LEVIAhub
SUPPLY CHAIN MASTER

NIS2: come adempiere alla Direttiva per evitare sanzioni grazie alle soluzioni Leviahub

I servizi di Cyber Security per prevenire gli attacchi informatici

A dicembre 2022 il Consiglio dell'Unione Europea e il Parlamento Europeo hanno adottato la **Direttiva Network and Information Security Directive (NIS2)**, o Direttiva 2022/2555, sulla sicurezza delle reti e dei sistemi informativi, con l'obiettivo di potenziare i sistemi di sicurezza per far fronte agli attacchi informatici sempre più frequenti e prevedere nuovi requisiti di **Cyber Security** più ampi per tutti gli Stati membri dell'UE. In Italia la Direttiva è stata recepita il **1° ottobre 2024** tramite il Decreto Legislativo n. 138/2024 e sarà pienamente operativa dal **1° gennaio 2026**. **Leviahub**, sempre attenta a garantire la massima sicurezza delle sue soluzioni, ha già lavorato per aderire al meglio alle nuove linee guida, ed è pronta ad accompagnare le aziende nell'adempimento alla NIS2 verso un business privo di rischi.

In un mondo in cui le **minacce digitali** sono in costante evoluzione **prevenzione**, **monitoraggio** e **ripristino** sono i tre concetti chiave per conformarsi alle normative e rimanere competitivi, e Leviahub è pronta a mettere in campo le più sofisticate soluzioni nonché un Team di esperti in **Cyber Security** pronto ad affiancare le aziende per proteggerle da rischi e attacchi indesiderati.

Tre i pilasti fondanti della nuova Direttiva NIS2: la richiesta ai soggetti responsabili di mettere in atto azioni adeguate e proporzionate in ambito **tecnico**, **operativo** e **organizzativo**, per prevenire e gestire i rischi, nonché limitare l'impatto di eventuali incidenti sui destinatari dei servizi e su altri servizi; la garanzia di **business continuity** anche in caso di gravi danni all'infrastruttura tecnologica, in modo da eliminare eventuali interruzioni del flusso lavorativo e perdita di dati essenziali; e la creazione di una rete di **cooperazione a livello europeo** per favorire lo scambio di informazioni tra gli Stati Membri e permettere la condivisione di best practices e una **risposta coordinata** agli incidenti Cyber a livello transnazionale. La NIS2, inoltre, amplia i settori coinvolti (che passano da 6 a 18) e richiede una maggiore attenzione alle **vulnerabilità** legate ai fornitori di terze parti: in questo modo viene coinvolta l'intera catena della **Supply Chain**.

Vengono infine inasprite le **sanzioni** per la non adesione alla Direttiva, che possono riguardare la mancata gestione dei rischi, l'inadempienza sugli obblighi di notifica degli incidenti o la non registrazione presso le autorità competenti. Ciò può comportante pesanti **danni** alle aziende, sia dal punto di vista di un'eventuale interruzione dell'attività, che per un danno alla brand reputation. Leviahub è il partner di fiducia pronto a **tutelare** le aziende dalle sanzioni della NIS2: l'esperienza degli esperti di Leviahub consente, infatti, di intervenire con precisione, offrendo **soluzioni su misura** che preservano la stabilità dei sistemi e riducono al minimo i rischi di interruzioni, garantendo che ogni azione contribuisca al rafforzamento della resilienza aziendale.

Penetration test, **Vulnerability Assessment**, **Cyber Threat Intelligence**, **Risk Assessment**, **Security Awareness**, **Brand Reputation**: sono solo alcune delle soluzioni per la Cyber Security che Leviahub è pronta a mettere in campo per prevenire gli attacchi informatici e ridurne l'impatto in modo da proteggere sistemi informatici, applicazioni, dispositivi, dati, risorse (anche finanziarie) e utenti da ransomware e altri malware, truffe di phishing, furti e manipolazioni di dati, e altre minacce informatiche.

Per maggiori informazioni sulle soluzioni di Cyber Security e su come adempiere al meglio alla nuova Direttiva NIS2 è possibile consultare il sito **leviahub.com** o a scrivere a press@leviahub.com.