DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Comunicat de presă

Parlamentul European a adoptat noi norme legislative pentru consolidarea rezilienței cibernetice a întregii Uniuni Europene – NIS2 și DORA

București, 11 noiembrie 2022

La data de 10 noiembrie 2022, Parlamentul European a adoptat noi norme cu rol în consolidarea rezilienței cibernetice la nivelul Uniunii Europene (UE).

Pentru a răspunde amenințărilor tot mai mari reprezentate de digitalizare și de intensificarea atacurilor cibernetice, **Comisia Europeană** a prezentat o propunere de înlocuire a **Directivei pentru Securitatea Informației și Rețelelor** (Network and Information Security Directive - NIS) și, prin urmare, de consolidare a cerințelor de securitate, de abordare a securității lanțurilor de aprovizionare, de raționalizare a obligațiilor de raportare și de introducere a unor măsuri de supraveghere, dar și a unor cerințe de aplicare mai stricte, inclusiv sancțiuni armonizate în întreaga UE.

Astfel, Parlamentul a adoptat **Directiva „NIS2”**, prin care sunt impuse statelor membre UE reguli mai riguroase în materie de securitate cibernetică pentru gestionarea riscurilor, raportarea și schimbul de informații. Cerințele se referă, printre altele, la răspunsul la incidente, securitatea lanțului de aprovizionare, criptare și divulgarea vulnerabilităților.

Mai multe entități și sectoare vor trebui să ia măsuri pentru a se proteja. Sectoarele esențiale, precum sectorul energiei, transporturile, sectorul bancar, sănătatea, infrastructura digitală, administrația publică și sectorul spațial, vor fi acoperite de noile dispoziții în materie de securitate.

De asemenea, noile norme impuse de Directiva NIS2 vor proteja sectoarele importante, precum serviciile poștale, gestionarea deșeurilor, substanțele chimice, produsele alimentare, fabricarea de dispozitive medicale, electronice, utilaje, autovehicule și furnizorii digitali. Toate companiile mijlocii și mari din anumite sectoare ar intra sub incidența legislației.

Astfel, Directiva NIS2 se aplică tuturor entităților economice care ating sau depășesc plafoanele pentru întreprinderile mijlocii. DNSC, organ de specialitate al administrației publice centrale cu responsabilități privind securitatea cibernetică a spațiului cibernetic național civil, componentă a securității naționale, în calitate de autoritate competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, a demarat deja procesul de stabilire a priorităților legislative și va conduce acțiunile de implementare a Directivei NIS2 la nivel național.

DNSC va lua în considerare deopotrivă includerea microîntreprinderilor și a întreprinderilor mici care îndeplinesc criterii specifice ce indică un rol esențial pe lista operatorilor de servicii esențiale/importante. Entităților esențiale/importante li se poate deja cere să certifice anumite produse, servicii și procese IT&C bazate pe sistemele europene de certificare a securității cibernetice adoptate în conformitate cu articolul 49 din Regulamentul (UE) 2019/881.

Directiva NIS2 propune o nouă abordare a actorilor, entități esențiale și entități importante, respectiv a sectoarelor economice, respectiv 11 sectoare esențiale și 7 sectoare importante.

Entități esențiale

- *11* sectoare: Energie, Transport, Bancar, Piața financiară, Sănătate, Apă potabilă, Ape uzate, Infrastructură digitală, Administrație publică, Managementul serviciilor ITC (B2B) și Spațiu.
- *9 subsectoare*: Electricitate, Încălzire și răcire centralizată, Petrol, Gaze, Hidrogen, Transport aerian, Transport feroviar, Transport pe apă și Transport Rutier.

Entități importante

- *7 sectoare*: Poștă și curierat, Gestionare deșeuri, Fabricarea, producția și distribuția de substanțe chimice, Alimente, Fabricare, Furnizori digitali și Cercetare.

- *6 subsectoare*: Dispozitive medicale, Computere, produse electronice și optice, Echipamente electrice, Mașini și echipamente n.a.p (neclasificate în altă parte), Autovehicule, remorci și semiremorci, Echipamente de transport.

Totodată, Directiva NIS2 abordează într-o nouă manieră instruirea permanentă a personalului în domeniul securității cibernetice, utilizarea criptării, utilizarea soluțiilor de autentificare cu mai mulți factori și introducerea de comunicații securizate de voce, video și text.

În plus față de Directiva NIS2, Parlamentul European a adoptat **Regulamentul european (cu putere de lege) pentru Reziliență Operațională Digitală** (Digital Operational Resilience Act - DORA), prin care vor fi armonizate și consolidate cerințele de reziliență operațională digitală pentru sectorul serviciilor financiare al UE. Proiectul de lege stabilește cerințe pentru protecția împotriva atacurilor, detecție, limitare, recuperare și recuperare în urma incidentelor legate de tehnologia informației și a comunicațiilor (TIC). Aceste cerințe vor fi asociate cu capacități de raportare și de testare digitală.

Noile norme DORA se vor aplica băncilor, furnizorilor de plăți, furnizorilor de monedă electronică, firmelor de investiții, furnizorilor de servicii de criptoactive, precum și furnizorilor terți de servicii TIC care sunt reglementați la nivelul UE.

Conform lui Frances Fitzgerald, membru al Parlamentului European, „*Instituțiile financiare și companiile, inclusiv în spațiul crypto, dețin informații extrem de sensibile despre clienți și este vital ca măsurile de securitate digitală la nivelul UE să fie puse în aplicare pentru a învinge amenințarea care există. Trebuie să punem în aplicare măsuri de protecție mai puternice pentru cetățenii noștri. Nu vrem ca informațiile financiare personale ale nimănui să fie piratate*."

La nivelul României, DNSC, autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, împreună cu Banca Națională a României (BNR) și Autoritatea de Supraveghere Financiară (ASF), vor identifica cele mai bune condiții privind asigurarea securității cibernetice a rețelelor și sistemelor informatice specifice sectorului bancar și a infrastructurii pieței financiare.

Contact pentru presă: Mihai Rotariu | mihai.rotariu@dnsc.ro | 0740 066 866