NIS2 și securitatea cibernetică în sectorul FINANCIAR

NIS2 și securitatea cibernetică în sectorul financiar

Ghid orientativ pentru bănci, instituții financiare, fintech-uri și furnizori de servicii financiare

1. Ce primești din acest document

Acest ghid este conceput pentru organizațiile din sectorul financiar și are rolul de a oferi:

- o **imagine clară a nivelului de risc specific sectorului financiar**;
- o **orientare generală privind aplicabilitatea cerințelor NIS2**;
- o înțelegere a **obligațiilor care pot apărea direct sau indirect**;
- o prezentare a **aspectelor care lipsesc frecvent în acest domeniu**;
- **recomandări clare și practice**, explicate pe înțelesul managementului și al factorilor de decizie.

Documentul are caracter informativ și nu reprezintă o evaluare individuală a unei organizații.

2. De ce sectorul financiar este relevant pentru NIS2

Sectorul financiar este unul dintre cele mai reglementate și sensibile domenii, având un rol esențial în stabilitatea economică și funcționarea piețelor. Incidentele de securitate cibernetică pot afecta sistemele de plăți, accesul la fonduri și încrederea publicului.

Instituțiile financiare operează infrastructuri digitale complexe, procesează volume mari de date sensibile și depind de continuitatea serviciilor IT pentru desfășurarea activității zilnice.

3. Unde se poziționează, în general, sectorul financiar față de NIS2

Directiva NIS2 include sectorul financiar printre domeniile vizate, însă acesta este caracterizat de o suprapunere cu alte cadre de reglementare specifice.

În funcție de tipul instituției și de activitățile desfășurate:

- unele organizații financiare pot fi **entități NIS2**;
- alte organizații pot fi reglementate prioritar prin alte acte normative, dar pot avea **obligații indirecte** relevante din perspectiva NIS2.

Încadrarea exactă depinde de rolul fiecărei organizații în ecosistemul financiar.

4. NIS2 – aplicabilitate directă în sectorul financiar

În mod uzual, pot intra sub incidența directă a NIS2:

- instituții financiare cu rol sistemic;
- entități care furnizează servicii financiare esențiale;
- infrastructuri critice de piață.

Pentru aceste organizații, NIS2 introduce obligații privind:

- managementul riscurilor de securitate cibernetică;
- protejarea sistemelor informatice critice;
- asigurarea continuității serviciilor;
- raportarea incidentelor de securitate.

Nu toate fintech-urile sau instituțiile financiare mici sunt automat entități NIS2.

5. Relația dintre NIS2 și DORA

Sectorul financiar este supus și Regulamentului (UE) 2022/2554 privind reziliența operațională digitală (DORA).

În practică:

- DORA stabilește cerințe detaliate privind reziliența operațională digitală;
- NIS2 completează cadrul general de securitate cibernetică;
- organizațiile trebuie să asigure coerența între cele două regimuri.

Pentru multe instituții financiare, DORA reprezintă cadrul principal, iar NIS2 are un rol complementar.

6. NIS2 – aplicabilitate indirectă și lanțul de aprovizionare

Sectorul financiar depinde de un ecosistem extins de furnizori IT, fintech-uri, procesatori de plăți și furnizori de servicii digitale.

Obligații indirecte pot apărea atunci când organizațiile:

- furnizează servicii către entități financiare reglementate;
- operează platforme sau aplicații utilizate de instituții NIS2;
- au acces la date financiare sau sisteme critice.

Cerințele de securitate sunt adesea impuse contractual și monitorizate prin audituri.

7. Alte obligații digitale relevante pentru sectorul financiar

Pe lângă NIS2 și DORA, organizațiile din sectorul financiar pot fi supuse și altor cerințe, precum:

- reglementări privind protecția datelor;
- cerințe de securitate impuse de autorități de supraveghere;
- obligații privind continuitatea operațională și raportarea incidentelor.

Neconformarea poate conduce la sancțiuni financiare, restricții operaționale sau măsuri de supraveghere.

8. Riscurile tipice în sectorul financiar

Riscurile frecvent întâlnite în acest sector includ:

- atacuri cibernetice asupra sistemelor de plăți;
- fraude digitale și compromiterea conturilor;
- breșe de date financiare sensibile;
- întreruperea serviciilor digitale pentru clienți.

Impactul poate fi imediat și semnificativ din punct de vedere financiar și reputațional.

9. Ce lipsește frecvent în sectorul financiar

Chiar și în organizații mature, sunt frecvent identificate:

- abordări fragmentate ale securității și rezilienței;
- dependență ridicată de furnizori terți;

- documentație insuficient aliniată între cerințe multiple;
- lipsa testării integrate a scenariilor de incident.

10. Ce se așteaptă, în mod realist, de la organizațiile din acest sector

Așteptările sunt ridicate, dar proporționale cu rolul fiecărei organizații.

În mod realist, se așteaptă:

- un nivel avansat de gestionare a riscurilor digitale;
- măsuri solide de securitate;
- capacitatea de a răspunde rapid la incidente;
- transparență și cooperare cu autoritățile de supraveghere.

11. Ce NU este obligatoriu

Pentru a evita confuziile:

- nu este impus un anumit furnizor sau tehnologie;
- nu este obligatorie o certificare unică pentru conformare;
- NIS2 nu înlocuiește reglementările financiare existente.

12. Concluzie și pași următori

Acest ghid oferă o imagine generală asupra cerințelor și riscurilor din sectorul financiar. Pentru stabilirea obligațiilor exacte și a măsurilor necesare într-un caz concret, este recomandată o analiză dedicată, adaptată tipului de instituție și cadrului de reglementare aplicabil.