certSIGN

Ghid pentru alinierea companiilor la Directiva NIS2

Despre Directiva NIS2

Directiva europeană NIS2 (nr. 2555/2022) a intrat în vigoare și în România, prin adoptarea de către Guvernul României a OUG nr 155, publicată în Monitorul Oficial la sfârșitul anului 2024.

Aceasta este ordonanța prin care se urmărește implementarea cerințelor prevăzute în directiva NIS 2, având un impact semnificativ asupra mediului de afaceri. Sunt practic extinse cerinţele de securitate cibernetică faţă de versiunea anterioară (NIS1) şi sunt impuse obligaţii stricte în materie de guvernanţă, risc şi conformitate.

Acest ghid este destinat companiilor care trebuie să se conformeze noilor cerinţe şi oferă informaţii esenţiale despre paşii necesari pentru conformare.

certSIGN

Ghid pentru alinierea companiilor la Directiva NIS2

Cine trebuie să se conformeze?

Directiva NIS2 vizează două categorii principale de entităţi:

1. Entităţi esenţiale

Activează în sectoare cu importanţă critică ridicată, ca:
• Energie
• Transporturi
• Apărare
• Finanţe
• Sănătate
• Apă potabilă şi ape uzate
• Spaţiu şi infrastructuri digitale

2. Entităţi importante

Noua directivă extinde domeniul de aplicabilitate pentru sectoare precum:
• Servicii poştale şi de curierat
• Gestionarea deşeurilor
• Industria alimentară
• Industria chimică
• Furnizori digitali (magazine online, motoare de căutare, reţele sociale)
• Producători de dispozitive medicale, echipamente electrice, autovehicule

Ce companii sunt vizate?

Directiva se aplică:
• **Companiilor medii** (50 - 249 angajaţi, cifră de afaceri până la 50 milioane euro)
• **Companiilor mari** (peste 250 de angajaţi, cifră de afaceri peste 50 milioane euro)

Astfel, nu doar marile corporaţii sunt vizate, ci şi afacerile medii, ceea ce impune o nevoie urgentă de aliniere la toate cerinţele directivei.

Sancţiuni pentru neconformare

Nerespectarea NIS2 poate atrage sancţiuni severe:
• **Entităţi importante:** amenzi de până la 7 milioane euro sau 1.4% din cifra de afaceri
• **Entităţi esenţiale:** amenzi de până la 10 milioane euro sau 2% din cifra de afaceri

Amenzile se pot dubla în cazul unor abateri grave, precum:
• Neinformarea autorităţilor despre incidente de securitate
• Obstrucţionarea auditurilor DNSC
• Oferirea de informaţii false despre măsurile de securitate

Ghid pentru alinierea companiilor la Directiva NIS2

Paşii pentru conformare

1. PREPARE (PREGĂTIRE)

- Realizarea unui **inventar complet** al echipamentelor, software-urilor şi datelor sensibile
- Definirea **rolurilor angajaţilor** şi a responsabilităţilor acestora, împreună cu organizarea unor cursuri de instruire a personalului care are acces la datele sensibile ale companiei
- Crearea unui **plan de continuitate a afacerii** pentru a răspunde la atacuri

2. PROTECT (PROTECȚIE)

- Implementarea de **mecanisme de control** al accesului
- Adoptarea de **tehnologii hardware şi software** pentru protecţia datelor
- **Actualizarea automată** a sistemelor de securitate
- **Criptarea informaţiilor sensibile**

3. DETECT (DETECŢIE)

- Implementarea de **sisteme de monitorizare** pentru identificarea atacurilor
- Identificarea rapidă a **riscurilor de securitate**
- Aplicarea de **contramăsuri automate** pentru limitarea efectelor atacurilor

4. RESPOND & RECOVER (RĂSPUNS ȘI RECUPERARE)

- Crearea unui **plan de intervenţie** pentru incidente de securitate
- Implementarea unui **plan de back-up** în vederea restaurării rapide a sistemelor
- Organizarea de **cursuri de instruire** pentru angajaţi privind securitatea cibernetică

Ce trebuie să facă antreprenorii?

1. Informare continuă
Monitorizați informările oficiale de la DNSC (www.dnsc.ro) pentru noutăţi privind normele de aplicare.

2. Realizarea unei evaluări iniţiale de conformitate
Colaboraţi cu specialiști în securitate cibernetică pentru a identifica riscurile şi punctele vulnerabile.

3. Revizuirea şi implementarea unei strategii de securitate
Pregătiți o strategie de securitate care să respecte standardele în materie și aplicați-o la nivelul companiei.

Implementați mecanisme avansate menite a proteja infrastructurile IT deținute, alături de cursuri de pregătire training pentru angajați.

Indentificați în timp real atacurile cibernetice, riscurile de securitate și folosiți instrumente de aplicare automată a unor contramăsuri în vederea eliminării acestora.

Și nu în ultimul rând implementați o serie de metode eficiente de răspuns la incidente care să asigure continuitatea afacerii.

Cu alte cuvinte, asiguraţi-vă că strategia companiei include Prepare, Protect, Detect, Respond & Recover.

4.Luarea unor măsuri de securitate a datelor sensibile ale companiei
Implementați mecanisme de control care vizează cine se conectează în rețeaua internă și folosește PC-urile sau alte dispozitive din infrastructura companiei.

Implementați tehnologii hardware și software care să permită protecția datelor.

certSIGN

Ghid pentru alinierea companiilor la Directiva NIS2

Setați actualizarea automată a sistemelor de securitate și crearea automată a backup-urilor prin definirea unui plan de Disaster Recovery.

Criptarea informațiilor sensibile stocate sau în tranzit este foarte importantă pentru a preveni accesul persoanelor neautorizate.

Realizați și implementați un plan de continuitate a afacerii, prin realizarea de back-up-uri planificate a sistemelor informatice.

Realizați și implementați cursuri și exerciții cu privire la antrenarea personalului în identificarea situațiilor de risc ce pot apărea.

5. Consultaţi experţi în securitate cibernetică
Apelaţi la companii atestate de DNSC pentru audituri şi servicii de consultanţă, precum certSIGN.

De reținut!

Directiva NIS2 impune pentru companii din diverse sectoare noi standarde de securitate cibernetică. Procesul de conformare poate părea complex, dar adoptarea unui plan structurat bazat pe **Prepare, Protect, Detect, Respond & Recover** va asigura protecţia afacerii şi evitarea sancţiunilor.

Pregătirea din timp şi colaborarea cu specialişti în domeniu reprezintă cheia succesului într-o lume digitală din ce în ce mai vulnerabilă la atacuri cibernetice.

Surse:
https://dnsc.ro/vezi/document/oug-privind-transpunerea-directivei-nis-2
https://legislatie.just.ro/public/DetaliiDocument/293121#id_artA842_ttl

Cyber360 by certSIGN

În calitate de auditor atestat de DNSC, vă punem la dispoziție expertiza și suportul nostru. Puteți lua legătura cu specialiștii noștri în secțiunea de contact din pagina certsign.ro/cyber360

certSIGN
www.certsign.ro
office@certsign.ro
+4 031 101 18 70
29 A Tudor Vladimirescu Blvd, AFI Tech Park 1, S5, Bucharest, Romania