BANCA NAȚIONALĂ A ROMÂNIEI

RUXANDRA AVRAM , Director
Direcția monitorizare a infrastructurilor pieței financiare și a plăților

04, OCTOMBRIE 2018

NOI REGLEMENTĂRI EUROPENE CU IMPACT ASUPRA SERVICIILOR BANCARE

Cadrul legislativ în temeiul PSD2

- **EBA/GL/2017/17** privind măsurile de securitate referitoare la riscurile operaționale și de securitate aferente serviciilor de plată, în temeiul PSD2
- **EBA/GL/2017/10** privind raportarea incidentelor majore în temeiul PSD2
- **EBA/GL/2018/05** referitor la cerințele de raportare a datelor privind fraudele din articolul 96 alineatul (6) din PSD2

Autoritățile competente

Aplicarea cadrului legislativ PSD2

Prestatorii de servicii de plată

EBA/GL/2017/17 privind măsurile de securitate referitoare la riscurile operaționale și de securitate aferente serviciilor de plată, în temeiul PSD2

MASURI DE SECURITATE

- **1. Cadrul de gestionare a riscurilor operaţionale si de securitate**
- **2. Evaluarea riscurilor**
- **3. Protecţia – masuri de securitate preventive**
- **4. Monitorizarea continuă si depistarea activităţilor anormale**
- **5. Continuitatea activităţii**
- **6. Testarea măsurilor de securitate**
- **7. Conștientizarea situaţiei si învăţarea continuă**
- **8. Gestionarea serviciilor de plată în relaţia cu utilizatorul**

MASURI DE SECURITATE

1. Cadrul de gestionare a riscurilor operaţionale si de securitate

- document de **politică de securitate** cuprinzător, astfel cum menţionează la **Art. 5 (1) lit. j) - PSD2**;

- să fie în **concordanţă cu apetitul pentru risc** al prestatorului de servicii de plată;

- definească si să **desemneze rolurile si responsabilităţile cheie**, precum și **liniile de raportare relevante**;

- stabilească **sistemele și procedurile necesare pentru identificarea, măsurarea, monitorizarea și gestionarea gamei de riscuri**;

- PSP trebuie să stabilească **3 *modalităţi de apărare eficiente*** sau un ***model intern de control si de gestionare a riscurilor echivalent***;

- ***auditate de auditori cu experienţă în securitatea IT si plăţi***;

- aprobat si revizuit, cel puţin o dată pe an, de către organul de conducere;

- trebuie integrat în întregime în procesele de gestionare a riscurilor generale ale PSP;

- ***nivelul de detaliu*** trebuie să fie proporţional cu dimensiunea PSP, precum si cu natura, scopul, complexitatea si caracterul riscant al serviciilor pe care PSP le furnizează.

MASURI DE SECURITATE

2. Evaluarea riscurilor

2.1 Identificarea funcțiilor, a proceselor și a activelor

- **identifice, să stabilească și să actualizeze regulat** inventarul **funcțiilor** aferente activității sale, al **rolurilor cheie** și al **proceselor de asistență** precum și interdependențele acestora privind riscurile operaționale și de securitate;
- PSP trebuie să identifice, să stabilească și să actualizeze regulat **inventarul activelor informaționale:** sistemele ITC, configurațiile acestora, alte infrastructuri, precum și interconexiunile cu alte sisteme externe și interne.

2.2 Clasificarea funcțiilor, a proceselor și a activelor

- PSP trebuie să clasifice **funcțiile** aferente activității, **procesele de asistență** și **activele informaționale** identificate, în funcție de **nivelul de risc asociat**.

2.3 Evaluarea riscurilor funcțiilor, a proceselor și a activelor

- PSP trebuie să se asigure că monitorizează permanent amenințările și vulnerabilitățile și că **revizuiesc regulat scenariile de risc**;
- PSP trebuie să efectueze și să documenteze **evaluările riscurilor**, cel puțin anual, 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 - art. 95 (2) din PSD2

MASURI DE SECURITATE

3. Protecţia – masuri de securitate preventive

3.1 Protecția

- PSP trebuie să elaboreze și să pună în aplicare măsurile de securitate preventive în conformitate cu riscurile identificate.

3.2 Integritatea și confidențialitatea datelor și a sistemelor

- PSP trebuie să se asigure că direcționarea, colectarea, prelucrarea, stocarea și/sau arhivarea și vizualizarea **datelor privind plățile sensibile** ale **USP** sunt adecvate;
- PSP trebuie să se asigure că s-au introdus mecanismele de verificare a integrității programului de software, a licențelor și a informațiilor privind serviciile de plată ale acestora.

3.3 Securitatea fizică și Controlul accesului

- PSP trebuie să introducă măsurile de **securitate fizică corespunzătoare** pentru protejarea datelor privind plățile sensibile ale USP, precum și a sistemelor ITC;
- **Accesul logic și fizic** la sistemele ITC trebuie să fie permis numai **persoanelor autorizate**;
- PSP - instituie **controale stricte privind accesul privilegiat la sisteme**;
- **Jurnalele de acces** trebuie păstrate o perioadă de timp proporțională cu starea critică a funcțiilor aferente activității.

MASURI DE SECURITATE

4. Monitorizarea continuă

4.1 Monitorizarea continuă si depistarea activităţilor anormale

- a) Factorii interni și externi relevanți, inclusiv funcțiile administrative privind ITC și cele aferente activității;
- b) Operațiunile pentru depistarea utilizării abuzive a accesului de către prestatorii de servicii sau de către alte entități;
- c) Amenințările interne și externe potențiale.

4.2 Monitorizarea și raportarea incidentelor operaționale sau de securitate

- PSP trebuie să stabilească **pragurile și criteriile** corespunzătoare pentru **clasificarea** unui eveniment drept **incident operațional sau de securitate**.
- PSP trebuie să instituie **procese corespunzătoare și structuri organizaționale** pentru a asigura **gestionarea incidentelor operaționale sau de securitate**.

MASURI DE SECURITATE

5. Continuitatea activității

5.1 Planificarea continuității activității pe bază de scenariu și dezvoltarea planurilor de răspuns și de redresare

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

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

  c) actualizate în conformitate cu lecțiile învățate.

5.2 Testarea planurilor de continuitate a activității

- PSP trebuie să testeze planurile de continuitate a activității cel puțin **anual**, sau **mai des** la **solicitarea autorității competente** – /// ;
- Trebuie să includă un set adecvat de scenarii;

5.3 Comunicarea în situații de criză

- PSP trebuie să se asigure că au introdus **măsuri de comunicare în situații de criză eficiente**.

6. Testarea măsurilor de securitate

6.1 Cadrul de testare adecvat

- Testele sunt efectuate ca parte a procesului formal de gestionare a modificărilor, mai ales în situația **modificărilor majore**;
- Testele sunt efectuate de **verificatori independenți**, care au **cunoștințe, competențe și expertiză** suficiente în testarea măsurilor de securitate a serviciilor de plată;
- Testele includ analize cu **scanere de vulnerabilitate** și **teste de penetrare** corespunzătoare nivelului de **risc identificat** în cadrul serviciilor de plată;
- Testele să fie **diverse** și **adecvate** (various scenarios).

7. Conștientizarea situației și învățarea continuă

7.1 Peisajul amenințărilor și conștientizarea situației

- PSP 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**;

- PSP trebuie să **analizeze** incidentele operaționale și de securitate să ia în considerare **lecțiile cheie învățate** din aceste analize și să **actualizeze** în consecință măsurile de securitate

7.2 Programe de formare și de conștientizare în materie de securitate

- PSP trebuie să stabilească un **program de formare pentru tot personalul**, pentru a se asigura că acesta este **instruit** pentru a-și îndeplini sarcinile și responsabilitățile;
- PSP trebuie să stabilească periodic **programe de conștientizare** în domeniul securității, care să impună personalului **raportarea oricărui incident**;

8. Gestionarea serviciilor de plată în relaţia cu utilizatorul

8.1 Gradul de conștientizare al USP privind riscurile de securitate și acțiunile de diminuare a riscurilor

- PSP trebuie să stabilească și să aplice **procese de sporire a gradului de conștientizare** al USP cu privire la **riscurile de securitate** asociate cu serviciile de plată, acordând **asistență** USP;
- PSP trebuie să acorde USP opțiunea de a primi **alerte** referitoare la **încercările inițiate și/sau eșuate** de începere a operațiunilor de plată;
- PSP informează USP despre actualizările procedurilor de securitate;
- PSP trebuie să acorde asistență USP în orice aspecte, cereri de sprijin și notificări de anomalii sau chestiuni **referitoare la probleme de securitate** legate de serviciile de plată;
- USP trebuie să fie informați în mod corespunzător despre modul de obținere a asistenței.

Vă mulțumesc pentru atenție!

Q&A

RUXANDRA AVRAM , Director
Direcția monitorizare a infrastructurilor pieței financiare și a plăților

BANCA NAȚIONALĂ A ROMÂNIEI

Str. Lipscani, nr. 25, România
E: ruxandra.avram@bnro.ro