BIT SENTINEL

Consultanță și audit de securitate pentru conformitate cu Directiva NIS

După intrarea în vigoare a regulamentului GDPR, Uniunea Europeană s-a concentrat pe întărirea rezilienței statelor în fața atacurilor cibernetice, pe protejarea infrastructurilor critice și digitale și pe asigurarea funcționării sistemelor care sunt fundamentale pentru societate.

Astfel, Directiva NIS (a se vedea UE 2016/1148) devenea primul act legislativ în materie de securitate cibernetică la nivelul Uniunii.

Pentru a ține pasul cu evoluția digitalizării și a peisajului amenințărilor la adresa securității cibernetice, normele UE în materie de securitate cibernetică din 2016 au fost actualizate prin Directiva NIS2, care a intrat în vigoare în 2023.

Directiva NIS2 extinde domeniului de aplicare al normelor de securitate cibernetică la noi sectoare și entități și îmbunătățește capacitățile de reziliență și de răspuns la incidente ale entităților publice și private, ale autorităților competente și ale Uniunii Europene în ansamblu. Directiva NIS2 se aplică tuturor statelor membre UE.

Entități care cad sub incidența prevederilor Directivei NIS2

◆ Entități esențiale

Organizații cu peste 250 de angajați și o cifră de afaceri de 50 de milioane de euro care activează în sectoare extrem de critice:

- Energie (energie electrică, termoficare și răcire centralizată, petrol, gaze și hidrogen)
- Transport (aerian, feroviar, naval, rutier)
- Bănci și piețe financiare (bănci, companii de asigurări, firme de investiții)
- Apă potabilă și ape reziduale
- Infrastructuri digitale și gestionarea serviciilor TIC (furnizori de servicii gestionate și furnizori de servicii de securitate gestionate)
- Administrație publică
- Spațiu

◆ Entități importante

Organizații cu peste 50 de angajați și o cifră de afaceri de 10 milioane de euro care activează în sectoare critice:

- Servicii poștale și de curierat
- Gestionarea deșeurilor
- Fabricarea, producția și distribuția de produse chimice
- Industria prelucrătoare (calculatoare și electronice, mașini și echipamente, autovehicule și alte echipamente de transport)
- Furnizori digitali (piețe online, motoare de căutare, furnizori de servicii de rețele sociale)
- Organizații de cercetare
- Producția, prelucrarea și distribuția alimentelor (producție și prelucrare industrială)

Entități care cad sub incidența prevederilor Directivei NIS

A) Operatorii de Servicii Esențiale (OSE) din 7 sectoare de activitate economică

- Energie
- Transport
- Sectorul bancar
- Infrastructuri ale pieței financiare
- Sectorul sănătății
- Furnizarea de apă potabilă
- Infrastructură digitală

B) Furnizorii de Servicii Digitale (FSD) din 3 categorii

- Piețe online
- Motoare de căutare online
- Servicii de cloud computing

**Entitățile importante includ și sectorul entităților esențiale, însă încadrat în pragurile specifice pentru entitățile importante.*

Toate aceste organizații trebuie să respecte aceleași cerințe de raportare și de gestionare a securității cibernetice. Totuși, directiva NIS2 stabilește o diferențiere a regimurilor de supraveghere între entitățile esențiale și cele importante, în vederea asigurării unui echilibru corect al obligațiilor atât pentru entități, cât și pentru autoritățile competente.

Cerințe impuse de către Directiva NIS2

◆ Managementul riscului

- ◆ analiza riscurilor
- ◆ politici de securitate a sistemelor informatice
- ◆ proceduri de gestionare a incidentelor
- ◆ pregătirea pentru asigurarea continuității activității și gestionarea crizelor
- ◆ securitatea lanțului de aprovizionare
- ◆ criptografie și criptare
- ◆ evaluarea eficacității gestionării riscurilor
- ◆ gestionarea riscurilor la terți în întregul lor lanț de aprovizionare

◆ Raportare

- ◆ incidente potențiale care ar putea provoca daune operaționale sau financiare substanțiale
- ◆ dispoziții precise privind procesul de raportare a incidentelor
- ◆ o echipă de răspuns la incidentele de securitate informatică (CSIRT) care facilitează interacțiunile dintre entitățile care raportează, producătorii IT și furnizorii de servicii IT

◆ Gestionarea și divulgarea vulnerabilităților

- ◆ hackerii etici pot raporta vulnerabilitățile
- ◆ remedierea vulnerabilităților raportate
- ◆ Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) păstrează o bază de date cu vulnerabilitățile cunoscute

Cerințe impuse de către Directiva NIS

A) Pentru Operatorii de Servicii Esențiale (OSE)

- managementul drepturilor de acces, al identificării și autentificării utilizatorilor
- conștientizarea și instruirea utilizatorilor și asigurarea securității personalului
- testarea și evaluarea securității rețelelor și sistemelor informatice
- managementul configurațiilor rețelelor și sistemelor informatice
- asigurarea disponibilității și continuității serviciului esențial și a funcționării rețelelor și sistemelor informatice
- răspunsul la incidente și managementul vulnerabilităților și alertelor de securitate
- mentenanța și asigurarea protecției fizice a rețelelor și sistemelor informatice
- realizarea planurilor de securitate
- asigurarea protecției produselor și serviciilor aferente rețelelor și sistemelor informatice

B) Pentru Furnizorii de Servicii Digitale (FSD)

- securitatea sistemelor și a instalării acestora
- gestionarea incidentelor de securitate
- gestionarea continuității activității
- monitorizarea, auditarea și testarea
- conformitatea cu standardele europene și internaționale

Sancțiuni pentru organizațiile care nu respectă prevederile Directivei NIS2

◆ **Pentru entitățile esențiale - maxim 10 milioane de euro sau 2 % din cifra de afaceri totală din exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare.**

◆ **Pentru entitățile importante - maxim 7 milioane de euro sau cel puțin 1,4 % din cifra de afaceri totală din exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare.**

Sancțiuni conform Directivei NIS

Entitățile care nu respectă normele NIS pot fi amendate cu până la 5% din cifra de afaceri. De asemenea, în cazul încălcărilor repetate, amenzile variază între 3.000 și 50.000 RON. Operatorii cu cifra de afaceri de peste 2 milioane RON riscă amenzi între 0.5% și 2% din cifra de afaceri.

Timeline pentru implementarea Directivei NIS2

16 ianuarie 2023
Directiva NIS2 intră în vigoare.

1

18 octombrie 2024
Termenul la care Statele Membre trebuie să transpună directiva în legislația națională.

2

17 aprilie 2025
Termenul la care Statele Membre trebuie să întocmească listele cu entități esențiale și importante.

3

Bit Sentinel deține atestatul de auditor de securitate cibernetică – special, comun și general pentru operatorii de servicii esențiale, emis de către DNSC – Directoratul Național de Securitate Cibernetică. Această acreditare este o recunoaștere a capabilității echipei și a companiei în a furniza servicii profesionale de securitate cibernetică pentru a atesta conformitatea cu Directiva NIS.

Contactează un specialist Bit Sentinel!

contact@bit-sentinel.com
bit-sentinel.com

BIT SENTINEL