Direttiva UE 2022/255 (NIS 2)

La Direttiva UE 2022/2555, conosciuta come NIS 2, è una normativa comunitaria in materia di cybersicurezza che mira a stabilire un livello comune di sicurezza informatica tra gli Stati Membri dell'Unione Europea imponendo stringenti obblighi alle organizzazioni operanti in settori ritenuti particolarmente critici. L'obiettivo principale della NIS2 è garantire la protezione dei dati e delle infrastrutture digitali, riducendo il rischio di incidenti informatici e assicurando una risposta efficace alle violazioni della sicurezza. Ci sono tre criteri che definiscono se un'organizzazione è soggetta alla Direttiva NIS: il criterio del **settore merceologico**, la **territorialità** e il **dimensionamento** dell'organizzazione.

1. Criterio del settore merceologico

La Direttiva declina il criterio del settore merceologico dividendo tra

- **Soggetti essenziali**
  Rientrano in questa categoria le organizzazioni pubbliche e private che operano nei seguenti settori:
  - energetico (energia elettrica, teleriscaldamento e teleraffreddamento, petrolio, gas, idrogeno);
  - trasporto (aereo, ferroviario, per vie d'acqua, su strada)
  - bancario;
  - infrastrutture dei mercati finanziari;
  - sanitario;
  - acqua potabile;
  - acque reflue;
  - infrastrutture digitali;
  - gestione dei servizi TIC (business-to-business);
  - spazio.
- **Soggetti importanti**
  Invece, con questa categoria si fa riferimento alle organizzazioni dei seguenti settori:
  - servizi postali e di corriere;
  - gestione dei rifiuti;
  - fabbricazione, produzione e distribuzione di sostanze chimiche;
  - produzione, trasformazione e distribuzione di alimenti;
  - fabbricazione (fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro, fabbricazione di computer e prodotti di elettronica e ottica, fabbricazione di apparecchiature elettriche, fabbricazione di macchinari e apparecchiature n.c.a., fabbricazione di autoveicoli, rimorchi e semirimorchi, fabbricazione di altri mezzi di trasporto);
  - fornitori di servizi digitali;

- ricerca.

Nella normativa NIS 2, i requisiti di cybersicurezza sono uniformi per "Soggetti essenziali" e "Soggetti importanti"; non si distinguono in termini di standard e pratiche di sicurezza da adottare. Tuttavia, esistono divergenze significative per quanto riguarda la severità dei controlli e l'entità delle sanzioni imposte. In particolare, le "entità essenziali" affrontano ispezioni più rigide e penalità finanziarie maggiori rispetto ai "Soggetti importanti". Questa distinzione sottolinea l'importanza delle prime nell'ecosistema della sicurezza informatica.

2. Criterio della territorialità

Secondo questo criterio, la NIS 2 si applicherà esclusivamente alle organizzazioni che offrono servizi o operano all'interno dell'Unione Europea.

3. Criterio del dimensionamento

La NIS2 sarà vincolante per le medie imprese, come definite ai sensi dell'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE, o per le organizzazioni che superano i limiti dimensionali delle medie imprese. Ciò significa che entreranno automaticamente nel perimetro di applicazione della Direttiva:

- le grandi imprese, con più di 250 dipendenti e un fatturato annuo maggiore di 50 milioni di euro o un totale di bilancio annuo superiore a 43 milioni di euro;
- le medie imprese, ossia quelle con un numero di dipendenti compreso fra 50 e 250 e un fatturato annuo compreso fra 10 e 50 milioni di euro o con un totale di bilancio annuo compreso tra i 10 e i 43 milioni di euro.

Tuttavia, all'art. 2 par. 2 vengono previste alcune eccezioni al criterio del dimensionamento. Viene infatti stabilito che, indipendentemente dalle dimensioni dell'organizzazione, la Direttiva NIS2 si applicherà qualora:

- i servizi siano forniti da fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico, prestatori di servizi di fiducia, registri dei nomi di dominio di primo livello e fornitori di sistema dei nomi di dominio;
- il soggetto sia l'unico fornitore in uno Stato membro di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;
- una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;
- una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;

- il soggetto sia critico in ragione della sua particolare importanza a livello nazionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro;
- il soggetto è un ente della pubblica amministrazione: dell'amministrazione centrale quale definito da uno Stato membro conformemente al diritto nazionale, oppure a livello regionale quale definito da uno Stato membro conformemente al diritto nazionale che, a seguito di una valutazione basata sul rischio, fornisce servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali o economiche critiche;
- ai soggetti identificati come critici ai sensi della Direttiva (UE) 2022/2557 (Direttiva CER) relativa alla resilienza dei soggetti critici;
- ai soggetti che forniscono servizi di registrazione dei nomi di dominio.