NIS2 și securitatea cibernetică în SECTORUL MEDICAL

NIS2 și securitatea cibernetică în sectorul medical

Ghid orientativ pentru spitale, clinici, furnizori de servicii medicale și entități conexe

1. Ce primești din acest document

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

- o **imagine clară a nivelului de risc specific sectorului medical**;
- 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 din sănătate.

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

2. De ce sectorul medical este relevant pentru NIS2

Sectorul medical este considerat unul dintre cele mai sensibile și critice domenii din perspectiva securității cibernetice. Funcționarea sa are impact direct asupra sănătății și vieții pacienților, iar indisponibilitatea serviciilor medicale poate genera consecințe grave.

Instituțiile medicale operează volume mari de date sensibile, sisteme informatice critice și echipamente conectate (aparatură medicală, sisteme de programare, sisteme clinice), ceea ce le face o țintă frecventă pentru atacuri cibernetice.

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

În cadrul Directivei NIS2, sectorul sănătății este explicit menționat ca domeniu de interes major.

În funcție de dimensiune, rol și tipul de servicii furnizate:

- unele organizații din sectorul medical pot fi **entități NIS2** (esențiale sau importante);
- alte organizații pot **să nu intre direct sub incidența NIS2**, dar să aibă obligații indirecte sau alte cerințe legale relevante.

Încadrarea exactă depinde de mai mulți factori, inclusiv de rolul în ecosistemul medical.

4. NIS2 – aplicabilitate directă în sectorul medical

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

- spitale publice și private de dimensiuni medii și mari;
- unități medicale cu rol critic în furnizarea serviciilor de sănătate;
- organizații care furnizează servicii medicale esențiale la scară largă.

Pentru aceste entități, NIS2 introduce obligații privind:

- managementul riscurilor de securitate cibernetică;
- implementarea unor măsuri tehnice și organizatorice adecvate;
- raportarea incidentelor de securitate.

Nu toate clinicile sau cabinetele medicale intră automat sub incidența directă a NIS2.

5. NIS2 – aplicabilitate indirectă și lanțul de aprovizionare

Chiar și organizațiile medicale care nu sunt entități NIS2 pot avea obligații indirecte, în special atunci când:

- furnizează servicii către spitale sau instituții medicale mari;
- operează sau administrează sisteme informatice utilizate de entități NIS2;
- au acces la date medicale sau infrastructuri critice.

În aceste situații, cerințele de securitate sunt adesea transferate prin contracte, politici interne sau audituri impuse de parteneri.

6. Alte obligații digitale relevante pentru sectorul medical

Pe lângă NIS2, organizațiile din domeniul sănătății sunt supuse și altor reglementări importante, precum:

- obligații privind protecția datelor cu caracter personal (date medicale);
- cerințe privind securitatea aplicațiilor și platformelor digitale utilizate;
- cerințe impuse de autorități naționale în domeniul digital și al sănătății.

Lipsa conformării poate conduce la sancțiuni, restricții operaționale sau pierderea încrederii pacienților.

7. Riscurile tipice în sectorul medical

Printre riscurile cel mai frecvent întâlnite în sectorul medical se numără:

- atacuri ransomware care blochează accesul la sisteme clinice;
- indisponibilitatea sistemelor de programare sau a dosarelor medicale;
- compromiterea datelor sensibile ale pacienților;
- afectarea continuității actului medical.

Aceste riscuri pot avea consecințe atât operaționale, cât și legale și reputaționale.

8. Ce lipsește frecvent în sectorul medical

În practică, multe organizații din sectorul medical se confruntă cu:

- lipsa unei abordări structurate de management al riscurilor cibernetice;
- responsabilități neclare privind securitatea IT;
- proceduri insuficiente de răspuns la incidente;
- măsuri tehnice minime neuniform implementate.

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

Cerințele nu sunt identice pentru toate organizațiile. Așteptările sunt proporționale cu dimensiunea și rolul fiecărei entități.

În mod realist, se așteaptă:

- existența unor politici și proceduri de bază;

- măsuri minime de securitate adaptate contextului medical;
- capacitatea de a detecta și gestiona incidentele.

10. Recomandări generale pentru sectorul medical

Pentru majoritatea organizațiilor din domeniu, sunt recomandate:

- evaluarea periodică a riscurilor cibernetice;
- clarificarea responsabilităților interne;
- protejarea sistemelor și datelor critice;
- pregătirea personalului 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 soluție tehnică;
- nu este necesară externalizarea completă a securității IT.

12. Concluzie și pași următori

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