tinexta
defence

Direttiva NIS2: aggiornamenti e implicazioni per le organizzazioni italiane

#TinextaDefenceBusiness

Introduzione

La Direttiva NIS2 entra in una fase cruciale di attuazione e le organizzazioni italiane sono chiamate a un adeguamento consapevole e tempestivo.

In questo documento del team **GRC Cyber** proponiamo una lettura chiara e aggiornata del quadro europeo sul tema della sicurezza informatica, offrendo strategie di conformità e risorse operative per supportare le organizzazioni.

Autori: Giorgia Lorusso
Sostituto Punto di Contatto NIS2 Tinexta Defence

tinexta defence

1. Pubblicato il primo EU Cybersecurity Index 2024

L’Agenzia dell’Unione Europea per la Cybersecurity (ENISA) ha rilasciato il primo indice comparativo sulle capacità di sicurezza informatica dei 27 Stati membri e l’Italia si distingue positivamente, collocandosi al di sopra della media europea pari ad un punteggio di 62,65 su 100. Il nostro Paese mostra una particolare solidità nella resilienza delle infrastrutture critiche, nella cooperazione internazionale e nella lotta al crimine informatico.

Restano tuttavia margini di miglioramento, soprattutto nell’adozione di tecnologie emergenti come l’intelligenza artificiale.

2. Proroga al 31 luglio 2025 per l’aggiornamento dei dati e prossime scadenze

L’Agenzia per la Cybersicurezza Nazionale ha prorogato al 31 luglio 2025 il termine per l’aggiornamento annuale dei dati da parte dei soggetti NIS, inizialmente previsto per la fine di maggio.

La proroga offre alle organizzazioni un maggior margine operativo per adempiere a un obbligo che implica responsabilità dirette per gli organi apicali.

Prossime scadenze previste dalla Direttiva NIS2:

- A partire dal 1° gennaio 2026 sarà attivo l’obbligo di notifica degli incidenti significativi di base;

- Entro il 30 settembre 2026, dovrà essere completata l’implementazione delle misure di sicurezza di base.

3. Pubblicata la Guida Tecnica ENISA per l’implementazione della NIS2

Il **26 giugno 2025**, l’Agenzia dell’Unione Europea per la Cybersecurity ha pubblicato una guida operativa per supportare le organizzazioni nell’implementazione della Direttiva NIS2.

Il documento fornisce indicazioni concrete sulla traduzione dei requisiti normativi in misure tecniche, con riferimento al Regolamento di Implementazione della Commissione numero 2024/2690 del 17 ottobre 2024. Sono inclusi esempi di evidenze documentali per la dimostrazione di conformità e mappature dei requisiti di sicurezza applicabili alle diverse categorie di soggetti.

4. Intensificata l’azione contro i ritardi nella trasposizione della Direttiva

Il **7 maggio 2025**, la Commissione Europea ha inviato una serie di pareri motivati a **19 Stati membri** per non aver comunicato la trasposizione completa della Direttiva NIS2.

Tra i Paesi coinvolti figurano Bulgaria, Repubblica Ceca, Danimarca, Germania, Estonia, Irlanda, Spagna, Francia, Cipro, Lettonia, Lussemburgo, Ungheria, Paesi Bassi, Austria, Polonia, Portogallo, Slovenia, Finlandia e Svezia, ai quali la Commissione ha concesso due mesi per rispondere ai pareri motivati, con la possibilità di denuncia alla Corte di Giustizia UE in caso di inadempienza persistente.

Conclusioni

Il consolidamento del quadro normativo europeo in materia di cybersecurity impone alle organizzazioni un impegno strutturato nell'adeguamento alla Direttiva NIS2. La posizione dell'Italia, positiva ma ancora migliorabile, evidenzia l'urgenza di investimenti nelle tecnologie emergenti per rafforzare la sua competitività.

La proroga delle scadenze e la disponibilità di strumenti tecnici (come la guida ENISA) rappresentano occasioni concrete per rafforzare i processi interni di compliance.

Allo stesso tempo, l'inasprimento delle azioni di enforcement da parte della Commissione Europea richiama la necessità di adottare un approccio proattivo a livello comunitario, diminuendo i rischi collegati ai ritardi nell'implementazione.