Directiva NIS2 în România: Companiile,obligate sa implementeze masuri de securitate cibernetica; amenzile pot ajunge la 10 milioane de euro

România a pus în aplicare una dintre cele mai ferme reglementari pentru companii publice si private - Directiva europeana NIS2 pentru securitate cibernetica, iar amenzile pot ajunge la zece milioane de euro sau 2% din cifra de afaceri, noteaza Centrul de Formare APSAP, într-un comunicat de presa .

"România a început aplicarea uneia dintre cele mai dure legi pentru companii, institutii si organizatii, Directiva europeana NIS2 pentru securitate cibernetica. Amenzile pentru neconformarea companiilor pot ajunge pâna la 10 milioane de euro sau 2% din cifra de afaceri, iar responsabilitatea principala cade acum pe conducerea firmelor, nu pe departamentul de IT, cu sanctiuni extrem de severe. Firmele sunt obligate si sa desemneze un responsabil NIS, care sa fi absolvit un curs de specialitate. Desi sanctiunile au intrat în vigoare la final de 2025, companiile vizate înca nu s-au conformat normelor Directivei europene NIS2. În România, între 15.000 si 20.000 de entitati intra sub incidenta NIS2, cu o crestere semnificativa fata de aproximativ 1.000 de entitati reglementate anterior prin NIS1. Acestea sunt obligate sa implementeze masuri tehnice, operationale si organizatorice de securitate cibernetica, sa raporteze incidentele semnificative si sa se supuna auditurilor de securitate", avertizeaza entitatea, unul dintre putinii furnizori din România autorizati de stat pentru conformare si auditare pe securitate cibernetica.

Directiva NIS2 a fost transpusa în România prin OUG nr. 155/2024, un act normativ cu impact direct si imediat asupra companiilor si institutiilor din sectoarele critice si importante ale economiei. Acest domeniu este gestionat de Directoratul National de Securitate Cibernetica (DNSC), institutia guvernamentala care controleaza si sanctioneaza companiile care nu respecta legea.

NIS2 (Network and Information Security Directive) stabileste un cadru comun la nivelul Uniunii Europene pentru cresterea nivelului de securitate a retelelor si sistemelor informatice, se aplica entitatilor esentiale si importante din domenii, precum: energie, transport, sanatate, apa, infrastructura digitala, administratie publica, servicii IT&C, productie industriala, servicii financiare, dar si altor sectoare prevazute expres în anexele actului normativ.

Potrivit APSAP, spre deosebire NIS, vechea reglementare, NIS2 extinde aria de aplicare, introduce obligatii clare pentru management si vine cu un regim de sanctiuni extrem de sever. Nivelul sanctiunilor este diferentiat în functie de tipul entitatii si de gravitatea încalcarilor, însa pragurile sunt fara precedent în legislatia românească în domeniu.

Astfel, entitatile esentiale sunt operatori din sectoare de importanta critica (energie, transporturi, infrastructura digitala, sanatate, apa potabila, ape uzate, infrastructura spatiala, sector bancar si infrastructura pietelor financiare), ce presteaza servicii vitale pentru mentinerea activitatilor societale si economice esentiale. Amenzile pentru aceasta categorie variaza între 10.000 de lei si 10 milioane de euro (echivalent în lei) sau pâna la 2% din cifra de afaceri anuala la nivel mondial, fiind luata în calcul valoarea cea mai mare.

La categoria entitatilor importante se încadreaza operatori din sectoare ca: servicii postale, gestionarea deseurilor, industria chimica, productia si distributia alimentelor, industria prelucratoare, furnizori de servicii digitale (cloud, datacenter, retele de livrare de continut), cercetare si alte sectoare definite în anexele OUG 155/2024. În cazul acestora, amenzile pot fi între 5.000 de lei si sapte milioane de euro sau pâna la 1,4% din cifra de afaceri anuala la nivel mondial, valoarea cea mai mare fiind aplicabila.

Sanctiunile pot fi aplicate pentru o serie de nereguli, cum ar fi: lipsa masurilor tehnice, operationale si organizatorice de securitate; neefectuarea auditului de securitate cibernetica; neîndeplinirea obligatiilor de

raportare si notificare a incidentelor; lipsa autoevaluarii nivelului de maturitate; neimplementarea planurilor de remediere; nealocarea resurselor necesare securitatii cibernetice; nerespectarea obligatiei ca membrii conducerii sa urmeze cursuri de formare în domeniul securitatii cibernetice; obstructionarea controalelor sau furnizarea de informatii false.

Conform specialistilor, pentru anumite abateri "administrative", amenzile pot varia între 1.000 de lei si 600.000 de lei, iar pentru încalcari grave sau repetate, sanctiunile pot ajunge pâna la 600.000 de lei, independent de alte masuri dispuse de autoritati.

Un element-cheie al NIS2 este responsabilizarea directa a conducerii, astfel ca membrii organelor de conducere pot fi sanctionati daca nu supravegheaza implementarea masurilor de securitate, nu aloca resursele necesare, nu desemneaza responsabili cu securitatea IT sau nu urmeaza programe de formare profesionala în domeniul securitatii cibernetice.

Centrul de Formare APSAP se numara printre putinii furnizori din România autorizati de DNSC pentru programele-cheie impuse de OUG nr. 155/2024, respectiv: Auditor de securitate cibernetica si Responsabil NIS.