NIS2 și securitatea cibernetică în SECTORUL TRANSPORTURILOR

NIS2 și securitatea cibernetică în sectorul transporturilor

Ghid orientativ pentru operatori de transport feroviar, aerian, rutier și maritim

1. Ce primești din acest document

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

- o **imagine clară a nivelului de risc specific sectorului transporturilor**;
- 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 antreprenorilor și managerilor.

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

2. De ce sectorul transporturilor este relevant pentru NIS2

Sectorul transporturilor este esențial pentru funcționarea economiei și pentru mobilitatea persoanelor și a bunurilor. Perturbarea serviciilor de transport poate avea efecte în lanț asupra comerțului, aprovizionării, siguranței publice și altor sectoare critice.

Organizațiile din acest domeniu utilizează sisteme informatice complexe pentru operarea, coordonarea și monitorizarea activităților, inclusiv sisteme de management al traficului, sisteme de control, platforme de rezervare și infrastructuri digitale interconectate.

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

Directiva NIS2 include sectorul transporturilor printre domeniile de interes major, având în vedere impactul său asupra siguranței și continuității serviciilor.

În funcție de dimensiune, rol și tipul de activitate:

- unele organizații din sectorul transporturilor pot fi **entități NIS2** (esențiale sau importante);
- alte organizații pot **să nu intre direct sub incidența NIS2**, dar să fie afectate indirect prin lanțul de aprovizionare sau relațiile contractuale.

Încadrarea exactă depinde de tipul de transport și de rolul organizației în ecosistem.

4. NIS2 – aplicabilitate directă în sectorul transporturilor

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

- operatori de transport feroviar, aerian, rutier sau maritim de dimensiuni medii și mari;
- administratori de infrastructuri de transport critice;
- organizații care furnizează servicii esențiale de mobilitate.

Pentru aceste entități, NIS2 introduce obligații privind:

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

Nu toate companiile de transport sunt automat încadrate ca entități NIS2.

5. NIS2 – aplicabilitate indirectă și lanțul de aprovizionare

Sectorul transporturilor depinde de o rețea extinsă de furnizori și parteneri, inclusiv firme de IT, mentenanță, logistică și servicii suport.

Organizațiile care nu sunt entități NIS2 pot avea obligații indirecte atunci când:

- furnizează servicii sau sisteme utilizate de operatori critici;
- au acces la date operaționale sensibile;
- sunt integrate în procesele operaționale ale unor entități NIS2.

Cerințele de securitate sunt adesea stabilite prin contracte și politici interne ale partenerilor mari.

6. Alte obligații digitale relevante pentru sectorul transporturilor

Pe lângă NIS2, organizațiile din transporturi pot fi supuse și altor cerințe, precum:

- reglementări sectoriale specifice siguranței transporturilor;
- cerințe privind securitatea sistemelor digitale utilizate;
- obligații privind protecția datelor și continuitatea operațională.

Neconformarea poate conduce la sancțiuni, restricții de operare sau pierderea licențelor.

7. Riscurile tipice în sectorul transporturilor

Riscurile frecvent întâlnite în acest sector includ:

- atacuri cibernetice asupra sistemelor de control sau management al traficului;
- indisponibilitatea sistemelor de rezervare sau coordonare;
- compromiterea datelor operaționale sau ale clienților;
- perturbarea serviciilor de transport și logistică.

Impactul poate fi atât operațional, cât și economic și reputațional.

8. Ce lipsește frecvent în sectorul transporturilor

În practică, sunt frecvent întâlnite:

- evaluări insuficiente ale riscurilor cibernetice;
- proceduri incomplete de răspuns la incidente;

- responsabilități neclare privind securitatea IT;
- lipsa testării planurilor de continuitate.

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

Așteptările sunt proporționale cu dimensiunea și rolul organizației în lanțul de transport.

În mod realist, se așteaptă:

- măsuri de securitate adaptate specificului operațional;
- gestionarea riscurilor digitale;
- capacitatea de a preveni și gestiona incidente;
- cooperarea cu autoritățile competente.

10. Recomandări generale pentru sectorul transporturilor

Pentru majoritatea organizațiilor din domeniu, sunt recomandate:

- evaluarea periodică a riscurilor cibernetice;
- protejarea sistemelor critice;
- clarificarea responsabilităților interne;
- pregătirea pentru incidente de securitate și întreruperi operaționale.

11. Ce NU este obligatoriu

Pentru a evita confuziile frecvente:

- nu este obligatorie certificarea ISO;
- nu este impus un anumit furnizor sau soluție tehnică;
- nu este necesară externalizarea completă a securității IT.

12. Concluzie și pași următori

Acest ghid oferă o imagine generală asupra cerințelor și riscurilor din sectorul transporturilor. Pentru stabilirea obligațiilor exacte și a măsurilor necesare într-un caz concret, este recomandată o analiză dedicată, adaptată specificului organizației.