Direttiva NIS 2

messa in sicurezza delle reti e dei sistemi informativi

La direttiva NIS2 istituisce un quadro giuridico unificato per sostenere la cibersicurezza in 18 settori critici in tutta l'UE. Invita inoltre gli Stati membri a definire strategie nazionali in materia di cibersicurezza e a collaborare con l'UE per la reazione e l'applicazione transfrontaliere.

La sicurezza informatica comporta la protezione **dei sistemi informativi e di rete** (NIS), dei loro utenti e di altri individui colpiti da incidenti e minacce informatiche. Per rispondere alla maggiore esposizione dell'Europa alle minacce informatiche, la direttiva 2022/2555, nota anche come NIS2,

ha sostituito la precedente direttiva (UE) 2016/1148 o NIS1. NIS2 innalza il livello comune di ambizione dell'UE in materia di cibersicurezza, attraverso un ambito di applicazione più ampio, norme più chiare e strumenti di vigilanza più solidi. Esso impone agli Stati membri di **rafforzare le loro capacità in materia di cibersicurezza**, introducendo nel contempo misure di gestione dei rischi e obblighi di segnalazione ai soggetti di un maggior numero di settori e stabilendo norme per la cooperazione, la condivisione delle informazioni, la vigilanza e l'applicazione delle misure di cibersicurezza.

La direttiva impone a ciascuno Stato membro di adottare una strategia nazionale in materia di cibersicurezza, che comprenda politiche per la sicurezza della catena di approvvigionamento, la gestione delle vulnerabilità e l'educazione e la sensibilizzazione in materia di cibersicurezza. Gli Stati membri devono inoltre redigere e aggiornare regolarmente un elenco di operatori di servizi essenziali, garantendo che tali soggetti rispettino i requisiti della direttiva.

Oltre ai settori già coperti dalla NIS 1 - energia, trasporti, assistenza sanitaria, finanza, gestione delle risorse idriche e infrastrutture digitali - le nuove norme si applicano anche ai fornitori di comunicazioni elettroniche pubbliche, a un maggior numero di servizi digitali (come le piattaforme sociali), alla gestione dei rifiuti e delle acque reflue, alla fabbricazione di prodotti critici, ai servizi postali e di corriere e alla pubblica amministrazione a livello centrale e regionale, nonché al settore spaziale. Di norma, i soggetti di medie e grandi dimensioni in questi settori critici dovranno adottare adeguate misure di gestione dei rischi per la cibersicurezza e notificare alle autorità nazionali competenti gli incidenti significativi. Si tratta di incidenti che potrebbero causare perturbazioni o danni significativi.

La direttiva comprende anche disposizioni in materia di vigilanza, applicazione e valutazioni inter pares volontarie per rafforzare la fiducia reciproca e le capacità di cibersicurezza in tutta l'UE. Introduce inoltre la responsabilità dell'alta dirigenza per il mancato rispetto delle misure di gestione dei rischi di cibersicurezza, portando così la cibersicurezza all'attenzione del consiglio di amministrazione.

La direttiva istituisce una rete di squadre di intervento per la sicurezza informatica in caso di incidente (CSIRT) per scambiare informazioni sulle minacce informatiche e rispondere agli incidenti. Queste squadre sono fondamentali per mantenere la consapevolezza situazionale e offrire assistenza. Per gestire gli incidenti o le crisi di cibersicurezza su vasta scala, la direttiva istituisce la rete europea di organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe). Questa rete sostiene la gestione coordinata e garantisce lo scambio regolare di informazioni tra gli Stati membri e le istituzioni dell'UE in caso di incidenti e crisi su vasta scala.

Parallelamente, il gruppo di cooperazione NIS

è una piattaforma istituita dalla direttiva NIS per facilitare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri dell'UE, la Commissione europea e l'Agenzia dell'UE per la cibersicurezza (ENISA). Il gruppo pubblica orientamenti e raccomandazioni non vincolanti a sostegno dell'attuazione della direttiva NIS.

Contesto

La direttiva NIS 1 (direttiva 2016/1148)

è stata la prima legislazione globale dell'UE volta a rafforzare la cibersicurezza delle reti e dei sistemi informativi per salvaguardare servizi vitali per l'economia e la società dell'UE. Nel dicembre 2020 la Commissione ha proposto la revisione della NIS 1, che ha portato all'adozione della NIS 2, entrata in vigore nel gennaio 2023. Gli Stati membri avevano tempo fino al 17 ottobre 2024 per recepire la direttiva NIS2 nel diritto nazionale. NIS 2 ha abrogato NIS1 a decorrere dal 18 ottobre 2024.