drošības incidentu apstrādi un kontroli, tostarp arī ar drošību saistītu klientu sūdzību apstrādi. Maksājumu pakalpojumu sniedzēji nosaka procedūras ziņojumu sniegšanai vadībai par šādiem incidentiem. Nozīmīgu maksājumu drošības incidentu gadījumā ziņo par to kompetentajām iestādēm.

3.1 Maksājumu pakalpojumu sniedzējiem ir pieejamas procedūras drošības incidentu un ar drošību saistīto klientu sūdzību uzraudzībai, apstrādei un kontrolei, un tie ziņo par šādiem incidentiem uzņēmuma vadībai.

3.2 Maksājumu pakalpojumu sniedzējiem ir pieejama procedūra, lai nekavējoties sniegtu ziņojumu kompetentajām iestādēm (t.i., uzraudzības un datu aizsardzības iestādēm), , par nozīmīgiem maksājumu drošības incidentiem saistībā ar sniegtajiem maksājumu pakalpojumiem.

3.3 Maksājumu pakalpojumu sniedzējiem ir pieejama procedūra, lai sadarbotos ar attiecīgajām tiesībsargājošajām iestādēm saistībā ar nozīmīgiem maksājumu drošības incidentiem, tostarp datu aizsardzības pārkāpumiem.

3.4 Maksājumu pakalpojumu sniedzēji ar līgumu pieprasa e-komersantiem, kas uzglabā, apstrādā vai pārsūta slepenus maksājumu datus, sadarboties nozīmīgu maksājumu drošībās incidentu jomā, tostarp par datu aizsardzības pārkāpumiem, gan ar viņiem, gan ar attiecīgajām uzraudzības iestādēm. Ja maksājumu pakalpojumu sniedzējs uzzina, ka e-komersants nesadarbojas, kā to prasa līgums, tas rīkojas, lai izpildītu šajā līgumā paredzētās saistības, vai laužlīgumu.

Riska kontrole un mazināšana

4. Maksājumu pakalpojumu sniedzēji īsteno drošības pasākumus atbilstoši drošības politikai, lai mazinātu konstatētos riskus. Šie pasākumi ietver vairākus drošības līmeņus, kur vienas aizsardzības līnijas pārrāvuma gadījumā, iesaistās nākamā aizsardzības līnija ("pastiprinātā aizsardzība").

   4.1 Izstrādājot, attīstot un uzturot interneta maksājumu pakalpojumus, maksājumu pakalpojumu sniedzēji pievērš īpašu uzmanību atbilstošai pienākumu nodalīšanai informācijas tehnoloģiju (IT) vidē (piemēram, izstrādes, testēšanas un ražošanas vidēm) un pienācīgai "mazāko privilēģiju" principa īstenošanai, kā pamatam pieejas tiesību pārvaldībai.[6]

   4.2 Maksājumu pakalpojumu sniedzējiem ir pieejami atbilstoši drošības risinājumi, lai aizsargātu tīklus, tīmekļa vietnes, serverus un sakaru nodrošinājumu pret vardarbību vai uzbrukumiem. Maksājumu pakalpojumu sniedzēji atslēdz serveros visas liekās funkcijas, lai tos aizsargātu (stiprinātu), un novērstu vai mazinātu lietojumprogrammu ievainojamību riska situācijās. Dažādu lietojumprogrammu piekļuve datiem jāmazina līdz minimumam saskaņā ar "mazāko privilēģiju" principu. Lai ierobežotu "viltotu" tīmekļa vietņu, kas atdarina likumīgās maksājumu pakalpojumu sniedzēja vietnes izmantošanu, transakciju tīmekļa vietnes, kas piedāvā interneta maksājumu pakalpojumus, aizsargā ar uzticamiem sertifikātiem, kas izsniegti ar maksājumu pakalpojumu sniedzēja nosaukumu vai citām līdzīgām autentifikācijas metodēm.

   4.3 Maksājumu pakalpojumu sniedzēji ievieš piemērotas procedūras, lai uzraudzītu, kontrolētu un ierobežotu piekļuvi: i) slepeniem maksājumu datiem, un ii) loģiskajiem un fiziskajiem kritiskas nozīmes resursiem, piemēram, tīkliem, sistēmām, datu bāzēm, drošības moduļiem utt. Maksājumu pakalpojumu sniedzēji izveido, uzglabā un analizē attiecīgus auditācijas pierakstus.

   4.4 Izstrādājot,[7] attīstot un uzturot interneta maksājumu pakalpojumus, maksājumu pakalpojumu sniedzēji nodrošina, ka datu vākšanas samazināšana[8] ir būtiska galvenās funkcijas sastāvdaļa: slepenu maksājumu datu vākšana, maršrutēšana, apstrāde, uzglabāšana, un/vai arhivēšana un vizualizācija jāsamazina līdz iespējamam minimumam.

[6] "Visām programmām un ikvienam privileģētajam sistēmas lietotājam jādarbojas, izmantojot vismazāko privilēģiju skaitu, kas nepieciešams, lai pabeigtu darbu. " Skatīt Saltzer, Dž. H. "Informācijas koplietošanas aizsardzība un kontrole Multics sistēmā", ACM asociācijas saziņa, (1974), 17. sējums, Nr. 7, 388. lpp.

[7] Privātuma aizsardzība.

[8] Datu vākšanas samazināšana attiecas uz personas informācijas datu, kas nepieciešami norādītās funkcijas veikšanai, vākšanu vismazākajos apmēros.

4.5 Drošības pasākumus attiecībā uz interneta maksājumu pakalpojumiem pārbauda riska pārvaldības funkcijas vadībā, lai nodrošinātu to drošumu un efektivitāti. Visas izmaiņas pakļaujamas noteiktajai izmaiņu pārvaldības procedūrai, nodrošinot, ka izmaiņas tiek pienācīgi plānotas, testētas, dokumentētas un ieviestas. Pamatojoties uz veiktajām izmaiņām un novērotajiem drošības draudiem, testus atkārto regulāri un izskata atbilstošos un zināmos iespējamo uzbrukumu scenārijus.

4.6 Maksājumu pakalpojumu sniedzēju noteiktos drošības pasākumus periodiski auditē, lai nodrošinātu to stabilitāti un efektivitāti. Auditē arī interneta maksājumu pakalpojumu ieviešanu. Nosakot šādu auditu regularitāti un mērķi, ņem vērā saistītos drošības riskus. Revīziju veic kompetenti un neatkarīgi (iekšējie vai ārējie) eksperti, kas nav iesaistīti sniegto interneta maksājumu pakalpojumu izstrādē, ieviešanā un uzturēšanā.

4.7 Ja maksājumu pakalpojumu sniedzēji sniedz ārpakalpojumus, kas saistīti ar interneta maksājumu pakalpojumu drošību, līgumā iekļauj noteikumus, kas prasa ievērot atbilstību ar šajās pamatnostādnēs noteiktajiem principiem un vadlīnijām.

4.8 Maksājumu pakalpojumu sniedzēji, piedāvājot iegādāties pakalpojumu, līgumā pieprasa e-komersantiem, kas apstrādā (t. i., glabā, apstrādā un pārsūta) slepenu maksājumu datus, pieprasa lai tie ieviestu drošības pasākumus to IT infrastruktūrā, saskaņā ar 4.1. līdz 4.7. punktiem, lai izvairītos no maksājumu datu zādzībām viņu sistēmās. Ja maksājumu pakalpojumu sniedzējs uzzina, ka e-komersants nav ieviesis nepieciešamos drošības pasākumus, tas rīkojas, lai izpildītu šajā līgumā paredzētās saistības, vai lauž līgumu.

Izsekojamība

5. Maksājumu pakalpojumu sniedzējiem ir pieejamas procedūras, lai nodrošinātu, ka visi darījumi, kā arī e-mandāta procedūras plūsma, ir atbilstoši izsekojama.

5.1 Maksājumu pakalpojumu sniedzēji nodrošina, ka to pakalpojums ietver drošības mehānismus, kas nodrošina darījuma detalizētu reģistrēšanu, tostarp ietverot darījuma kārtas numuru, darījuma laika zīmogu, izmaiņas parametrizācijā, kā arī jebkuru piekļuvi e-mandāta un darījuma datiem.

5.2 Maksājumu pakalpojumu sniedzēji nodrošina auditācijas pierakstus, kas ļauj izsekot visām darījuma vai e-mandāta datu papildinājuma, izmaiņu vai dzēšanas darbībām.

5.3 Maksājumu pakalpojumu sniedzēji regulāri pārskata un analizē darījumu auditācijas pierakstus un šim mērķim lieto metodes un rīkus , kas ļauj to veikt efektīvi. Šīs procedūras īsteno tikai pilnvarotais personāls.

Īpaša kontrole un drošības pasākumi interneta maksājumiem

Sākotnējā klienta identifikācija, informācija

6. Klienti tiek atbilstoši identificēti, saskaņā ar Eiropas tiesību aktiem par nelikumīgi iegūtu līdzekļu legalizēšanu,[9] un tie apstiprina gatavību veikt interneta maksājumus, pirms tiem tiek piešķirta piekļuve šādiem pakalpojumiem. Maksājumu pakalpojumu sniedzēji sniedz klientam pietiekamu "iepriekšēju", "regulāru" vai, attiecīgā gadījumā, "*ad hoc*" informāciju par šo pakalpojumu riskiem un nepieciešamajām prasībām (piemēram, aprīkojumu, procedūrām), lai veiktu drošus interneta maksājumus.

6.1 Maksājumu pakalpojumu sniedzēji nodrošina, ka klientam tiek veiktas klienta uzticamības pārbaudes procedūras, kā arī, ka klients iesniedz nepieciešamos identitāti apliecinošus dokumentus[10] un saistīto informāciju, pirms viņam tiek piešķirta piekļuve interneta maksājumu pakalpojumiem.[11]

6.2 Maksājumu pakalpojumu sniedzēji nodrošina, ka sākotnējā informācija[12], kas tiek nodota klientam, satur visu nepieciešamo informāciju attiecībā uz interneta maksājumu pakalpojumu drošību. Nepieciešamības gadījumā tajā iekļauj:

- skaidru informāciju par prasībām attiecībā uz klienta datortehniku, programmatūru vai citiem nepieciešamajiem instrumentiem (piemēram, pretvīrusu programmatūru, ugunsmūri);
- pamatnostādnes par autentifikācijas datu pareizu un drošu lietošanu;
- detalizētu, soli-pa-solim procedūras aprakstu, lai klients spētu iesniegt un apstiprināt maksājumu darījumu un/vai iegūt informāciju, tajā skaitā katras darbības sekas;
- prasības par, klientam nodotās, aparatūras un programmatūras drošu un pareizu izmantošanu;
- darbības, kas veicamasautentifikācijas datu vai klienta iekārtu vai programmatūras, kas paredzēta piekļuvei vai darījumu veikšanai, nozaudēšanas vai nozagšanas gadījumā;

[9] Piemēram, Eiropas Parlamenta un Padomes Direktīva 2005/60/EK (2005. gada 26. oktobris) par to, lai nepieļautu finanšu sistēmas izmantošanu nelikumīgi iegūtu līdzekļu legalizēšanai un teroristu finansēšanai. OV L 309, 25.11.2005., 15.-36. lpp. Skatīt arī Komisijas Direktīva 2006/70/EK (2006. gada 1. augusts), ar ko nosaka īstenošanas pasākumus Eiropas Parlamenta un Padomes Direktīvai 2005/60/EK attiecībā uz "politiski ietekmējamas personas" definīciju un tehniskajiem kritērijiem vienkāršotām klienta uzticamības pārbaudes procedūrām un atbrīvojumam sakarā ar finanšu darbību, kuru veic reti vai ļoti ierobežotos apjomos. OV L 214, 4.8.2006., 29.-34. lpp.

[10] Piemēram, pase, identifikācijas karte vai drošs elektroniskais paraksts.

[11] Klienta identifikācijas procedūra neskar nevienu no izņēmumiem, kas paredzēti spēkā esošajos tiesību aktos par nelikumīgi iegūtu līdzekļu legalizēšanu. Maksājumu pakalpojumu sniedzēji neveic atsevišķu klienta identifikācijas procedūru interneta maksājumu pakalpojumiem, ar noteikumu, ka šāda klienta identifikācija jau ir veikta, piemēram, saistībā ar citiem esošajiem ar maksājumiem saistītajiem pakalpojumiem vai ar konta atvēršanu.

[12] Šo informāciju papildina Maksājumu pakalpojumu direktīvas 42. pants, kas precizē informāciju, kuru maksājumu pakalpojumu sniedzēji sniedz maksājumu pakalpojuma lietotājam pirms noslēgts līgums par maksājumu pakalpojumu sniegšanu.

- darbības, kas veicamas, ja tiek konstatēta ļaunprātīga konta izmantošana vai ja rodas aizdomas par to;

- Maksājumu pakalpojumu sniedzēja un klienta pienākumu un saistību aprakstu, ņemot vērā konkrēto interneta maksājumu pakalpojumu.

6.3 Maksājumu pakalpojumu sniedzēji nodrošina, ka līgumā ar klientu ir norādīts, ka maksājumu pakalpojumu sniedzējs var bloķēt noteiktu darījumu vai maksājumu instrumentu, [13] pamatojoties uz drošības apsvērumiem. Nosaka metodes un nosacījumus par ziņojumu sniegšanu klientam, un kā klients var sazināties ar maksājumu pakalpojumu sniedzēju, lai "atbloķētu" interneta maksājumu darījumu vai pakalpojumu, saskaņā ar Maksājumu pakalpojumu direktīvu.

Droša klienta autentifikācija

7. Interneta maksājumu uzsākšanu, kā arī piekļuvi slepeniem maksājuma datiem aizsargā ar drošu klienta autentifikāciju. Maksājumu pakalpojumu sniedzējs ievieš drošu klientu autentifikācijas procedūru saskaņā ar šajās pamatnostādnēs sniegto definīciju.

7.1 [kredīta pārvedums/e-mandāts/e-nauda] Maksājumu pakalpojumu sniedzēji veic drošu klientu autentifikāciju klienta interneta maksājumu darījumu autorizēšanai (ieskaitot saistītos kredīta pārvedumus) un elektronisko tiešo debeta mandātu izsniegšanai vai grozīšanai. Tomēr maksājumu pakalpojumu sniedzēji var izmantot alternatīvus klienta autentifikācijas pasākumus:

- maksājumiem uzticamam saņēmējam, kas iekļauts iepriekš izveidotā apstiprināto maksājumu sarakstā vai baltajā sarakstā (white list);

- darījumiem starp viena klienta diviem kontiem, kurus uztur viens un tas pats maksājumu pakalpojumu sniedzējs;

- pārvedumiem viena un tā paša maksājumu pakalpojumu sniedzēja ietvaros, ko apstiprina darījuma riska analīze;

- maza apjoma maksājumiem, kā minēts Maksājumu pakalpojumu direktīvā.[14]

[13] Skatīt Maksājumu pakalpojumu direktīvas 55. pantu par maksājumu instrumentu izmantošanas ierobežojumiem.

[14] Skatīt maza apjoma maksājumu instrumentu definīciju Maksājumu pakalpojumu direktīvas 34. panta 1. punktā un 53. panta 1. punktā.

7.2 Lai piekļūtu vai lai grozītu slepenos maksājumu datus (tostarp baltā saraksta izveidošana un grozīšana) nepieciešama droša klienta autentifikācija. Ja maksājumu pakalpojumu sniedzējs piedāvā tikai informatīvus pakalpojumus, kas neatspoguļo slepenu klienta vai maksājumu informāciju, piemēram, maksājumu kartes datus, kurus ir iespējams ļaunprātīgi izmantot krāpšanas nolūkos, maksājumu pakalpojumu sniedzējs var pielāgot savas autentifikācijas prasības, pamatojoties uz riska novērtējumu.

7.3 [kartes] Attiecībā uz karšu darījumiem, visām maksājumu pakalpojumu sniedzēja izsniegtajām kartēm jāatbalsta droša kartes turētāja autentifikācija. Visām izsniegtajām kartēm jābūt tehniski gatavām (reģistrētām) izmantošanai ar drošu autentifikāciju.

7.4 [kartes] Maksājumu pakalpojumu sniedzēji, piedāvājot iegādāties pakalpojumu, atbalsta tehnoloģijas, kas ļauj izsniedzējam veikt drošu kartes turētāja autentifikāciju kartes maksājumu sistēmās, kurās pircējs piedalās.

7.5 [kartes] Maksājumu pakalpojumu sniedzēji, piedāvājot iegādāties pakalpojumu, pieprasa savam e-komersantam atbalstīt risinājumus, kas ļauj izsniedzējam veikt drošu kartes turētāja autentifikāciju darījumiem ar karti internetā. Alternatīvus autentifikācijas pasākumus apsver iepriekš noteiktām zema riska darījumu kategorijām, piemēram, pamatojoties uz darījumu riska analīzi, vai maza apjoma maksājumiem, kā minēts Maksājumu pakalpojumu direktīvā.

7.6 [kartes] Virtuālā maciņa pakalpojumu sniedzēji pieprasa drošu autentifikāciju, ja likumīgais turētājs pirmo reizi reģistrē kartes datus.

7.7 Virtuālā maciņa pakalpojumu sniedzēji atbalsta klienta autentifikāciju, ja klients piesakās virtuāla maciņa maksājumu pakalpojumiem vai veic darījumus ar karti internetā. Alternatīvus autentifikācijas pasākumus apsver iepriekš noteiktām zema riska darījumu kategorijām, piemēram, pamatojoties uz darījumu riska analīzi, vai maza apjoma maksājumiem, kā minēts Maksājumu pakalpojumu direktīvā.

7.8 [kartes] Virtuālajām kartēm sākotnējā reģistrācija notiek drošā un uzticamā vidē.[15] Droša klienta autentifikācija nepieciešama virtuālās kartes datu ģenerēšanas procedūrai, ja karte izsniegta interneta vidē.

7.9 Maksājumu pakalpojumu sniedzēji nodrošina atbilstīgu divpusēju autentifikāciju, sazinoties ar e-komersantu par interneta maksājumu uzsākšanu un par piekļuvi slepeniem maksājumu datiem.

[15] Maksājumu pakalpojumu sniedzēju atbildības vide, kurā atbilstoša klienta un maksājumu pakalpojumu sniedzēju, kas piedāvā šo pakalpojumu, autentifikācija un konfidenciālas/slepenas informācijas aizsardzība tiek nodrošināta arī: i) maksājumu pakalpojumu sniedzēju telpās; ii) interneta bankas vai citās drošās tīmekļa vietnēs, piemēram, ja GA piedāvā salīdzināmus drošības līdzekļus, *inter alia,* kā tas definēts 4. pamatnostādnē; vai iii) bankomātu (ATM) pakalpojumiem. (Bankomātiem nepieciešama droša klientu autentifikācija. Šādu autentifikāciju parasti nodrošina ar mikroshēmu un PIN kodu vai mikroshēmu un biometrijas standartiem).

Pieteikšanās autentifikācijas instrumentiem un/vai programmatūrai un to piegāde

8. Maksājumu pakalpojumu sniedzēji nodrošina, ka klienta pieteikšanās autentifikācijas līdzekļiem, kas nepieciešami, lai izmantotu interneta maksājumu pakalpojumu un to piegāde tiek veikta drošā veidā.

    8.1 Pieteikšanās autentifikācijas līdzekļiem un to piegāde atbilst šādām prasībām.

    - Saistītās procedūras veic drošā un uzticamā vidē, vienlaikus ņemot vērā iespējamos riskus, kas izriet no ierīcēm, kas neatrodas maksājumu pakalpojumu sniedzēja kontrolē.

    - Ievieš efektīvas un drošas procedūras autentifikācijas datu, ar maksājumiem saistītās programmatūras un visu ar interneta maksājumiem saistīto personalizēto ierīču piegādei. Internetā piegādāto programmatūru paraksta maksājumu pakalpojumu sniedzējs, kas pircējam dod iespēju pārbaudīt tās autentiskumu, un pārliecināties, ka tā nav iepriekš lietota.

    - [kartes] Darījumiem ar karti, klientam ir iespēja reģistrēties drošai autentifikācijai neatkarīgi no konkrētā interneta pirkuma. Ja aktivizācija tiek piedāvāta tiešsaistes iepirkšanās laikā, to dara, novirzot klientu uz drošu un uzticamu vidi.

    8.2 [kartes] Izsniedzēji aktīvi veicina kartes turētāja reģistrāciju drošai autentifikācijai un ļauj turētājiem apiet reģistrāciju tikai izņēmuma kārtā un tikai ierobežotam skaitam gadījumu, ja to attaisno risks, kas saistīts ar darījuma ar karti specifiskumu.

Autentifikācijas mēģinājumi, sesijas noilgums, autentifikācijas derīgums

9. Maksājumu pakalpojumu sniedzēji ierobežo pieteikšanās vai autentifikācijas mēģinājumu skaitu, nosaka prasībaspar interneta maksājumu pakalpojumu sesijas "noilgumu" un nosaka autentifikācijas mēģinājumu skaitu.

    9.1 Izmantojot vienreizēju/unikālu paroli autentifikācijai, maksājumu pakalpojumu sniedzēji nodrošina, ka šādas paroles derīguma termiņš ir ierobežots līdz minimumam.

    9.2 Maksājumu pakalpojumu sniedzēji nosaka autentifikācijas mēģinājumu maksimālo skaitu, pēc kura piekļuve interneta maksājumu pakalpojumam tiek bloķēta (īslaicīgi vai pastāvīgi). Ir noteikta droša procedūra, lai aktivizētu bloķētus interneta maksājumu pakalpojumus.

    9.3 Maksājumu pakalpojumu sniedzēji nosaka laika periodu, pēc kura neaktīva interneta maksājumu pakalpojumu sesija tiek automātiski pārtraukta.

Darījumu uzraudzība un pārraudzība

10. Darījumu uzraudzības un pārraudzības risinājumus, kas paredzēti, lai novērstu, atklātu un bloķētu krāpnieciskus maksājumu darījumus, izmanto pirms maksājumu pakalpojumu sniedzēja pēdējā pilnvarojuma; aizdomīgiem vai augsta riska darījumiem piemēro īpašu uzraudzības un izvērtēšanas procedūru. Līdzvērtīgus drošības uzraudzības un autorizācijas risinājumus ievieš arī e-mandātu izsniegšanai.

    10.1 Maksājumu pakalpojumu sniedzēji izmanto krāpšanas atklāšanas un novēršanas sistēmas vai risinājumus, lai identificētu aizdomīgus darījumu pirms maksājumu pakalpojumu sniedzējs to autorizē. Šāda sistēma balstās uz, piemēram, noteikumiem ar kritērijiem (piemēram, kompromitētu vai zagtu karšu datu melnais saraksts), un uzrauga klienta netipiskas uzvedības modeļus (piemēram, interneta protokola (IP) adreses maiņa[16] vai IP diapazona maiņa interneta maksājumu pakalpojumu sesijas laikā, kas tiek identificēta IP ģeogrāfiskās atrašanās vietas pārbaudē,[17] netipiskas e-komersanta kategorijas izmantošana vai konkrētam klientam neparasti darījuma dati, utt.). Šāda sistēma spēj noteikt datorvīrusa infekcijas pazīmes sesijas laikā un identificēt zināmos krāpšanas scenārijus. Uzraudzības un pārraudzības risinājumu apjoms, sarežģītība un pielāgošana tiek noteikti ievērojot aktuālos personas datu aizsardzības tiesību aktus un tie ir samērīgi ar riska novērtējuma rezultātiem.

    10.2 Maksājumu pakalpojumu sniedzēji iegādājas krāpšanas atklāšanas un novēršanas sistēmu vai risinājumu, lai uzraudzītu e-komersanta darbību.

    10.3 Maksājumu pakalpojumu sniedzēji veic darījumu pārbaudes un novērtēšanas procedūras pietiekami īsā laika periodā, lai nepamatoti neatliktu attiecīgā maksājuma izpildi.

    10.4 Ja maksājumu pakalpojumu sniedzējs saskaņā ar tā riska politiku, nolemj bloķēt maksājumu darījumu, kas identificēts, kā iespējami krāpniecisks, maksājumu pakalpojumu sniedzējs saglabā nobloķēšanu uz tik īsu laiku, cik vien tas iespējams, līdz drošības jautājumi ir atrisināti.

[16] IP adrese ir unikāls ciparu kods, kas identificē katru datoru, kas ir savienots ar internetu.

[17] "Geo-IP" pārbaudē tiek pārbaudīts, vai izdevēja valsts atbilst IP adresei, no kuras lietotājs uzsāk darījumu.

Slepenu maksājumu datu aizsardzība

11. Uzglabājot, apstrādājot vai pārsūtot slepenus maksājumu datus tie ir jāaizsargātos.

    11.1 Visi dati, ko izmanto, lai identificētu un autentificētu klientus (piemēram, pieslēgšanās, uzsākot interneta maksājumu vai izsniedzot, grozot vai atceļot e-mandātus), jānodrošina pret zādzībām, nesankcionētu piekļuvi vai grozīšanu.

    11.2 Maksājumu pakalpojumu sniedzēji nodrošina, ka, veicot slepenu maksājumu datu apmaiņu internetā, tiek nodrošināta droša šifrēšana[18] saziņā starp pusēm visā attiecīgās sakaru sesijas laikā, lai nodrošinātu datu konfidencialitāti un integritāti, izmantojot drošas un plaši atzītas šifrēšanas metodes.

    11.3 Maksājumu pakalpojumu sniedzēji, piedāvājot pieņēmēja pakalpojumus, aicina e-komersantus neglabāt jebkurus slepenus maksājumu datus. Gadījumā, ja e-komersants apstrādā, t.i., uzglabā, apstrādā vai pārsūta slepenus maksājumu datus, tad maksājumu pakalpojumu sniedzējs uz līguma pamata pieprasa e-komersantam ieviest nepieciešamos pasākumus, lai aizsargātu šos datus. Maksājumu pakalpojumu sniedzēji veic regulāras pārbaudes un ja maksājumu pakalpojumu sniedzēji konstatē, ka e-komersants, apstrādājot slepenus maksājumu datus, nav ieviesis nepieciešamos drošības pasākumus, tie rīkojas, lai izpildītu šīs līgumā paredzētās saistības, vai pārtrauc līgumu.

Klientu informēšana, izglītošana un komunikācija ar klientu

Klientu informēšana un izglītošana

12. Maksājumu pakalpojumu sniedzēji, ja nepieciešams, sniedz palīdzību un norādījumus klientiem attiecībā uz drošu interneta maksājumu pakalpojumu izmantošanu. Maksājumu pakalpojumu sniedzēji sazinās ar saviem klientiem tādā veidā, lai pārliecinātu viņus par saņemto ziņu īstumu.

    12.1 Maksājumu pakalpojumu sniedzēji nodrošina vismaz vienu drošu kanālu[19] pastāvīgai komunikācijai ar klientiem par pareizu un drošu interneta maksājumu pakalpojumu izmantošanu. Maksājumu pakalpojumu sniedzēji informē klientus par šo kanālu un skaidro, ka jebkura cita maksājumu pakalpojumu sniedzēja vārdā nosūtītā ziņa, izmantojot citus līdzekļus, piemēram, e-pastu, kas attiecas uz pareizu un drošu interneta maksājumu pakalpojumu izmantošanu, nav ticama. Maksājumu pakalpojumu sniedzējs skaidro:

[18] Droša vai pilnīga šifrēšana attiecas uz šifrēšanu avota sistēmā un ar atbilstošu atšifrēšanu, kas notiek mērķa gala sistēmā. ETSI EN 302, 109 V1.1.1. (2003-06)

[19] Piemēram, speciāla pastkastīte maksājumu pakalpojumu sniedzēja drošā tīmekļa vietnē.

- kārtību kādā klienti ziņo maksājumu pakalpojumu sniedzējam (par aizdomām) par krāpniecisku maksājumu, incidentiem vai novirzēm interneta maksājumu pakalpojumu sesijas laikā un/vai par iespējamiem sociālās inženierijas [20] centieniem;

- turpmākos soļus, t.i., kā maksājumu pakalpojumu sniedzējs sniegs atbildi klientam;

- kā maksājumu pakalpojumu sniedzējs informēs klientu par (potenciālajiem) krāpnieciskiem darījumiem vai brīdinās klientu par notikušu uzbrukumu (piemēram, pikšķerēšanas e-pasta ziņojumi).

12.2 Maksājumu pakalpojumu sniedzējs, izmantojot drošu kanālu, informē klientus par izmaiņām drošības procedūrās attiecībā uz interneta maksājumu pakalpojumiem. Visus brīdinājumus par būtiskiem potenciāliem riskiem (piemēram, brīdinājumi par sociālo inženieriju) sniedz izmantojot drošu kanālu.

12.3 Maksājumu pakalpojumu sniedzēji ievieš klientu palīdzības dienestu pieejamu visiem jautājumiem, sūdzībām, lūgumiem pēc atbalsta un paziņojumiem par anomālijām vai incidentiem attiecībā uz interneta maksājumiem un saistītajiem pakalpojumiem, un atbilstoši informē klientus par to, kā šādu palīdzību var saņemt.

12.4 Maksājumu pakalpojumu sniedzēji uzsāk klientu izglītības un izpratnes programmas, kas izstrādātas, lai nodrošinātu klientu sapratni, kā minimums par to, ka ir nepieciešams:

- aizsargāt savas paroles, kodu kalkulatorus un citus konfidenciālos datus;

- pienācīgi pārvaldīt personiskās ierīces drošību (piemēram, datoru), izmantojot drošības komponentu instalēšanu un atjaunināšanu (antivīruss, ugunsmūris, drošības ielāpi);

- izskatīt būtiskus apdraudējumus un riskus, kas saistīti ar programmatūras lejupielādi internetā, ja klients nevar būt pārliecināts, ka programmatūra ir oriģināla un nav mainīta;

- izmantot patiesu maksājumu pakalpojumu sniedzēja interneta maksājumu tīmekļa vietni.

[20] Sociālā inženierija šajā kontekstā nozīmē paņēmienus manipulācijai ar cilvēkiem, lai iegūtu informāciju (piemēram, izmantojot e-pastu vai tālruņa zvanus) vai izgūstot informāciju no sociālajiem tīkliem krāpšanas nolūkā, vai iegūstot neatļautu piekļuvi datoram vai tīklam.

12.5 Maksājumu pakalpojumu sniedzēji pieprasa e-komersantiem skaidri nodalīt ar maksājumiem saistītās procedūras no tiešsaistes veikala, lai atvieglotu klientiem noteikt, kad viņi komunicē ar maksājumu pakalpojumu sniedzēju nevis ar maksājuma saņēmēju (piemēram, novirzot klientu un atverot atsevišķu logu tā, ka maksājumu procedūra netiek rādīta e-komersanta ietvarā).

Paziņojumi un maksājumu limitu noteikšana

13. Maksājumu pakalpojumu sniedzēji nosaka maksājumu limitus un sniedz saviem klientiem iespēju izvēlēties turpmākus riska ierobežojošus pasākumus. Tie paredz arī brīdinājumus un klienta profila pārvaldības pakalpojumus.

13.1 Pirms sniegt klientam interneta maksājumu pakalpojumus, maksājumu pakalpojumu sniedzēji nosaka maksājumu limitu,[21] kas attiecas uz minētajiem pakalpojumiem (piemēram, ierobežojot katra atsevišķa maksājuma maksimālo summu vai kopsummu konkrētā laika periodā) un attiecīgi informē savus klientus. Maksājumu pakalpojumu sniedzēji ļauj klientiem bloķēt interneta maksājumu funkcionalitāti.

Klientu piekļuve informācijai par maksājumu uzsākšanas un izpildes statusu

14. Maksājumu pakalpojumu sniedzēji apliecina saviem klientiem maksājumu uzsākšanu un savlaicīgi sniedz klientiem nepieciešamo informāciju, lai pārbaudītu, ka maksājuma darījums ir pareizi uzsākts un/vai izpildīts.

14.1 [kredīta pārvedumi/e-mandāts] Maksājumu pakalpojumu sniedzēji nodrošina klientus ar reālā laika iespēju pārbaudīt darījumu izpildes statusu, kā arī konta atlikumu jebkurā laikā[22] drošā un uzticamā vidē.

14.2 Visi detalizētie elektroniskie paziņojumi un pārskati ir pieejami drošā un uzticamā vidē. Ja maksājumu pakalpojumu sniedzēji informē klientus par elektronisko paziņojumu pieejamību (piemēram, veicot periodisku e-paziņojuma izsūtīšanu, vai pēc darījumu izpildes), izmantojot alternatīvu kanālu, piemēram, SMS, e-pastu vai vēstuli, tad slepeni maksājumu dati nedrīkst tikt iekļauti šādos paziņojumos, vai, ja tie tiek iekļauti, tie ir jāmaskē.

III sadaļa. Pārejas noteikumi un īstenošana

15. Pamatnostādnes tiek piemērotas no 01.08.2015.

[21] Maksājumu limitus var piemērot vispārīgi (t. i., visiem maksājumu instrumentiem, kas ļauj veikt interneta maksājumus) vai individuāli.

[22] Izņemot ārkārtas situācijās tehnisku iemeslu dēļ vai būtisku incidentu gadījumā.

1. pielikums. Labas prakses piemēri

Papildus iepriekš noteiktajām prasībām, šajās pamatnostādnēs aprakstītas daži labas prakses piemēri, kas maksājumu pakalpojumu sniedzējiem un attiecīgajiem tirgus dalībniekiem tiek ieteikti, bet nav obligāti. Vienkāršības labad norādītas nodaļas, uz kurām attiecas šie labas prakses piemēri.

Vispārējā kontrole un drošības vide

Vadība

1. Drošības politiku nosaka atsevišķā dokumentā.

Riska kontrole un mazināšana

2. Maksājumu pakalpojumu sniedzēji nodrošina drošības risinājumus (piemēram, ierīces un/vai pielāgotas pārlūkprogrammas ar atbilstošu aizsardzību), lai aizsargātu klienta interfeisu pret to nelikumīgu lietošanu vai uzbrukumiem (piemēram, "cilvēks pārlūkprogrammā"(man in the browser) uzbrukumi).

Izsekojamība

3. Maksājumu pakalpojumu sniedzēji, piedāvājot pieņēmēja pakalpojumus, līgumā pieprasa e-komersantiem, kas uzglabā maksājumu informāciju ieviest atbilstošas procedūras izsekojamības nodrošināšanai.

Īpaša kontrole un drošības pasākumi interneta maksājumiem

Sākotnējā klienta identifikācija, informācija

4. Klients tā vietā, lai parakstītu noteikumus, kas iekļauti maksājumu pakalpojumu sniedzēja plašākā vispārējā pakalpojumu līgumā, paraksta atsevišķu pakalpojumu līgumu par interneta maksājumu darījumu veikšanu.

5. Maksājumu pakalpojumu sniedzēji nodrošina, ka klienti tiek patstāvīgi vai atbilstoši konkrētam gadījumam informēti, izmantojot piemērotus līdzekļus (piemēram, bukletus, tīmekļa vietnes lapas), un nodrošināti ar skaidriem un saprotamiem norādījumiem, izskaidrojot viņu atbildību par drošu pakalpojuma lietošanu.

Droša klienta autentifikācija

6. [kartes] E-komersanti atbalsta izdevēja drošu kartes turētāja autentifikāciju darījumiem ar karti, izmantojot internetu.

7. Klientu ērtībām maksājumu pakalpojumu sniedzēji apsver iespēju izmantot vienu drošu klientu autentifikācijas rīku visiem interneta maksājumu pakalpojumiem. Tas varētu palielināt risinājuma pieņemšanu starp klientiem un veicināt atbilstošu lietošanu.

8. Droša klientu autentifikācija iekļauj elementus, kas savieno autentifikāciju, ar noteiktu summu un maksājuma saņēmēju. Tas varētu nodrošināt klientus ar paaugstinātu drošību, kad viņš apstiprina maksājumus. Tehnoloģiskajam risinājumam, kas veiktu drošu autentificēšanas datu un darījumu dati sasaisti, jābūt nodrošinātam pret viltojumiem.

Slepenu maksājumu datu aizsardzība

9. Ir vēlams, ka e-komersanti, kas apstrādā slepenus maksājumu datus, atbilstoši apmāca savus krāpniecības novēršanas darbiniekus un regulāri atjaunina šīs apmācības, lai nodrošinātu, ka tiek saglabāta atbilstība dinamiskai drošības videi.

Klientu informēšana un izglītošana

10. Vēlams, lai maksājumu pakalpojumu sniedzēji, piedāvājot pakalpojumu iegādi, organizē izglītības programmas e-komersantiem par krāpšanas novēršanu.

Paziņojumi un maksājumu limitunoteikšana

11. Ievērojot norādītos maksājumu limitus, maksājumu pakalpojumu sniedzēji nodrošina savus klientus ar iespēju pārvaldīt šos limitus drošā un uzticamā vidē.

12. Maksājumu pakalpojumu sniedzēji ievieš brīdinājumus klientiem, piemēram, izmantojot tālruņa zvanus vai SMS, par aizdomīgiem vai augsta riska maksājumu darījumiem, kas pamatojas uz riska vadības politiku.

13. Maksājumu pakalpojumu sniedzēji ļauj klientiem noteikt vispārējus, personalizētus noteikumus, piemēram, savas uzvedības kritērijus attiecībā uz interneta maksājumiem un saistītajiem pakalpojumiem, piemēram, ka viņi varēs uzsākt maksājumus tikai no noteiktām valstīm, un ka maksājumi, kas uzsākti no citurienes ir jābloķē, vai ka viņi var iekļaut īpašus maksājumu saņēmējus baltajā vai melnajā sarakstā.