Gpi Phishing
AI POWERED PROTECTION

CYBERSECURITY & COMPLIANCE

NIS2: la conformità non si ottiene nominando un CISO

La direttiva europea trasforma l'intera struttura organizzativa in un sistema di responsabilità condivisa. Ecco perché non basta introdurre nuovi ruoli tecnici.

A cura di Rosario Mauro Catanzaro

10 aprile 2026 www.gpiphishing.com

CONFORMITÀ NIS2 — D.LGS. 138/2024

C'è una convinzione diffusa, e pericolosamente semplicistica, che circola ancora oggi nei Consigli di Amministrazione di molte organizzazioni: per essere conformi alla NIS2 è sufficiente nominare un CISO, formalizzare qualche procedura e attendere che la macchina si metta in moto da sola. Chi ragiona in questi termini sta commettendo un errore strategico che potrebbe costare caro, sia in termini di sanzioni che di vulnerabilità reale.

La direttiva NIS2, entrata in vigore nell'ottobre 2024 e recepita in Italia con il D.Lgs. 138/2024, non si limita ad ampliare il perimetro dei soggetti obbligati. Ridefinisce in profondità il modo in cui la sicurezza informatica deve essere concepita all'interno di un'organizzazione: non come una funzione verticale e isolata, ma come una responsabilità distribuita, radicata in ogni livello della struttura aziendale.

01 Nuovi ruoli: necessari, ma non sufficienti

La NIS2 introduce figure specifiche che le organizzazioni sono tenute a designare formalmente. Ciascuna ha un perimetro d'azione preciso e non intercambiabile.

RUOLO

CISO

Supervisiona la strategia di sicurezza complessiva e coordina la gestione del rischio cyber a livello di organizzazione.

RUOLO

Punto di Contatto NIS

Rappresenta l'interfaccia ufficiale verso l'Autorità Nazionale Competente, garantendo il flusso informativo con le istituzioni.

RUOLO

Referente CSIRT

Gestisce operativamente gli incidenti e coordina le notifiche obbligatorie nei tempi previsti dalla normativa (24/72 ore).

RUOLO

Incident Response Team

Squadra dedicata alla risposta tecnica agli incidenti, attiva per garantire interventi tempestivi e contenimento del danno.

Questi ruoli sono essenziali e la loro assenza espone l'organizzazione a responsabilità dirette. Ma da soli non bastano. La vera architettura della conformità si costruisce integrando la sicurezza nei processi che già esistono, coinvolgendo reparti che tradizionalmente non si sono mai occupati di cybersecurity.

A cura di Rosario Mauro Catanzaro

02 La sfida reale: far evolvere chi è già in azienda

La NIS2 impone un cambio di paradigma che investe funzioni apparentemente lontane dal perimetro IT. Ogni reparto diventa un presidio di sicurezza.

GOVERNANCE

Organo Direttivo (CDA)

Approva la strategia di sicurezza, stanzia il budget e partecipa attivamente alla formazione. La NIS2 prevede responsabilità personali per i vertici.

SUPPLY CHAIN

Procurement & Acquisti

Deve integrare clausole di sicurezza informatica nei contratti con i fornitori e valutare il rischio della catena di approvvigionamento.

CULTURA

Risorse Umane

Sviluppa programmi di formazione continua e gestisce le procedure di accesso, fondamentali per ridurre il rischio insider.

REGOLATORIO

Legale & Compliance

Presidia le policy interne e gestisce le implicazioni legali di violazioni, sanzioni amministrative e notifiche agli interessati.

REPUTAZIONE

Comunicazione

In caso di incidente, la gestione della comunicazione esterna è determinante per preservare la fiducia di clienti e stakeholder.

VERIFICA

Internal Audit & IT

L'Audit verifica l'efficacia delle misure adottate; l'IT evolve da funzione tecnica a partner strategico abilitante della resilienza.

> *La NIS2 non introduce solo nuovi ruoli: trasforma l'intera organizzazione in un sistema di responsabilità condivisa, in cui ogni funzione aziendale è chiamata a presidiare il proprio perimetro di rischio.*

03 Come agire concretamente

Il punto di partenza è una gap analysis che non riguardi solo l'infrastruttura tecnologica, ma mappi le responsabilità di sicurezza lungo tutta la struttura organizzativa. Da lì è possibile costruire un piano di adeguamento che integri governance, processi e competenze, senza lasciare isolato il CISO a gestire da solo un problema che è, per definizione, collettivo.

Le organizzazioni che coglieranno questa opportunità per ripensare la propria cultura della sicurezza non si limiteranno a essere conformi: saranno più resilienti, più affidabili per i loro clienti e più competitive in un mercato che considera la cybersecurity un fattore abilitante, non un costo da minimizzare.

A cura di Rosario Mauro Catanzaro

GPI PHISHING — CYBERSECURITY PLATFORM

Costruisci una cultura della sicurezza conforme alla NIS2

Individuazione del phishing, simulazioni reali, formazione continua
e misurazioni concrete del rischio, tutto in un'unica piattaforma enterprise.

Phishing
AI POWERED PROTECTION

www.gpiphishing.com