acs srl
SYSTEM & CONSULTING

Direttiva NIS 2

(Network and Information Systems 2)

www.acsweb.it

Direttiva NIS 2 (Network and Information Systems 2)

La NIS 2 (Network and Information Systems 2) è una Direttiva UE (2022/2555) entrata in vigore il 17 gennaio 2023 che dovrà essere recepita dai singoli Stati membri entro il 17 ottobre 2024. Lo scopo principale di questo provvedimento è quello di rafforzare la sicurezza informatica nell'Unione, in risposta alle crescenti minacce informatiche e alla necessità di un quadro normativo aggiornato per garantire una cibersicurezza coerente e robusta.

La direttiva NIS 2 ha aggiornato la precedente NIS 1, che era stata approvata nel 2016 dall'UE (Direttiva UE 2016/1148) e recepita nel 2018 dall'Italia. La precedente direttiva NIS è stata il primo passo significativo verso la regolamentazione della cibersicurezza a livello europeo, ma è stata superata dagli sviluppi tecnologici e dalle sfide emergenti.

Chi deve rispettarla?

La direttiva NIS 2 impone requisiti di cibersicurezza a un'ampia gamma di settori e attività economiche, ampliando notevolmente il campo di applicazione rispetto alla precedente direttiva NIS. Per stabilire quali aziende devono rispettare gli obblighi previsti, la direttiva NIS 2 indica tre criteri:

1. **Settore di appartenenza**
   La direttiva si applica ai *soggetti essenziali*, ovvero quelli che operano nei settori ad alta criticità e ai *soggetti importanti*, ovvero che operano negli altri settori critici. I primi sono settori che per la natura delle attività svolte sono cruciali per il funzionamento del sistema paese (ad esempio energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario ecc..), i secondi invece sono settori di elevato interesse pubblico (ad esempio servizi postali e di corriere, gestione dei rifiuti, produzione e distribuzione di alimenti, prodotti chimici e farmaceutici ecc…);

2. **Criterio dimensionale**
   La NIS 2 si applica principalmente a soggetti, indipendentemente dalla loro natura pubblica o privata, di medie o grandi dimensioni che operano nei settori critici coperti dalla direttiva. Ai sensi dei criteri del dimensionamento, sono automaticamente coinvolte tutte le grandi imprese dei settori individuati, vale a dire quelle con più di 250 dipendenti o un fatturato annuo maggiore di 50 milioni di euro o un totale di bilancio annuo superiore a 43 milioni di euro. Sono inoltre coinvolte le medie imprese, ossia quelle con un numero di dipendenti compreso fra 50 e 250 o un fatturato annuo o un totale di bilancio compreso fra 10 e 50 milioni di euro o con un totale di bilancio annuo non superiore a 43 milioni di euro, che operano nei settori individuati.
   L'introduzione di questo criterio è volto ad assicurare che l'applicazione della normativa sia proporzionata alla capacità e alle risorse delle organizzazioni;

3. **Ruolo**
   Si tratta di un criterio che consente di analizzare il ruolo che le aziende hanno nel loro settore, imponendo l'adeguamento a coloro che svolgono attività che potrebbero avere un impatto rilevante sulla sicurezza informatica dell'UE.

È importante sottolineare che, sebbene le grandi e medie organizzazioni siano le principali destinatarie della direttiva, la NIS 2 riconosce anche la necessità di proteggere le catene di fornitura e le partnership di organizzazioni di tutte le dimensioni, comprese le piccole imprese, poiché potrebbero rappresentare punti di ingresso per gli attacchi informatici.
In generale, quindi, la direttiva copre le grandi organizzazioni nei settori chiave, ma anche le piccole e medie imprese (PMI) possono essere incluse se operano in settori considerati critici o ad alto rischio.

Cosa prevede la NIS 2?

La direttiva NIS 2 stabilisce delle norme minime che tutti gli Stati membri devono rispettare per avere una maggiore armonizzazione a livello UE di legislazioni e procedure di cibersicurezza. Tuttavia, i singoli Stati sono liberi di approvare norme nazionali ancora più severe, decidendo di innalzare ulteriormente il loro livello di cibersicurezza nazionale.

I requisiti della direttiva NIS 2 quindi riguardano:

- l'adozione di misure di sicurezza per la gestione dei rischi informatici;
- la segnalazione tempestiva degli incidenti informatici alle autorità competenti;
- la gestione della sicurezza delle catene di fornitura informatiche;
- la cooperazione con le autorità e altre organizzazioni in caso di incidenti informatici.

Dal punto di vista della governance, la NIS 2 prevede che gli organi di gestione dei soggetti essenziali e importanti, debbano approvare le misure per la gestione dei rischi adottate dall'Organizzazione, seguire una formazione periodica su tematiche di cybersicurezza e offrire una formazione analoga ai loro dipendenti.

In ambito risk management, pertanto, vi è l'obbligo di valutare i rischi e attuare le necessarie misure tecniche e organizzative (Art. 21 della direttiva). Tali rischi comprendono anche quelli legati alla supply-chain, ovvero le organizzazioni in perimetro sono tenute a garantire la sicurezza della propria catena di approvvigionamento, presidiando gli aspetti di sicurezza dei rapporti con i propri fornitori, considerandone le vulnerabilità specifiche nonché la qualità complessiva di prodotti e pratiche di cybersicurezza.

In sintesi, l'adozione della NIS 2 richiede un impegno significativo da parte delle organizzazioni interessate, ma offre anche benefici a lungo termine per la sicurezza informatica e la stabilità delle infrastrutture critiche in tutta l'UE. La compliance non solo migliorerà la protezione contro gli attacchi informatici, ma rafforzerà anche la capacità di risposta e ripristino in caso di incidenti.