NIS2 și securitatea cibernetică în ADMINISTRAȚIA PUBLICĂ

NIS2 și securitatea cibernetică în administrația publică

Ghid orientativ pentru autorități și instituții publice centrale și locale

1. Ce primești din acest document

Acest ghid este conceput pentru organizațiile din administrația publică și are rolul de a oferi:

- o **imagine clară a nivelului de risc specific administrației publice**;
- 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 conducerii și personalului non-tehnic.

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

2. De ce administrația publică este relevantă pentru NIS2

Administrația publică joacă un rol esențial în funcționarea statului și în furnizarea serviciilor publice către cetățeni și mediul de afaceri. Indisponibilitatea sau compromiterea sistemelor informatice publice poate afecta direct drepturile cetățenilor, continuitatea serviciilor și încrederea în instituții.

Instituțiile publice gestionează volume mari de date, inclusiv date cu caracter personal, registre naționale și sisteme informatice critice, adesea interconectate cu alte platforme guvernamentale.

3. Unde se poziționează, în general, administrația publică față de NIS2

Directiva NIS2 include administrația publică printre domeniile vizate, în special la nivel central și pentru anumite structuri locale cu rol critic.

În funcție de nivelul administrativ și de tipul serviciilor furnizate:

- unele instituții publice pot fi **entități NIS2**;
- alte instituții pot **să nu intre direct sub incidența NIS2**, dar să fie supuse unor obligații indirecte sau altor reglementări digitale.

Încadrarea exactă depinde de rolul instituției și de impactul serviciilor oferite.

4. NIS2 – aplicabilitate directă în administrația publică

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

- instituții publice centrale;
- autorități cu rol critic în furnizarea serviciilor publice;
- structuri administrative care operează sisteme informatice esențiale.

Pentru aceste entități, NIS2 introduce obligații privind:

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

Nu toate instituțiile publice locale sunt automat încadrate ca entități NIS2.

5. NIS2 – aplicabilitate indirectă și lanțul de aprovizionare

Administrația publică depinde de numeroși furnizori externi de IT, software, mentenanță și servicii digitale.

Obligații indirecte pot apărea pentru instituțiile care:

- utilizează servicii furnizate de entități NIS2;
- externalizează operarea unor sisteme informatice critice;
- gestionează proiecte digitale complexe cu furnizori terți.

Cerințele de securitate sunt adesea incluse în contracte și proceduri de achiziție publică.

6. Alte obligații digitale relevante pentru administrația publică

Pe lângă NIS2, administrația publică este supusă și altor cadre de reglementare, precum:

- cerințe privind digitalizarea și interoperabilitatea sistemelor;
- obligații privind protecția datelor cu caracter personal;
- cerințe impuse de autorități naționale în domeniul digital.

Neconformarea poate conduce la sancțiuni, blocaje operaționale sau afectarea serviciilor publice.

7. Riscurile tipice în administrația publică

Riscurile frecvent întâlnite în acest domeniu includ:

- atacuri ransomware asupra sistemelor publice;
- indisponibilitatea platformelor digitale pentru cetățeni;
- compromiterea registrelor și bazelor de date;
- afectarea continuității serviciilor publice.

Aceste riscuri pot avea impact major asupra funcționării instituțiilor și asupra încrederii publice.

8. Ce lipsește frecvent în administrația publică

În practică, sunt frecvent identificate:

- lipsa unei strategii coerente de securitate cibernetică;
- resurse limitate dedicate securității IT;
- proceduri insuficient testate pentru gestionarea incidentelor;
- responsabilități neclare între departamente.

9. Ce se așteaptă, în mod realist, de la instituțiile publice

Așteptările sunt proporționale cu rolul și nivelul fiecărei instituții.

În mod realist, se așteaptă:

- implementarea unor măsuri minime de securitate;
- gestionarea riscurilor digitale;
- capacitatea de a reacționa la incidente;
- cooperarea cu autoritățile competente în domeniul securității cibernetice.

10. Recomandări generale pentru administrația publică

Pentru majoritatea instituțiilor, sunt recomandate:

- evaluarea periodică a riscurilor de securitate;
- protejarea sistemelor și datelor critice;
- clarificarea responsabilităților interne;
- instruirea personalului privind securitatea cibernetică.

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 administrația publică. Pentru stabilirea obligațiilor exacte și a măsurilor necesare într-un caz concret, este recomandată o analiză dedicată, adaptată specificului instituției.