NIS2 și securitatea cibernetică în SECTORUL SPAȚIAL

NIS2 și securitatea cibernetică în sectorul spațial

Ghid orientativ pentru operatori spațiali, furnizori de servicii satelitare și organizații din ecosistemul spațial

1. Ce primești din acest document

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

- o **imagine clară a nivelului de risc specific sectorului spațial**;
- 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**, formulate 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 spațial este relevant pentru NIS2

Sectorul spațial are un rol strategic în funcționarea economiei moderne și a securității naționale, furnizând servicii esențiale precum comunicații satelitare, navigație, observație a Pământului și sincronizare de timp. Multe dintre aceste servicii sunt utilizate de alte sectoare critice, inclusiv energie, transporturi, apă, administrație publică și apărare.

Sistemele spațiale sunt extrem de complexe, distribuite și dificil de recuperat în cazul unui incident, ceea ce face ca securitatea cibernetică și reziliența operațională să fie esențiale.

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

Directiva NIS2 include sectorul spațial printre domeniile de interes, având în vedere impactul său transversal asupra altor servicii critice.

În funcție de rol și tipul de activitate:

- unele organizații din sectorul spațial pot fi **entități NIS2**;
- alte organizații pot **să nu intre direct sub incidența NIS2**, dar să aibă obligații indirecte relevante.

Încadrarea exactă depinde de natura serviciilor furnizate și de impactul acestora.

4. NIS2 – aplicabilitate directă în sectorul spațial

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

- operatori de infrastructuri spațiale critice;
- furnizori de servicii satelitare esențiale;
- organizații care operează sau controlează sisteme spațiale cu impact major.

Pentru aceste entități, NIS2 introduce obligații privind:

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

Nu toate organizațiile din ecosistemul spațial sunt automat entități NIS2.

5. NIS2 – aplicabilitate indirectă și lanțul de aprovizionare

Sectorul spațial se bazează pe un ecosistem complex de furnizori, inclusiv producători de echipamente, software, servicii IT și centre de control.

Obligații indirecte pot apărea atunci când organizațiile:

- furnizează tehnologii sau servicii către entități spațiale NIS2;
- operează sisteme integrate în infrastructuri spațiale critice;
- au acces la date sensibile sau sisteme de control.

Cerințele de securitate sunt adesea impuse prin contracte și acorduri de cooperare.

6. Alte obligații digitale relevante pentru sectorul spațial

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

- reglementări privind securitatea națională și infrastructurile critice;
- obligații privind protecția datelor și informațiilor sensibile;
- cerințe contractuale impuse de agenții sau parteneri internaționali.

Neconformarea poate conduce la sancțiuni, restricții operaționale sau excluderea din programe și parteneriate.

7. Riscurile tipice în sectorul spațial

Riscurile frecvent întâlnite în acest sector includ:

- atacuri cibernetice asupra segmentelor de control și comunicații;
- compromiterea semnalelor satelitare;
- pierderea controlului asupra sistemelor spațiale;
- efecte în lanț asupra serviciilor critice dependente.

Impactul acestor riscuri este ridicat și dificil de remediat.

8. Ce lipsește frecvent în sectorul spațial

În practică, sunt frecvent identificate:

- abordări insuficient integrate de securitate cibernetică;
- separare neclară a responsabilităților între IT, operațional și securitate;
- proceduri limitate de răspuns la incidente complexe;
- dependență ridicată de furnizori specializați fără evaluări adecvate.

9. 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 securitate cibernetică;
- gestionarea riguroasă a riscurilor;
- capacitatea de a preveni și gestiona incidente;
- cooperarea strânsă cu autoritățile și partenerii relevanți.

10. Recomandări generale pentru sectorul spațial

Pentru majoritatea organizațiilor din domeniu, sunt recomandate:

- evaluarea periodică a riscurilor de securitate;
- protejarea sistemelor critice și a segmentelor de control;
- clarificarea responsabilităților interne;
- pregătirea pentru incidente de securitate cu impact major.

11. Ce NU este obligatoriu

Pentru a evita confuziile:

- nu este obligatorie certificarea ISO ca cerință unică;
- nu este impus un anumit furnizor sau tehnologie;
- NIS2 nu se aplică automat tuturor organizațiilor din domeniu.

12. Concluzie și pași următori

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