EBA/GL/2017/17

12/01/2018

Ghid

privind măsurile de securitate referitoare la riscurile operaționale și de securitate aferente serviciilor de plată, în temeiul Directivei (UE) 2015/2366(PSD2)

1. Conformitate și obligații de raportare

Statutul prezentului ghid

1. Prezentul document conține orientări emise în temeiul articolului 16 din Regulamentul (UE) nr. 1093/2010[1]. În conformitate cu articolul 16 alineatul (3) din Regulamentul (UE) nr. 1093/2010, autoritățile competente și instituțiile financiare trebuie să depună toate eforturile necesare pentru a respecta orientările.

2. Ghidul prezintă punctul de vedere al ABE privind practicile adecvate în materie de supraveghere în cadrul Sistemului european al supraveghetorilor financiari sau privind modul în care ar trebui aplicat dreptul Uniunii într-un anumit domeniu. Autoritățile competente cărora li se aplică ghidul, astfel cum sunt definite la articolul 4 alineatul (2) din Regulamentul (UE) nr. 1093/2010, trebuie să se conformeze și să îl integreze în practicile lor, după caz (de exemplu, prin modificarea cadrului legislativ sau a procedurilor de supraveghere ale acestora), inclusiv în cazurile în care anumite puncte din cuprinsul documentului sunt adresate în primul rând instituțiilor.

Cerințe de raportare

3. În conformitate cu articolul 16 alineatul (3) din Regulamentul (UE) nr. 1093/2010, autoritățile competente trebuie să notifice ABE dacă se conformează sau intenționează să se conformeze prezentului ghid sau, în caz contrar, motivele neconformării, până la 12.03.2018. În absența unei notificări până la acest termen, ABE va considera că autoritățile competente nu s-au conformat. Notificările se trimit prin intermediul formularului disponibil pe site-ul ABE la adresa compliance@eba.europa.eu , cu mențiunea „EBA/GL/2017/17”. Notificările trebuie trimise de persoane care au autoritatea de a raporta cu privire la respectarea ghidului în numele autorităților competente. Orice schimbare cu privire la starea de conformare trebuie adusă, de asemenea, la cunoștința ABE.

4. Notificările vor fi publicate pe site-ul ABE, în conformitate cu articolul 16 alineatul (3).

[1] Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea bancară europeană), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/78/CE a Comisiei (JO L 331, 15.12.2010, p.12).

2. Obiect, domeniu de aplicare și definiții

Obiectul și domeniul de aplicare

5. Prezentul ghid a fost elaborat ca urmare a mandatului acordat ABE în baza articolului 95 alineatul (3) din Directiva (UE) nr. 2015/2366[2] (PSD2).

6. Prezentul ghid cuprinde cerințele privind elaborarea, punerea în aplicare și monitorizarea măsurilor de securitate pe care prestatorii de servicii de plată trebuie să le ia, în conformitate cu articolul 95 alineatul (1) din Directiva (UE) 2015/2366 în vederea gestionării riscurilor de operaționale și de securitate legate de serviciile de plată pe care le furnizează.

Destinatari

7. Prezentul ghid se adresează prestatorilor de servicii de plată (PSP), astfel cum sunt definiți în articolul 4 alineatul (11) din Directiva (UE) 2015/2366 și astfel cum se menționează în definiția termenului „instituții financiare" la articolul 4 alineatul (1) din Regulamentul (UE) 1093/2010 și autorităților competente (AC), astfel cum sunt definite la articolul 4 alineatul (2) punctul (i) din Regulamentul respectiv, prin trimitere la Directiva 2007/64/CE abrogată[3] (în prezent, Directiva (UE) 2015/2366[4]).

Definiții

8. Cu excepția cazului în care se prevede altfel, termenii utilizați și definiți în Directiva (UE) 2015/2366 au același înțeles în prezentul ghidul. În plus, în sensul prezentului ghid, se aplică următoarele definiții:

Organul de conducere	– În cazul prestatorilor de servicii de plată care sunt instituții de credit, acest termen are același înțeles ca definiția de la articolul 3 alineatul (1) punctul (7)din Directiva 2013/36/UE[5];

[2] Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului din 25 noiembrie 2015 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 2002/65/CE, 2009/110/CE și 2013/36/UE și a Regulamentului (UE) nr. 1093/2010 și de abrogare a Directivei 2007/64/CE (JO L 337, 23.12.2015, p. 35).
[3] Directiva 2007/64/CE a Parlamentului European și a Consiliului din 13 noiembrie 2007 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 97/7/CE, 2002/65/CE, 2005/60/CE și 2006/48/CE și de abrogare a Directivei 97/5/CE (JO L 319, 5.12.2007, pag. 1).
[4] În conformitate cu al doilea subparagraf al articolului 114 din Directiva (UE) 2015/2366, orice trimitere la Directiva 2007/64/CE care a fost abrogată se interpretează drept trimitere la Directiva (UE) 2015/2366 și se citește în conformitate cu tabelul de corespondență din anexa II la Directiva (UE) 2015/2366.
[5] Directiva 2013/36/UE a Parlamentului European și a Consiliului cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit și a firmelor de investiții, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE (JO L 176, 27.6.2013, pag. 338).

	– În cazul prestatorilor de servicii de plată care sunt instituții de plată sau instituții emitente de monedă electronică, acest termen se referă la directorii sau persoanele responsabile cu gestionarea prestatorilor de servicii de plată și, dacă este cazul, la persoanele responsabile cu gestionarea activităților legate de serviciile de plată ale prestatorilor de servicii de plată; – În cazul prestatorilor de servicii de plată la care se face trimitere la articolul 1 alineatul (1) punctele (c), (e) și (f) din Directiva (UE) 2015/2366, acest termen are semnificația conferită în temeiul legislației naționale sau a UE aplicabile.
Incident operațional sau de securitate	Un eveniment unic sau o serie de evenimente corelate neprevăzute de prestatorul de servicii de plată, care are/au sau va/vor avea probabil un impact negativ asupra integrității, disponibilității, confidențialității, autenticității și/sau continuității serviciilor aferente plăților.
Conducere superioară	(a) În cazul prestatorilor de servicii de plată care sunt instituții de credit, acest termen are același înțeles ca definiția de la articolul 3 alineatul (1) punctul (9) din Directiva 2013/36/UE; (b) În cazul prestatorilor de servicii de plată care sunt instituții de plată și instituții emitente de monedă electronică, acest termen se referă la persoanele fizice care ocupă funcții executive în cadrul unei instituții și care sunt responsabile și răspunzătoare în fața organului de conducere pentru gestionarea zilnică a prestatorilor de servicii de plată; (c) În cazul prestatorilor de servicii de plată la care se face trimitere la articolul 1 alineatul (1) punctele (c), (e) și (f) din Directiva (UE) 2015/2366, acest termen are semnificația conferită în temeiul legislației naționale sau a UE aplicabile.
Risc de securitate	Riscul care rezultă din procesele interne sau evenimentele externe eșuate sau necorespunzătoare, care au sau ar putea avea un impact negativ asupra disponibilității, integrității, confidențialității și asupra sistemelor de tehnologie a informației și a comunicațiilor și/sau asupra informațiilor utilizate pentru furnizarea serviciilor de plată. Sunt incluse riscurile aferente atacurilor cibernetice sau securitatea fizică necorespunzătoare.
Apetitul pentru risc	Nivelul și tipurile cumulate de risc pe care o instituție este dispusă să și le asume în limita capacității sale de risc, conform modelului său de afaceri, în vederea realizării obiectivelor sale strategice.

3. Punerea în aplicare

Data aplicării

9. Prezentul ghid se aplică de la 13 ianuarie 2018.

4. Ghid

Orientarea 1: Principii generale

1.1 Toți prestatorii de servicii de plată trebuie să respecte toate prevederile din prezentul ghid. Nivelul de detaliu trebuie să fie proporțional cu dimensiunea prestatorului de servicii de plată, precum și cu natura, scopul, complexitatea și caracterul riscant al serviciilor respective pe care prestatorul de servicii de plată le furnizează sau intenționează să le furnizeze.

Orientarea 2: Guvernanță

Cadrul de gestionare a riscurilor operaționale și de securitate

2.1 Prestatorii de servicii de plată trebuie să stabilească un cadru eficient de gestionare a riscurilor operaționale și de securitate (denumit în continuare, cadru de gestionare a riscurilor), care trebuie aprobat și revizuit, cel puțin o dată pe an, de către organul de conducere și, dacă este cazul, de conducerea superioară. Acest cadru trebuie să pună accentul pe măsurile de securitate de diminuare a riscurilor operaționale și de securitate și trebuie integrat în întregime în procesele de gestionare a riscurilor generale ale prestatorilor de servicii de plată.

2.2 Cadrul de gestionare a riscurilor trebuie:

a) să includă un document de politică de securitate cuprinzător, astfel cum menționează la articolul 5 alineatul (1) litera (j) din Directiva (UE) 2015/2366;

b) să fie în concordanță cu apetitul pentru risc al prestatorului de servicii de plată;

c) să definească și să desemneze rolurile și responsabilitățile cheie, precum și liniile de raportare relevante, necesare pentru punerea în aplicare a măsurilor de securitate și pentru gestionarea riscurilor operaționale și de securitate;

d) să stabilească sistemele și procedurile necesare pentru identificarea, măsurarea, monitorizarea și gestionarea gamei de riscuri, care decurg din activitățile legate de plată ale prestatorului de servicii de plată și la care acesta este expus, inclusiv măsurile de asigurare a continuității activității.

2.3 Prestatorii de servicii de plată se asigură că respectivul cadru de gestionare a riscurilor este documentat în mod corespunzător și actualizat cu „lecțiile învățate” și documentate pe parcursul punerii în aplicare și monitorizării acestuia.

2.4 Prestatorii de servicii de plată trebuie să se asigure că, înainte de o modificare majoră la nivelul infrastructurii, al proceselor sau al procedurilor și că după fiecare incident operațional sau de securitate major care afectează securitatea serviciilor de plată furnizate, aceștia examinează

necesitatea de a modifica sau de a îmbunătăți cadrul de gestionare a riscurilor, fără întârzieri nejustificate.

Gestionarea riscurilor și modelele de control

2.5 Prestatorii de servicii de plată trebuie să stabilească trei modalități de apărare eficiente sau un model de control și de gestionare a riscurilor intern echivalent, pentru a identifica și gestiona riscurile operaționale și de securitate. Prestatorii de servicii de plată trebuie să se asigure că modelul de control intern menționat mai sus are suficientă autoritate, independență și resurse și modalități de raportare directă către organul de conducere și, dacă este cazul, către conducerea superioară.

2.6 Măsurile de securitate prevăzute în acest ghid trebuie să fie auditate de auditori cu experiență în securitatea IT și plăți și să fie independenți din punct de vedere operațional de prestatorul de servicii de plată sau în cadrul acestuia. Frecvența și punctul central al unor astfel de audituri trebuie să ia în considerare riscurile de securitate corespunzătoare.

Externalizarea

2.7 Prestatorii de servicii de plată trebuie să asigure eficacitatea măsurilor de securitate prevăzute în acest ghid, atunci când funcțiile operaționale ale serviciilor de plată, inclusiv ale sistemelor IT, sunt externalizate.

2.8 Prestatorii de servicii de plată trebuie să se asigure că obiectivele de securitate, măsurile și obiectivele de performanță corespunzătoare și proporționale sunt incluse în contractele și acordurile la nivel de servicii încheiate cu prestatorii către care au externalizat funcțiile respective. Prestatorii de servicii de plată trebuie să monitorizeze și să se asigure că prestatorii respectivi îndeplinesc obiectivele de securitate, măsurile de securitate și obiectivele de performanță.

Orientarea 3: Evaluarea riscurilor

Identificarea funcțiilor, a proceselor și a activelor

3.1 Prestatorii de servicii de plată trebuie să identifice, să stabilească și să actualizeze regulat inventarul funcțiilor aferente activității sale, al rolurilor cheie și al proceselor de asistență, pentru a identifica importanța fiecărei funcții, a fiecărui rol și a proceselor de asistență, precum și interdependențele acestora privind riscurile operaționale și de securitate.

3.2 Prestatorii de servicii de plată trebuie să identifice, să stabilească și să actualizeze regulat inventarul activelor informaționale, spre exemplu, sistemele TIC, configurațiile acestora, alte infrastructuri, precum și interconexiunile cu alte sisteme externe și interne, în vederea gestionării activelor care sprijină procesele și funcțiile esențiale aferente activității acestora.

Clasificarea funcțiilor, a proceselor și a activelor

3.3 Prestatorii de servicii de plată trebuie să clasifice funcțiile aferente activității, procesele de asistență și activele informaționale identificate, în funcție de starea critică.

Evaluarea riscurilor funcțiilor, a proceselor și a activelor

3.4 Prestatorii de servicii de plată trebuie să se asigure că monitorizează permanent amenințările și vulnerabilitățile și că revizuiesc regulat scenariile de risc, cu impact asupra funcțiilor aferente activității, asupra proceselor esențiale și asupra activelor informaționale. Ca parte a obligației de a efectua și de a furniza autorităților competente o evaluare a riscurilor actualizată și cuprinzătoare a riscurilor operaționale și de securitate referitoare la serviciile de plată pe care le furnizează și în ceea ce privește adecvarea măsurilor de atenuare și a mecanismelor de control implementate ca răspuns la riscurile respective, astfel cum este prevăzut la articolul 95 alineatul (2) din Directiva (UE) 2015/2366, prestatorii de servicii de plată trebuie să efectueze și să documenteze evaluările riscurilor, cel puțin anual sau la intervale mai scurte, astfel cum este stabilit de autoritățile competente, privind funcțiile, procesele și activele informaționale pe care le-au identificat și clasificat, în vederea identificării și evaluării riscurilor operaționale și de securitate cheie. Astfel de evaluări ale riscurilor trebuie să fie efectuate înaintea oricărei modificări majore la nivelul infrastructurii, al proceselor și al procedurilor care afectează securitatea serviciilor de plată.

3.5 Pe baza evaluărilor riscurilor, prestatorii de servicii de plată trebuie să stabilească în ce măsură și dacă sunt necesare sau nu modificări ale măsurilor de securitate existente, ale tehnologiilor utilizate și ale procedurilor sau serviciilor de plată oferite. Prestatorii de servicii de plată trebuie să ia în considerare durata necesară pentru punerea în aplicare a modificărilor și durata necesară pentru luarea măsurilor de securitate în vederea minimizării incidentelor de securitate sau operaționale, a fraudei și a efectelor potențial perturbatoare în ceea ce privește furnizarea serviciilor de plată.

Orientarea 4: Protecția

4.1 Prestatorii de servicii de plată trebuie să elaboreze și să pună în aplicare măsurile de securitate preventive împotriva riscurilor operaționale și de securitate identificate. Măsurile respective trebuie să asigure un nivel corespunzător de securitate, în conformitate cu riscurile identificate.

4.2 Prestatorii de servicii de plată trebuie să elaboreze și să pună în aplicare o abordare de tipul „apărare în adâncime”, instituind controale pe mai multe niveluri, care vizează persoane, procese și tehnologia, fiecare nivel servind drept mecanism de siguranță pentru nivelurile anterioare. Apărarea în adâncime trebuie înțeleasă ca definind mai multe controale care acoperă același risc, precum principiul celor patru ochi, autentificarea pe baza a doi factori, segmentarea rețelei și multiple mecanisme firewall.

4.3 Prestatorii de servicii de plată trebuie să asigure confidențialitatea, integritatea și disponibilitatea activelor fizice și logice, ale resurselor și ale datelor de plată sensibile esențiale ale utilizatorilor

de servicii de plată, fie că sunt în stare de repaus, în tranzit sau în folosință. Dacă datele includ date cu caracter personal, astfel de măsuri trebuie puse în aplicare în conformitate cu Regulamentul (UE) 2016/679[6] sau, dacă este cazul, Regulamentul (CE) 45/2001.[7]

4.4 Prestatorii de servicii de plată trebuie să stabilească în permanență dacă modificările la nivelul mediului operațional existent influențează măsurile de securitate existente sau dacă impun adoptarea altor măsuri pentru atenuarea riscurilor implicate. Aceste modificări trebuie să facă parte din procesul formal de gestionare a modificărilor al prestatorilor de servicii de plată, proces care trebuie să garanteze că modificările sunt planificate, testate, documentate și autorizate în mod corespunzător. Pe baza amenințărilor la adresa securității constatate și a modificărilor efectuate, trebuie să se realizeze un test, care să includă scenariile atacurilor potențiale cunoscute și relevante.

4.5 În conceperea, dezvoltarea și furnizarea de servicii de plată, prestatorii de servicii de plată trebuie să se asigure că se aplică separarea sarcinilor și principiile „privilegiilor minime”. Prestatorii de servicii de plată trebuie să acorde o atenție deosebită separării mediilor IT, în special în ceea ce privește dezvoltarea, testarea și mediile de producție.

Integritatea și confidențialitatea datelor și a sistemelor

4.6 În conceperea, dezvoltarea și furnizarea de servicii de plată, prestatorii de servicii de plată trebuie să se asigure că direcționarea, colectarea, prelucrarea, stocarea și/sau arhivarea și vizualizarea datelor privind plățile sensibile ale utilizatorului de servicii de plată sunt adecvate, relevante și limitate la ceea ce este necesar pentru prestarea serviciilor de plată.

4.7 Prestatorii de servicii de plată trebuie să verifice în mod regulat dacă programul de software utilizat pentru prestarea serviciilor de plată, inclusiv programul de software legat de plăți al utilizatorilor este actualizat și dacă patch-urile de securitate sunt introduse. Prestatorii de servicii de plată trebuie să se asigure că s-au introdus mecanismele de verificare a integrității, pentru a verifica integritatea programului de software, a firmware și a informațiilor privind serviciile de plată ale acestora.

Securitatea fizică

4.8 Prestatorii de servicii de plată trebuie să introducă măsurile de securitate fizică corespunzătoare, în special pentru protejarea datelor privind plățile sensibile ale utilizatorilor de servicii de plată, precum și a sistemelor TIC utilizate pentru prestarea serviciilor de plată.

[6] Regulamentul (UE) al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul General privind Protecția Datelor) (JO L 119, 4.5.2016, p. 1).

[7] Regulamentul (CE) nr 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de instituțiile și organele comunitare și libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

Controlul accesului

4.9 Accesul logic și fizic la sistemele TIC trebuie să fie permis numai persoanelor autorizate. Autorizarea trebuie atribuită în conformitate cu sarcinile și responsabilitățile personalului, limitată la persoanele care sunt instruite și monitorizate în mod corespunzător. Prestatorii de servicii de plată trebuie să instituie controale care să restricționeze în mod fiabil un astfel de acces la sistemele TIC pentru persoanele cu o cerință operațională legitimă. Accesul electronic prin depunerea de cereri de acces la date și sisteme trebuie să fie limitat la minimul necesar pentru prestarea serviciului relevant.

4.10 Prestatorii de servicii de plată trebuie să instituie controale stricte privind accesul privilegiat la sisteme, prin limitarea strictă și prin supravegherea îndeaproape a personalului cu drepturi de acces la sisteme de nivel superior. Trebuie implementate controale, precum accesul în funcție de roluri, logarea și examinarea activităților sistemelor utilizatorilor privilegiați, autentificarea puternică și monitorizarea în scopul identificării anomaliilor. Prestatorii de servicii de plată trebuie să gestioneze drepturile de acces la activele informaționale și sistemele lor de asistență pe baza „necesității de a cunoaște”. Drepturile de acces trebuie revizuite periodic.

4.11 Jurnalele de acces trebuie păstrate o perioadă de timp proporțională cu starea critică a funcțiilor aferente activității, a proceselor de asistență și a activelor informaționale identificate, în conformitate cu GL 3.1 și Gl 3.2, fără a aduce atingere cerințelor de păstrare a datelor, prevăzute în legislația națională și a UE. Prestatorii de servicii de plată trebuie să utilizeze aceste informații pentru facilitarea identificării și investigării activităților anormale, depistate în cadrul prestării serviciilor de plată.

4.12 Pentru a asigura comunicarea în condiții de siguranță și reducerea riscurilor, accesul administrativ de la distanță la componentele TIC esențiale trebuie acordat numai pe baza principiului necesității de a cunoaște și atunci când se utilizează soluții de autentificare.

4.13 Funcționarea produselor, a instrumentelor și a procedurilor referitoare la procesele de control al accesului trebuie să protejeze procesele de control al accesului împotriva compromiterii sau eludării acestora. Aceasta include înregistrarea, livrarea, revocarea și retragerea produselor, a instrumentelor și a procedurilor corespunzătoare.

Orientarea 5: Depistarea

Monitorizarea continuă și depistarea

5.1 Prestatorii de servicii de plată trebuie să elaboreze și să implementeze procese și competențe de monitorizare continuă a funcțiilor aferente activității, a proceselor de asistență și a activelor informaționale, pentru a depista activitățile anormale în ceea ce privește prestarea serviciilor de plată. În cadrul monitorizării continue, prestatorii de servicii de plată trebuie să introducă capacități corespunzătoare și eficiente de depistare a intruziunilor logice și fizice, precum și a încălcărilor confidențialității, ale integrității și ale disponibilității activelor informaționale utilizate în prestarea serviciilor de plată.

5.2 Monitorizarea continuă și procesele de depistare trebuie să acopere:

a) Factorii interni și externi relevanți, inclusiv funcțiile administrative privind TIC și cele aferente activității;

b) Operațiunile pentru depistarea utilizării abuzive a accesului de către prestatorii de servicii sau de către alte entități și

c) Amenințările interne și externe potențiale.

5.3 Prestatorii de servicii de plată trebuie să pună în aplicare măsuri de detecție pentru a identifica eventualele scurgeri de informații, coduri dăunătoare și alte amenințări la adresa securității și vulnerabilitățile cunoscute în mod public ale programelor de software și hardware și pentru a verifica existența unor noi actualizări de securitate corespunzătoare.

Monitorizarea și raportarea incidentelor operaționale sau de securitate

5.4 Prestatorii de servicii de plată trebuie să stabilească pragurile și criteriile corespunzătoare pentru clasificarea unui eveniment drept incident operațional sau de securitate, astfel cum este prevăzut în secțiunea „definiții” din prezentul ghid, precum și drept indicatori de alertă timpurie care ar trebui să servească drept alertă pentru prestatorul de servicii de plată, pentru a permite depistarea timpurie a incidentelor operaționale și de securitate.

5.5 Prestatorii de servicii de plată trebuie să instituie procese corespunzătoare și structuri organizaționale pentru a asigura monitorizarea, manevrarea și urmărirea integrate și consecvente ale incidentelor operaționale sau de securitate.

5.6 Prestatorii de servicii de plată trebuie să elaboreze o procedură privind raportarea către conducerea superioară a unor astfel de incidente operaționale și de securitate, precum și a plângerilor legate de securitate ale clienților.

Orientarea 6: Continuitatea activității

6.1 Prestatorii de servicii de plată trebuie să stabilească un proces solid de gestionare a continuității activității pentru a maximiza în permanență capacitatea de prestare de servicii de plată și pentru a limita pierderile în caz de întrerupere gravă a activității.

6.2 Pentru a stabili un plan solid de gestionare a continuității activității, prestatorii de servicii de plată trebuie să analizeze cu grijă expunerea la întreruperea gravă a activității și să evalueze, cantitativ și calitativ, impactul potențial al acestora, folosind date interne și/sau externe și analize pe bază de scenariu. Pe baza funcțiilor, a proceselor, a sistemelor, a operațiunilor și a interdependențelor esențiale, clasificate și identificate, în conformitate cu GL 3.1 până la GL 3.3, prestatorii de servicii de plată trebuie să prioritizeze acțiunile de continuitate a activității, folosind o abordare bazată pe riscuri, care se poate fundamenta pe evaluările riscurilor efectuate în temeiul GL 3. În funcție de modelul de afaceri al prestatorului de servicii de plată, acesta poate, spre exemplu, facilita prelucrarea ulterioară a operațiunilor esențiale, în timp ce continuă eforturile de remediere.

6.3 Pe baza analizei efectuate în temeiul GL 6.2, prestatorii de servicii de plată trebuie să introducă:

a) planuri de continuitate a activității pentru a se asigura că pot răspunde în mod corespunzător la urgențe și că pot păstra activitățile lor operaționale esențiale;

b) Măsuri de atenuare care urmează să fie adoptate în cazul încetării prestării serviciilor de plată și în cazul rezilierii contractelor existente, pentru evitarea efectelor negative asupra sistemelor de plată și asupra utilizatorilor de servicii de plată și pentru a asigura efectuarea operațiunilor de plată în așteptare.

Planificarea continuității activității pe bază de scenariu

6.4 Prestatorul de servicii de plată trebuie să ia în considerare o serie de scenarii diferite, inclusiv cele extreme sau plauzibile, la care ar putea fi expus și să evalueze impactul potențial al unor astfel de scenarii.

6.5 Pe baza analizei efectuate în temeiul GL 6.2 și a potențialelor scenarii identificate în temeiul GL 6.4, prestatorul de servicii de plată trebuie să dezvolte planuri de răspuns și de redresare, care trebuie:

a) Să pună accentul pe impactul asupra funcționării funcțiilor, a proceselor, a sistemelor, a operațiunilor și a interdependențelor esențiale;

b) Să fie documentate și puse la dispoziția unităților operaționale și de asistență și ușor accesibile în caz de urgență;

c) Să fie actualizate în conformitate cu lecțiile învățate din teste, cu noile riscuri și amenințări identificate și cu prioritățile și obiectivele de redresare modificate.

Testarea planurilor de continuitate a activității

6.6 Prestatorii de servicii de plată trebuie să testeze planurile de continuitate a activității și să se asigure că funcționarea funcțiilor, a proceselor, a sistemelor, a operațiunilor și a interdependențelor esențiale ale acestora sunt testate cel puțin anual. Planurile trebuie să sprijine obiectivele de a proteja și, dacă este cazul, a restabili integritatea și disponibilitatea operațiunilor lor și confidențialitatea activelor lor informaționale.

6.7 Planurile trebuie să fie actualizate cel puțin anual, pe baza rezultatelor testelor, a informațiilor privind amenințările curente, a partajării de informații și a lecțiilor învățate din evenimentele anterioare și a obiectivelor de redresare care se modifică, precum și pe baza analizei scenariilor plauzibile din punct de vedere tehnic și operațional, care nu au avut încă loc și, dacă este cazul, după modificările la nivelul sistemelor și proceselor. Prestatorii de servicii de plată trebuie să se consulte și să coopereze cu părțile interesate interne și externe, pe parcursul elaborării planurilor de continuitate a activității.

6.8 Testarea planurilor de continuitate a activității ale prestatorilor de servicii de plată trebuie:

a) Să includă un set adecvat de scenarii, astfel cum se menționează în GL 6.4;

b) Să fie concepute pentru a contesta presupunerile pe care se bazează planurile de continuitate a activității, inclusiv mecanismele de guvernanță și planurile de comunicare în situații de criză; și

c) Să includă proceduri pentru a verifica competența personalului și procese de răspuns n mod corespunzător la scenariile de mai sus.

6.9 Prestatorii de servicii de plată trebuie să supravegheze regulat eficiența planurilor de continuitate a activității și să documenteze și să analizeze orice provocări sau deficiențe rezultate în urma testelor.

Comunicarea în situații de criză

6.10 În cazul unei perturbări sau al unei urgențe și pe parcursul punerii în aplicare a planurilor de continuitate a activității, prestatorii de servicii de plată trebuie să se asigure că au introdus măsuri de comunicare în situații de criză eficiente, astfel încât toate părțile interesate interne și externe relevante, inclusiv prestatorii de servicii externi să fie informați în timp util și în mod corespunzător.

Orientarea 7: Testarea măsurilor de securitate

7.1 Prestatorii de servicii de plată trebuie să elaboreze și să pună în aplicare un cadru de testare, care să valideze robustețea și eficiența măsurilor de securitate și să se asigure că respectivul cadru este adaptat pentru a lua în considerare noile amenințări și vulnerabilități, identificate prin intermediul activităților de monitorizare a riscurilor.

7.2 Prestatorii de servicii de plată trebuie să se asigure că testele se efectuează în eventualitatea unor modificări la nivelul infrastructurii, al proceselor și al procedurilor și dacă modificările sunt efectuate, ca urmare a incidentelor operaționale sau de securitate majore.

7.3 Cadrul de testare trebuie să cuprindă, de asemenea, măsurile de securitate relevante cu privire la (i) terminalele de plată și dispozitivele utilizate pentru prestarea serviciilor de plată, (ii) terminalele de plată și dispozitivele utilizate pentru autentificarea utilizatorului de servicii de plată și (iii) dispozitivele și programul de software furnizat de prestatorul de servicii de plată utilizatorului de servicii de plată pentru a genera/primi un cod de autentificare.

7.4 Cadrul de testare trebuie să asigure că testele:

a) Sunt efectuate ca parte a procesului formal de gestionare a modificărilor, pentru a asigura robustețea și eficiența acestora;

b) Sunt efectuate de verificatori independenți, care au cunoștințe, competențe și expertiză suficiente în testarea măsurilor de securitate a serviciilor de plată și nu sunt implicați în dezvoltarea măsurilor de securitate aferente serviciilor de plată sau sistemelor care urmează să fie testate, cel puțin pentru testele finale înainte de a pune în aplicare măsurile de securitate;

c) Includ analize cu scanere de vulnerabilitate și teste de penetrare corespunzătoare nivelului de risc identificat în cadrul serviciilor de plată.

7.5 Prestatorii de servicii de plată trebuie să efectueze teste în permanență și în mod repetat cu privire la măsurile de securitate ale serviciilor lor de plată. În cazul sistemelor care sunt esențiale pentru furnizarea serviciilor de plată (astfel cum este descris în GL 3.2), aceste teste vor fi efectuate cel puțin anual. Sistemele care nu sunt esențiale trebuie testate regulat printr-o abordare bazată pe riscuri, dar cel puțin la fiecare trei ani.

7.6 Prestatorii de servicii de plată trebuie să monitorizeze și să evalueze rezultatele testelor efectuate și să-și actualizeze măsurile de securitate în mod corespunzător și fără întârzieri nejustificate în ceea ce privește sistemele esențiale.

Orientarea 8: Conștientizarea situației și învățarea continuă

Peisajul amenințărilor și conștientizarea situației

8.1 Prestatorii de servicii de plată trebuie să înființeze și să pună în aplicare procese și structuri operaționale, pentru a identifica și supraveghea constant amenințările la adresa securității și cele operaționale, care ar putea afecta semnificativ capacitatea acestora de a furniza servicii de plată.

8.2 Prestatorii de servicii de plată trebuie să analizeze incidentele operaționale și de securitate, care au fost identificate sau care au avut loc în cadrul și/sau în afara organizației. Prestatorii de servicii de plată trebuie să ia în considerare lecțiile cheie învățate din aceste analize și să actualizeze în consecință măsurile de securitate.

8.3 Prestatorii de servicii de plată trebuie să supravegheze activ dezvoltările în tehnologie, pentru a se asigura că sunt conștienți de riscurile de securitate.

Programe de formare și de conștientizare în materie de securitate

8.4 Prestatorii de servicii de plată trebuie să stabilească un program de formare pentru toți membrii personalului, pentru a se asigura că aceștia sunt instruiți pentru a-și îndeplini sarcinile și responsabilitățile, în conformitate cu procedurile și politicile de securitate relevante, în vederea diminuării erorii umane,a furtului, a fraudei, a utilizării necorespunzătoare sau a pierderii. Prestatorii de servicii de plată trebuie să se asigure că programul de formare prevede instruirea membrilor personalului cel puțin anual și mai frecvent, dacă este cazul.

8.5 Prestatorii de servicii de plată trebuie să se asigure că membrii personalului care îndeplinesc rolurile cheie identificate conform GL 3.1 sunt instruiți anual privind securitatea informațiilor vizate sau mai frecvent, dacă este cazul.

8.6 Prestatorii de servicii de plată trebuie să elaboreze și să pună în aplicare periodic programe de conștientizare în domeniul securității, pentru a-și educa personalul și pentru a aborda riscurile aferente securității informațiilor. Aceste programe ar trebui să impună personalului prestatorului de servicii de plată raportarea oricărui incident sau a oricărei activități neobișnuite.

Orientarea 9: Gestionarea serviciilor de plată în relația cu utilizatorul

Gradul de conștientizare al utilizatorului de servicii de plată privind riscurile de securitate și acțiunile de diminuare a riscurilor

9.1 Prestatorii de servicii de plată trebuie să stabilească și să pună în aplicare procese de sporire a gradului de conștientizare al utilizatorilor de servicii de plată cu privire la riscurile de securitate asociate cu serviciile de plată, acordând asistență și îndrumare utilizatorilor de servicii de plată.

9.2 Asistența și îndrumarea acordate utilizatorilor de servicii de plată trebuie să fie actualizate în funcție de noile amenințări și vulnerabilități, iar utilizatorul de servicii de plată trebuie să fie informat despre modificări.

9.3 În cazul în care funcționalitatea produsului o permite, prestatorii de servicii de plată trebuie să le permită utilizatorilor de servicii de plată să dezactiveze funcționalitățile de plată specifice, aferente serviciilor de plată furnizate de prestatorul de servicii de plată, utilizatorului de servicii de plată.

9.4 În cazul în care, în conformitate cu articolul 68 alineatul (1) din Directiva (UE) 2015/2366, un prestator de servicii de plată a acceptat limitele de cheltuieli ale plătitorului în ceea ce privește operațiunile de plată efectuate prin intermediul instrumentelor de plată specifice, prestatorul de servicii de plată trebuie să ofere plătitorului opțiunea de a ajusta aceste limite până la limita maximă admisă.

9.5 Prestatorii de servicii de plată trebuie să acorde utilizatorilor de servicii de plată opțiunea de a primi alerte referitoare la încercările inițiate și/sau eșuate de începere a operațiunilor de plată, permițându-le să depisteze utilizarea frauduloasă sau malițioasă a conturilor lor.

9.6 Prestatorii de servicii de plată trebuie să-i informeze pe utilizatorii de servicii de plată despre actualizările procedurilor de securitate, care afectează utilizatorii de servicii de plată în ceea ce privește prestarea serviciilor de plată.

9.7 Prestatorii de servicii de plată trebuie să acorde asistență utilizatorilor de servicii de plată în orice chestiuni, cereri de sprijin și notificări de anomalii sau chestiuni referitoare la probleme de securitate legate de serviciile de plată. Utilizatorii de servicii de plată trebuie să fie informați în mod corespunzător despre modul de obținere a asistenței respective.