PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5905 di Lunedì 25 agosto 2025

Sicurezza informatica: guida all'implementazione tecnica NIS2

Disponibile la guida tecnica di ENISA per supportare aziende e autorità nell'attuazione della Direttiva NIS2, definendo requisiti di cybersicurezza, best practice e competenze necessarie per proteggere infrastrutture critiche e servizi digitali nell'UE.

La sicurezza informatica è divenuta un aspetto cruciale per la tutela delle infrastrutture critiche e la continuità operativa delle organizzazioni a livello globale. All'interno dell'Unione Europea, questo tema ha assunto una rilevanza crescente, portando all'adozione di normative e direttive volte a innalzare gli standard di sicurezza informatica tra gli Stati membri. Tra queste, la Direttiva NIS2, aggiornata rispetto alla precedente NIS, si pone come un nuovo standard che amplia la portata e rafforza gli obblighi in materia di cybersecurity. In tale contesto, il documento intitolato "NIS2 Technical Implementation Guidance" pubblicato dall'Agenzia dell'Unione Europea per la Cybersicurezza (ENISA) rappresenta uno strumento fondamentale per la traduzione tecnica di tali requisiti normativi.

L'obiettivo principale di questo documento è fornire indicazioni tecniche concrete e operative alle entità soggette alla Direttiva NIS2, così da facilitare e rendere più efficace il processo di implementazione delle misure di sicurezza previste dalla normativa. Questo è particolarmente importante considerando la complessità delle infrastrutture digitali, la molteplicità di settori coinvolti e la necessità di un approccio coordinato e coerente tra i diversi Paesi membri. La guida di ENISA si configura quindi come un supporto pratico volto a tradurre in azioni precise e verificabili quanto previsto dalla Direttiva e dai regolamenti correlati.

Il documento nasce dalla collaborazione stretta tra ENISA, il Gruppo di Cooperazione NIS e la Commissione Europea. Inoltre, è stato oggetto di una consultazione pubblica aperta al settore privato e ad altri stakeholder, garantendo così una pluralità di prospettive e un'applicabilità più ampia alle realtà operative. Questo approccio partecipativo ha permesso di raccogliere feedback e di affinare le indicazioni tecniche, rendendo la guida un riferimento aggiornato e ben strutturato.

La Direttiva NIS2, adottata nel 2022 con il Regolamento (UE) 2022/2555, amplia la gamma di settori considerati critici includendo infrastrutture digitali, energia, trasporti, salute e altri ambiti essenziali per la sicurezza e il benessere della società. Inoltre, introduce requisiti più stringenti per la gestione dei rischi di cybersecurity e per la risposta agli incidenti, con l'obiettivo di innalzare il livello di resilienza complessiva delle reti e dei sistemi informativi nell'Unione. La trasposizione di questi requisiti nei diversi ordinamenti nazionali e la loro attuazione pratica rappresentano una sfida significativa per molte organizzazioni.

A tale proposito, il Regolamento di Esecuzione (UE) 2024/2690, emanato dalla Commissione Europea nell'ottobre 2024, fornisce dettagli aggiuntivi e specifici requisiti per i settori delle infrastrutture digitali e dei servizi ICT gestiti. Questi regolamenti si propongono di armonizzare a livello europeo le modalità di attuazione e di controllo, garantendo un quadro normativo coerente e omogeneo. La guida tecnica di ENISA si inserisce in questo contesto fornendo esempi pratici, modelli di prova e una mappatura dei requisiti di sicurezza che facilitano l'adozione e la verifica delle misure prescritte.

Tra i contenuti principali del documento, particolare attenzione viene data alla gestione del rischio di cybersecurity, un processo continuo che deve coinvolgere tutte le componenti organizzative e tecniche dell'entità. La guida suggerisce come identificare, valutare e mitigare i rischi in modo efficace, sottolineando l'importanza di politiche di sicurezza ben definite e di un costante monitoraggio delle vulnerabilità. Vengono inoltre approfondite le modalità di gestione degli incidenti informatici, dalla loro rilevazione fino alla risposta e al recupero, al fine di minimizzare l'impatto e di garantire la continuità operativa.

Il documento affronta anche temi fondamentali quali la sicurezza della catena di approvvigionamento, riconosciuta come un elemento critico nella protezione delle infrastrutture digitali. La complessità e la globalizzazione delle catene di fornitura rendono necessario un controllo accurato dei fornitori e dei partner, affinché non diventino un vettore di rischio. La guida propone pertanto linee guida per la valutazione e la gestione di tali rischi, stimolando l'adozione di misure di controllo e di monitoraggio appropriate.

Un altro aspetto rilevante riguarda la sicurezza nello sviluppo, nell'acquisizione e nella manutenzione dei sistemi informativi e delle reti. Il documento suggerisce l'adozione di pratiche di sicurezza integrate nei processi di sviluppo del software e nella gestione delle infrastrutture, come parte integrante della strategia di cybersecurity. Viene inoltre enfatizzata l'importanza di formazione continua e di campagne di sensibilizzazione rivolte al personale, affinché siano adeguatamente preparati a riconoscere e gestire le minacce.

Per quanto riguarda la compliance e la verifica, la guida tecnica di ENISA propone metodi e strumenti per valutare l'efficacia delle misure di sicurezza implementate. Questa attività è fondamentale per garantire un miglioramento continuo e per fornire evidenze concrete agli organismi di vigilanza nazionali e alle autorità competenti. L'adozione di metriche, indicatori e audit regolari costituisce un elemento chiave per il mantenimento di elevati standard di sicurezza.

Il documento non ha natura vincolante, e non sostituisce i quadri regolatori o le linee guida nazionali. Le organizzazioni soggette alla Direttiva NIS2 sono quindi invitate a interfacciarsi con le autorità nazionali di riferimento per comprendere appieno i propri obblighi specifici e per adattare le indicazioni generali della guida al proprio contesto operativo. Tuttavia, la guida rappresenta un utile punto di riferimento per allineare le proprie pratiche agli standard europei e per migliorare la propria postura di sicurezza.

A complemento delle indicazioni tecniche, ENISA ha sviluppato il Quadro Europeo delle Competenze in Cybersicurezza (ECSF), che mira a definire e valutare le competenze professionali nel settore. In relazione alla NIS2, la stessa agenzia ha prodotto un documento di orientamento dedicato ai ruoli e alle competenze necessarie per l'attuazione efficace delle misure di sicurezza. Questa mappatura tra obblighi normativi e profili professionali consente alle organizzazioni di strutturare meglio il proprio capitale umano e di indirizzare formazione e sviluppo secondo le esigenze specifiche dettate dalla direttiva.

ENISA ? Technical Implementation Guidance - Guida all'implementazione tecnica NIS2.

On Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures.

Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS2)

Regolamento Di Esecuzione (UE) 2024/2690 Della Commissione del 17 ottobre 2024 - recante modalità di applicazione della direttiva (UE) 2022/2555 per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza e l'ulteriore specificazione dei casi in cui un incidente è considerato significativo per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network e i prestatori di servizi fiduciari.

RFG

www.puntosicuro.it