NIS2 și securitatea cibernetică în SECTORUL INDUSTRIAL

NIS2 și securitatea cibernetică în sectorul Industrial

Ghid orientativ pentru producție industrială, industrie chimică și industria alimentară

1. Ce primești din acest document

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

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

Sectorul industrial joacă un rol esențial în economia națională și europeană, asigurând producția de bunuri critice, materiale de bază și produse necesare funcționării altor sectoare. În special în industria chimică și alimentară, incidentele pot avea impact direct asupra siguranței populației.

Organizațiile industriale operează frecvent sisteme informatice și sisteme operaționale (OT), inclusiv linii de producție automatizate, echipamente industriale conectate și sisteme de control, ceea ce crește expunerea la riscuri cibernetice cu impact operațional și fizic.

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

Directiva NIS2 include anumite activități industriale printre domeniile de interes, în special atunci când acestea au un impact semnificativ asupra societății sau economiei.

În funcție de dimensiune, tipul de producție și rolul în lanțul de aprovizionare:

- unele organizații industriale pot fi **entități NIS2**;
- multe organizații industriale **nu intră direct sub incidența NIS2**, dar pot avea obligații indirecte relevante.

Încadrarea depinde de natura activităților și de importanța acestora.

4. NIS2 – aplicabilitate directă în sectorul industrial

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

- producători din industrii considerate critice;
- operatori de instalații industriale cu impact major;

- organizații din industria chimică sau alimentară cu rol esențial în aprovizionare.

Pentru aceste organizații, NIS2 introduce obligații privind:

- managementul riscurilor de securitate cibernetică;
- protejarea sistemelor IT și OT;
- continuitatea operațiunilor;
- raportarea incidentelor de securitate.

Nu toate fabricile sau unitățile de producție sunt automat entități NIS2.

5. NIS2 – aplicabilitate indirectă și lanțul de aprovizionare

Sectorul industrial este profund integrat în lanțuri de aprovizionare complexe.

Organizațiile pot avea obligații indirecte atunci când:

- furnizează produse sau servicii către entități NIS2;
- operează sisteme integrate cu infrastructuri critice;
- depind de furnizori sau tehnologii esențiale.

Cerințele de securitate sunt frecvent impuse prin contracte și standarde interne ale partenerilor.

6. Alte obligații digitale relevante pentru sectorul industrial

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

- reglementări sectoriale privind siguranța și mediul;
- cerințe privind securitatea infrastructurilor industriale;
- obligații privind protecția datelor și trasabilitatea.

Neconformarea poate conduce la sancțiuni, oprirea activității sau pierderi comerciale.

7. Riscurile tipice în sectorul industrial

Riscurile frecvent întâlnite în sectorul industrial includ:

- atacuri asupra sistemelor de control industrial (ICS/SCADA);
- oprirea sau perturbarea liniilor de producție;
- incidente cu impact asupra siguranței fizice;
- compromiterea datelor de producție sau rețetelor.

Impactul acestor riscuri poate fi major atât economic, cât și operațional.

8. Ce lipsește frecvent în sectorul industrial

În practică, sunt frecvent identificate:

- lipsa separării între rețelele IT și OT;
- măsuri de securitate insuficiente pentru echipamentele industriale;
- proceduri incomplete de răspuns la incidente;
- responsabilități neclare între IT și operațional.

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

Așteptările sunt proporționale cu dimensiunea și rolul organizației în lanțul industrial.

În mod realist, se așteaptă:

- măsuri de securitate adaptate mediului industrial;
- gestionarea riscurilor IT și OT;

- capacitatea de a preveni și gestiona incidente;
- cooperarea cu autoritățile și partenerii.

10. Recomandări generale pentru sectorul industrial

Pentru majoritatea organizațiilor din domeniu, sunt recomandate:

- evaluarea periodică a riscurilor cibernetice;
- protejarea sistemelor industriale critice;
- clarificarea responsabilităților între IT și operațional;
- pregătirea pentru incidente de securitate.

11. Ce NU este obligatoriu

Pentru a evita confuziile frecvente:

- nu este obligatorie certificarea ISO;
- nu este impus un anumit furnizor sau produs;
- 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 industrial. Pentru stabilirea obligațiilor exacte și a măsurilor necesare într-un caz concret, este recomandată o analiză dedicată, adaptată specificului organizației.