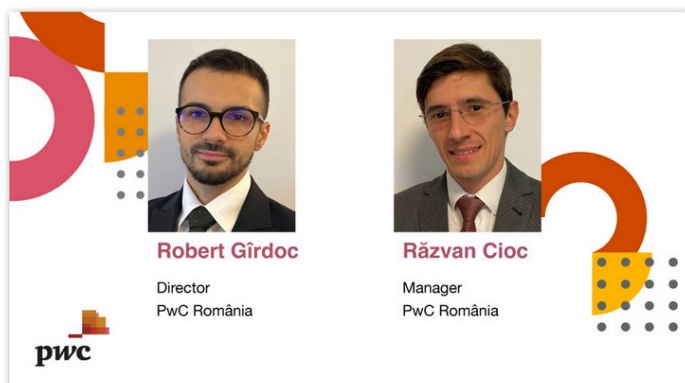


## Conformarea la directiva de securitate cibernetica NIS2 a intrat în linie dreapta. Ce trebuie sa știe companiile?



**Companiile din România care activează în sectoarele esențiale și critice pentru societate și economie, respectiv energie, transport, sanatate, financiar-bancar, apa potabila și infrastructura digitala, precum și din alte domenii considerate importante precum serviciile poștale și de curierat, gestionarea deșeurilor, industria chimica sau cea alimentara trebuie sa se conformeze prevederilor directivei europene NIS2 privind securitatea cibernetica.**

Guvernul a publicat la finalul anului 2024 ordonanța de urgență care transpune în legislația națională NIS2 și care impune o serie de măsuri de gestionare a riscurilor de securitate cibernetica precum continuitatea activității, gestionarea incidentelor sau securitatea lanțului de aprovizionare. Aceasta presupune, de asemenea, entităților vizate sa raporteze autorităților competente incidentele care au un impact semnificativ asupra activității lor. Sarcinile de supraveghere și asigurare a respectării reglementărilor revine Directoratului Național de Securitate Cibernetica (DNSC), autoritate competenta responsabila cu securitatea cibernetica.

### De ce este importanta directiva NIS2?

Atacurile cibernetice au devenit o realitate cotidiana o data cu creșterea nivelului de digitalizare, interconectarea sistemelor informatice și apariția noilor tehnologii - 5G, IoT, AI, dar și a instabilității geopolitice, iar cele mai vizate sunt companiile din sectoare critice. De altfel, în ordonanța de urgență a Guvernului de la finalul anului 2024 care transpune în legislația națională directiva NIS2, este amintit incidentul din primul trimestru al anului 2024, care a afectat 26 de spitale la nivel național. Consecințele atacurilor pot fi devastatoare, de la pierderea de date și întreruperea activității până la daune reputaționale și amenzi substanțiale.

Spre exemplu, în cazul unui atac cibernetice care afectează operațiunile din cauza unui proces de gestionare a riscurilor insuficient monitorizat la o entitate extrem de critica, printre consecințe se regasesc cheltuieli precum plăți de rascumparare, costuri pentru furnizorii externi de servicii, amenzi pentru încălcarea reglementărilor specifice, cât și a cerințelor DNSC, dar și raspunderea directorilor generali și executivi pentru prejudiciile suferite ca urmare a încălcării obligațiilor de monitorizare (cu excepția sectorului administrației publice).

### Ce înseamna NIS 2 pentru companii?

Entitățile care fac obiectul NIS2 trebuie sa aiba în vedere îmbunătățirea atât a măsurilor lor de gestionare a riscurilor de securitate cibernetica, cât și a programelor de raportare a incidentelor, pentru a se conforma cerințelor impuse. Nerespectarea NIS2 poate conduce la amenzi semnificative din partea autorităților, dar și la costuri semnificative pentru organizații.

Pentru a se pregăti, entitățile vizate de NIS 2 trebuie sa ia în considerare: stabilirea unui cadru de guvernanta

privind securitate cibernetică care să acopere toate aspectele identificarea, evaluarea și gestionarea riscurilor, actualizarea periodică a politicilor de securitate IT, implementarea unor controale stricte referitoare la accesul la date, microsegmentarea, adoptarea unor tehnologii (avansate) de detecție și răspuns aliniată la obiectivele și principalele zone de risc ale business-ului, proceduri clare de raportare a incidentelor, detecție și monitorizare automatizată în timp real sau periodic, formarea continuă a personalului, înregistrarea detaliată a incidentelor de securitate cibernetică, evaluări regulate ale riscurilor și audituri. Implementarea acestor măsuri va sprijini un management integrat al riscurilor la nivelul companiei.

Măsurile luate trebuie să asigure un nivel de securitate cibernetică adecvat nivelului de risc al entității, care se evaluează conform metodologiei cuprinse în ordinul directorului DNSC. De asemenea, entitățile esențiale și cele importante sunt obligate să se supună efectuării unui audit de securitate cibernetică în condițiile și cu periodicitatea stabilite de DNSC, în funcție de nivelul de risc.

Comaniile vizate trebuie să raporteze, fără întârzieri nejustificate, orice incident care are un impact semnificativ asupra prestării serviciilor lor prin intermediul Platformei naționale pentru raportarea incidentelor de securitate cibernetică - PNRISC. Astfel, trebuie să raporteze nu mai târziu de 24 de ore de la data la care au luat cunoștința de incidentul semnificativ, o avertizare timpurie care, după caz, dacă există suspiciuni că incidentul este cauzat de acțiuni ilicite sau rauvoitoare sau că ar putea avea un impact transfrontalier sau nu mai târziu de 72 de ore din momentul în care au luat cunoștința de incidentul semnificativ dacă prezintă o evaluare inițială a acestuia, inclusiv a gravității și a impactului acestuia, precum și a indicatorilor de compromitere.

Un incident este considerat semnificativ sau impactul unui incident este considerat semnificativ dacă a provocat sau poate provoca perturbări operaționale grave ale serviciilor sau pierderi financiare pentru entitatea în cauză, a afectat sau poate afecta alte persoane fizice sau juridice, cauzând prejudicii materiale sau nonmateriale considerabile.

DNSC poate derula activități de supraveghere, verificare și control efectuate de persoane desemnate în acest sens și poate dispune efectuarea de audituri de securitate ad-hoc, realizate de un auditor de securitate cibernetică atestat.

### **Care sunt consecințele nerespectării reglementărilor?**

Următoarele fapte constituie încălcări grave: neîndeplinirea obligației de notificare sau de remediere a incidentelor semnificative, neîndeplinirea obligației de remediere a deficiențelor constatate de către autoritățile competente, obstrucționarea auditurilor sau a activității de monitorizare dispuse de DNSC în urma constatarilor, furnizarea de informații false sau vadiți denaturate, îngrădirea accesului personalului desemnat de către DNSC în spațiile supuse controlului, cât și asupra datelor și informațiilor necesare controlului, etc.

Vor fi aplicate contravenții pentru nerespectarea, printre altele, a obligațiilor privind luarea unor măsuri tehnice, operaționale și organizatorice, de a se supune unui audit de securitate cibernetică în condițiile stabilite, de a transmite datele solicitate, de a realiza și transmite anual autoevaluarea nivelului de maturitate, de a întocmi și transmite planul de măsuri pentru remedierea deficiențelor, în termen de 30 de zile de la realizarea autoevaluării, de a pune în aplicare măsurile de gestionare a riscurilor, de a urma cursuri de formare profesională în domeniul securității cibernetică, etc

Pentru entitățile esențiale, amenzile pornesc de la 10.000 lei și pot ajunge la 10 milioane euro sau cel mult 2% din cifra de afaceri netă, luându-se în considerare valoarea cea mai mare dintre acestea.

Pentru entitățile importante, amenzile pot ajunge până la cel mult 7 milioane euro sau cel mult 1,4% din cifra de afaceri netă.

Sectoare de importanța critică ridicată sunt energie, transport, sectorul financiar-bancar, sănătate, apă potabilă, infrastructură, digitală, administrație publică. Alte sectoare de importanța critică sunt serviciile poștale și de curierat, gestionarea deșeurilor, fabricarea, producția și distribuția de substanțe chimice, producția, prelucrarea și distribuția de alimente, fabricarea de dispozitive medicale, computere, echipamente electronice și furnizorii de servicii digitale.