NIS2 și securitatea cibernetică în SECTORUL ENERGETIC

NIS2 și securitatea cibernetică în sectorul energetic

Ghid orientativ pentru producători, distribuitori și operatori de transport energie

1. Ce primești din acest document

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

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

Sectorul energetic este considerat infrastructură critică esențială pentru funcționarea societății și a economiei. Orice perturbare a producției, transportului sau distribuției energiei poate avea efecte în lanț asupra altor sectoare critice, inclusiv sănătate, transporturi, comunicații și servicii publice.

Organizațiile din acest domeniu operează sisteme informatice și operaționale complexe (IT și OT), inclusiv sisteme industriale de control, ceea ce le expune la riscuri cibernetice cu impact potențial major, inclusiv impact fizic.

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

Directiva NIS2 tratează sectorul energetic ca domeniu prioritar, cu un nivel ridicat de criticitate.

În funcție de dimensiune, rol și tipul de activitate desfășurată:

- multe organizații din sectorul energetic pot fi **entități NIS2** (în special entități esențiale);
- alte organizații pot **să nu intre direct sub incidența NIS2**, dar să fie afectate indirect prin relațiile comerciale sau operaționale.

Încadrarea exactă depinde de poziția fiecărei organizații în lanțul energetic.

4. NIS2 – aplicabilitate directă în sectorul energetic

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

- producători de energie electrică, termică sau gaze;

- operatori de transport și distribuție;
- entități care operează infrastructuri energetice critice.

Pentru aceste organizații, NIS2 introduce obligații privind:

- managementul riscurilor de securitate cibernetică;
- protecția sistemelor IT și OT;
- asigurarea continuității operaționale;
- raportarea incidentelor semnificative.

Nu toate companiile din sectorul energetic sunt automat încadrate ca entități NIS2.

5. NIS2 – aplicabilitate indirectă și lanțul de aprovizionare

Organizațiile din sectorul energetic colaborează cu un număr mare de furnizori și parteneri, inclusiv firme de mentenanță, IT, automatizări și servicii suport.

Chiar dacă nu sunt entități NIS2, aceste organizații pot avea obligații indirecte atunci când:

- furnizează servicii sau echipamente pentru infrastructuri energetice critice;
- au acces la sisteme sau date sensibile;
- sunt integrate operațional în procesele unor entități NIS2.

Cerințele de securitate sunt frecvent impuse prin contracte și proceduri interne.

6. Alte obligații digitale relevante pentru sectorul energetic

Pe lângă NIS2, organizațiile din sectorul energetic pot fi supuse și altor cerințe legale și de reglementare, inclusiv:

- reglementări sectoriale specifice energiei;
- cerințe privind securitatea infrastructurilor critice;
- obligații privind protecția datelor și continuitatea serviciilor digitale.

Neconformarea poate atrage sancțiuni, restricții operaționale sau pierderea licențelor.

7. Riscurile tipice în sectorul energetic

Riscurile frecvent întâlnite în acest sector includ:

- atacuri asupra sistemelor industriale de control (SCADA/ICS);
- întreruperi ale furnizării energiei;
- ransomware cu impact asupra operațiunilor;
- incidente cibernetice cu efecte fizice sau de siguranță.

Impactul acestor riscuri poate fi semnificativ atât din perspectivă economică, cât și socială.

8. Ce lipsește frecvent în sectorul energetic

În practică, se observă adesea:

- separare insuficientă între sistemele IT și OT;
- lipsa unor proceduri clare de gestionare a incidentelor;
- vizibilitate redusă asupra riscurilor cibernetice;

- responsabilități neclare privind securitatea cibernetică.

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

Așteptările sunt proporționale cu rolul și impactul fiecărei organizații în lanțul energetic.

În mod realist, se așteaptă:

- implementarea unor măsuri de securitate adecvate;
- gestionarea riscurilor IT și OT;
- capacitatea de a preveni și gestiona incidentele;
- cooperarea cu autoritățile competente.

10. Recomandări generale pentru sectorul energetic

Pentru majoritatea organizațiilor din domeniu, sunt recomandate:

- evaluarea periodică a riscurilor cibernetice;
- protejarea infrastructurilor critice;
- clarificarea responsabilităților interne;
- pregătirea pentru gestionarea incidentelor de securitate.

11. Ce NU este obligatoriu

Pentru a evita interpretările eronate:

- nu este obligatorie certificarea ISO;

- nu este impus un anumit furnizor sau produs;
- nu este necesară externalizarea completă a securității cibernetice.

12. Concluzie și pași următori

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