

Implementarea noii Directive NIS2, în linie dreaptă. Care sunt noutățile pentru companii?

**Robert Gîrdoc**Senior Manager
PwC România**Răzvan Cioc**Manager
PwC România

Directiva NIS2, privind securitatea cibernetică pentru protejarea infrastructurilor critice și digitale, care a intrat în vigoare saptamâna aceasta, actualizează lista sectoarelor și a activităților vizate și prevede cai de atac și sancțiuni pentru a asigura respectarea legislației. Actul normativ trebuie transpus în legislațiile statelor membre în termen de 21 de luni.

În contextul intensificării și agresivității atacurilor cibernetice din ultimii ani marcați de pandemie, război, criza energetică, noile norme vin astfel să consolideze reziliența infrastructurilor critice la o serie de amenințări, inclusiv la riscuri naturale, atacuri teroriste sau sabotaj. În același timp, statele membre vor trebui să adopte o strategie națională și să efectueze evaluări periodice ale riscurilor pentru a identifica entitățile considerate critice sau vitale pentru societate și economie.

Potrivit raportului “PwC 2023 Digital Trust Insights” pentru Europa Centrală și Est, circa 60% dintre directorii generali din această zonă, inclusiv din România, susțin că securitatea cibernetică s-a îmbunătățit ca urmare a investițiilor masive în infrastructura cibernetică și îmbunătățirii colaborării din interiorul companiei, însă mai este mult de lucru având în vedere creșterea complexității, prin interconectarea a tot mai multe sisteme și date, și a atacurilor tot mai elaborate. De altfel, probabilitatea unui atac cibernetic major se află pe locul doi în topul celor cinci scenarii pe care directorii generali le integrează în planurile de reziliență pentru 2023, după recesiunea globală, și au în plan continuarea creșterii bugetului pentru investiții în securitatea cibernetică.

Care sunt principalele modificări aduse de noua directivă

În primul rând, se aplică unui număr mai mare de sectoare și entități decât cele reglementate până acum de NIS1. Astfel, lista de aplicare a NIS2 a fost extinsă de la operatorii de servicii esențiale la toate entitățile mijlocii și mari care își desfășoară activitatea în sectoarele reglementate de directivă sau care furnizează servicii reglementate de directivă. Un număr de 11 sectoare sunt vizate de către noua directivă, printre care: sectorul energetic, transporturi, sectorul bancar, infrastructuri ale pieței financiare, servicii digitale, sănătate, etc.

Noua directivă impune obligații directe asupra managementului companiilor/instituțiilor vizate în ceea ce privește punerea în aplicare și supravegherea respectării legislației de către organizația lor, ceea ce poate duce la amenzi și la interzicerea temporară a exercitării funcțiilor de conducere.

Entitățile vizate trebuie să implementeze măsuri de gestionare a riscurilor cibernetice, care includ cerințe de atenuare a riscurilor de securitate și obligația de diligență din partea furnizorilor/ furnizorilor de servicii terțe. În același timp, acestea trebuie să identifice rapid impactul potențial al incidentelor, înainte sau pe măsura ce acestea se desfășoară, asupra rețelei și sistemelor informatice afectate, cât și asupra dependenței de aceste sisteme, precum și durata și gravitatea întreruperii serviciilor.

Au fost modificate și cerințele privind raportarea incidentelor, NIS2 impunând obligații de notificare în etape, inclusiv o notificare inițială în termen de 24 de ore de la luarea la cunoștință a anumitor incidente sau amenințări cibernetice, iar detaliile trebuie transmise în termen de 72 de ore. O raportare mai detaliată este necesară la o lună de la apariția unui incident semnificativ, ca măsură de monitorizare. Totuși, noul act legislativ raționalizează obligațiile de raportare pentru a evita raportarea excesivă și crearea unei sarcini excesive pentru entitățile vizate.

În ceea ce privește sancțiunile, statelor membre li se acorda libertatea de a stabili măsurile pentru nerespectarea reglementărilor NIS2, precum și amenzi administrative pentru anumite încălcări, de până la 10 milioane euro sau 2% din cifra de afaceri totală.

În plus, Directiva va institui în mod oficial Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice, UE-CyCLONe, care va sprijini gestionarea coordonată a incidentelor și crizelor de securitate cibernetică de mare amploare.

Textul clarifică, de asemenea, faptul că directiva nu se va aplica entităților care desfășoară activități în domenii precum apărarea sau securitatea națională, siguranța publică și asigurarea respectării legii. Sistemul judiciar, parlamentele și băncile centrale sunt de asemenea excluse din domeniul de aplicare. NIS2 se va aplica, însă, administrațiilor publice de la nivel central și regional. În plus, statele membre pot decide ca aceasta să se aplice unor astfel de entități și la nivel local.