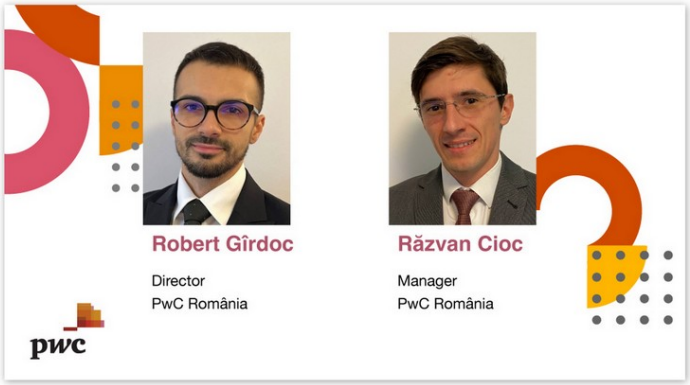
Conformarea la directiva de securitate cibernetica NIS2 a intrat în linie dreapta. Ce trebuie sa știe companiile?



Companiile din România care activeaza 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 urgența care transpune în legislatia nationala NIS2 și care impune o serie de masuri 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 respectarii reglementarilor 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 ordonanta de urgenta a Guvernului de la finalul anului 2024 care transpune în legislatia nationala 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 pâna la daune reputaționale și amenzi substanțiale.
Spre exemplu, în cazul unui atac cibernetic care afecteaza operațiunile din cauza unui proces de gestionare a riscurilor insuficient monitorizat la o entitate extrem de critica, printre consecințe se regasesc cheltuieli precum plați de rascumparare, costuri pentru furnizorii externi de servicii, amenzi pentru încalcarea reglementarilor specifice, cat și a cerințelor DNSC, dar și raspunderea directorilor generali și executivi pentru prejudiciile suferite ca urmare a încalcarii obligațiilor de monitorizare (cu excepția sectorului administrației publice).

Ce înseamna NIS 2 pentru companii?

Entitațile care fac obiectul NIS2 trebuie sa aiba în vedere îmbunatațirea atât a masurilor 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 pregati, entitațile vizate de NIS 2 trebuie sa ia în considerare: stabilirea unui cadru de guvernanta

privind securitate cibernetica care sa acopere toate aspectele identificarea, evaluarea şi gestionarea riscurilor, actualizarea periodica a politicilor de securitate IT, implementarea unor controale stricte referitoare la accesul la date, microsegmentarea, adoptarea unor tehnologii (avansate) de detecţie şi raspuns aliniate la obiectivele şi principalele zone de risc ale business-ului, proceduri clare de raportare a incidentelor, detectare şi monitorizare automatizata în timp real sau periodic, formarea continua a personalului, înregistrarea detaliata a incidentelor de securitate cibernetica, evaluari regulate ale riscurilor şi audituri. Implementarea acestor masuri va sprijini un management integrat al riscurilor la nivelul companiei.

Masurile luate trebuie sa asigure un nivel de securitate cibernetica adecvat nivelului de risc al entitaţii, care se evalueaza conform metodologiei cuprinse în ordinul directorului DNSC. De asemenea, entitaţile esenţiale şi cele importante sunt obligate sa se supuna efectuarii unui audit de securitate cibernetica în condiţiile şi cu periodicitatea stabilite de DNSC, în funcţie de nivelul de risc.

Companiile vizate trebuie sa raporteze, fara întârzieri nejustificate, orice incident care are un impact semnificativ asupra prestarii serviciilor lor prin intermediul Platformei naţionale pentru raportarea incidentelor de securitate cibernetica - PNRISC. Astfel, trebuie sa raporteze nu mai târziu de 24 de ore de la data la care au luat cunoştinţa de incidentul semnificativ, o avertizare timpurie care, dupa caz, daca exista suspiciuni ca incidentul este cauzat de acţiuni ilicite sau rauvoitoare sau ca ar putea avea un impact transfrontalier sau nu mai târziu de 72 de ore din momentul în care au luat cunoştinţa de incidentul semnificativ daca prezinta o evaluare iniţiala a acestuia, inclusiv a gravitaţii şi a impactului acestuia, precum şi a indicatorilor de compromitere.

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

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

Care sunt consecinţele nerespectarii reglementarilor?

Urmatoarele fapte constituie încalcari grave: neîndeplinirea obligaţiei de notificare sau de remediere a incidentelor semnificative, neîndeplinirea obligaţiei de remediere a deficienţelor constatate de catre autoritaţile competente, obstrucţionarea auditurilor sau a activitaţii de monitorizare dispuse de DNSC în urma constatarilor, furnizarea de informaţii false sau vadit denaturate, îngradirea accesului personalului desemnat de catre DNSC în spaţiile supuse controlului, cât şi asupra datelor şi informaţiilor necesare controlului, etc.

Vor fi aplicate contravenţii pentru nerespectarea, printre altele, a obligaţiilor privind luarea unor masuri tehnice, operaţionale şi organizatorice, de a se supune unui audit de securitate cibernetica în condiţiile stabilite, de a transmite datele solicitate, de a realiza şi transmite anual autoevaluarea nivelului de maturitate, de a întocmi şi transmite planul de masuri pentru remedierea deficienţelor, în termen de 30 de zile de la realizarea autoevaluarii, de a pune în aplicare masurile de gestionare a riscurilor, de a urma cursuri de formare profesionala în domeniul securitaţii cibernetice, etc

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

Pentru entitaţile importante, amenzile pot ajunge pâna la cel mult 7 milioane euro sau cel mult 1,4% din cifra de afaceri neta.

Sectoare de importanţa critica ridicata sunt energie, transport, sectorul financiar-bancar, sanatate, apa potabila, infrastrtuctura, digitala, administraţie publica. Alte sectoare de importanţa critica sunt serviciile poştale şi de curierat, gestionarea deseurilor, fabricarea, producţia şi distribuţia de substanţe chimice, producţia, prelucrarea şi distribuţia de alimente, fabricarea de dispozitive medicale, computere, echipamente electronice şi furnizorii de servicii digitale.