Securitate cibernetica: România transpune Directiva NIS2. Ce urmeaza?

Directiva (UE) 2022/2555 (NIS2) are scopul de a întari reziliența cibernetica a Uniunii Europene, solicitând entităților din diverse sectoare sa își consolideze masurile de securitate cibernetica. NIS2 înlocuiește fosta Directiva NIS1 (UE) 2016/1148, extinde gama de entitați reglementate și introduce cerințe mai stricte pentru acestea.

Pe 31 decembrie 2024, Guvernul României a adoptat Ordonanța de Urgența nr. 155/2024 (OUG 155/2024) pentru transpunerea NIS2 în legislația națională.

Cine este vizat?

NIS2 și OUG 155/2024 se aplica entităților din diverse sectoare economice, împarțindu-le în entitați esențiale și entitați importante. Entitățile din urmatoarele domenii trebuie sa verifice daca aceste reglementari li se aplica:

- Entitați esențiale: energie (electricitate, încalzire centralizata, petrol, gaze, hidrogen); transport (aerian, feroviar, naval, rutier); bancar; infrastructuri ale pieței financiare; sanatate; apa potabila; apa uzata; administrație publica și spațiu. Infrastructura digitala și serviciile de gestionare a TIC au obligații și mai stricte.

- Entitați importante: servicii poștale și de curierat; gestionarea deșeurilor; fabricarea, producția și distribuția de produse chimice; producția, procesarea și distribuția alimentelor; fabricarea de dispozitive medicale; produse informatice, electronice și optice; echipamente electrice; mașini și echipamente; autovehicule, remorci și semiremorci, alte echipamente de transport; furnizori digitali de piețe online, motoare de cautare și rețele sociale.

Chiar daca exista praguri de dimensiune (NIS2 și OUG 155/2024 se aplica în principal întreprinderilor mijlocii și mari), o entitate mai mica poate fi totuși supusa acestor reguli daca are un rol critic într-un sector specific. De asemenea, unele obligații se extind și la furnizorii acestor entitați, întrucât NIS2 vizeaza și creșterea nivelului de securitate cibernetica în lanțurile de aprovizionare.

Ce trebuie facut?

Daca o entitate constata ca intra sub incidența NIS2 și OUG 155/2024, aceasta trebuie sa respecte toate obligațiile prevazute pentru categoria sa. Printre masurile impuse de OUG 155/2024 se numara:

- Implementarea unor masuri tehnice, operaţionale şi organizatorice adecvate şi proporţionale pentru gestionarea riscurilor de securitate şi reducerea impactului incidentelor asupra sistemelor informatice, respectând cerinţele specifice fiecarui sector.
- Înregistrarea la Directoratul Naţional de Securitate Cibernetica (DNSC), autoritatea responsabila cu aplicarea prevederilor OUG 155/2024.
- Efectuarea de audituri periodice şi comunicarea rezultatelor acestora catre DNSC.
- Instruirea conducerii în domeniul securităţii cibernetice şi asigurarea faptului ca persoana responsabila cu deciziile privind securitatea cibernetica este independenta de şeful operaţional IT.
- Raportarea incidentelor cibernetice autorităţilor în termen de 6-24 ore, iar, în funcţie de caz, informarea persoanelor afectate sau a partenerilor contractuali.

Sancţiuni

OUG 155/2024 stabileşte un regim sever de sancţiuni pentru fiecare încalcare a obligaţiilor impuse:

→ Firmele esenţiale: amenzi de pâna la 10 milioane EUR sau 2% din cifra de afaceri globala anuala (se aplica valoarea mai mare).
→ Firmele importante: amenzi de pâna la 7 milioane EUR sau 1,4% din cifra de afaceri globala anuala (se aplica valoarea mai mare).
În plus, NIS2 şi OUG 155/2024 introduc raspunderea personala a membrilor conducerii pentru nerespectarea obligaţiilor.

Ce urmeaza?

OUG 155/2024 a stabilit un termen-limita pentru înregistrarea la DNSC care a expirat pe 30 ianuarie 2025. Totuşi, în prezent, DNSC nu a emis înca normele de aplicare necesare pentru efectuarea înregistrarii.

Conform unui comunicat de presa de pe site-ul DNSC, înregistrarile se vor efectua pe baza normelor de aplicare pe care DNSC s-a angajat sa le publice în primul trimestru al anului 2025. Dupa publicarea acestora, entitaţile vizate vor trebui sa se înregistreze conform cerinţelor şi termenelor stabilite.

Neîndeplinirea obligaţiilor de securitate cibernetica poate atrage nu doar amenzi pentru companie şi conducere, ci şi cereri de despagubire din partea partenerilor contractuali, daca aceştia sufera pierderi din cauza unui incident ce putea fi prevenit prin masuri corespunzatoare.

Entitaţile vizate ar trebui sa ia masuri cât mai curând posibil pentru a respecta aceste cerinţe legale.