



Cybersicurezza, Petricca su direttiva NIS2: «Per ad responsabili di incidenti obbligo di formazione»•

Descrizione

(Adnkronos) «Le aziende italiane si trovano di fronte a una rivoluzione normativa che sta ridefinendo completamente il concetto di responsabilità in materia di cybersecurity. Con l'entrata in vigore della direttiva NIS2, migliaia di imprese scoprono che i loro amministratori delegati, sindaci e vertici aziendali sono ora personalmente e direttamente responsabili degli incidenti informatici, con l'obbligo tassativo di notificare qualsiasi violazione entro 72 ore alle autorità competenti. Secondo i dati più recenti, nel 2023 l'Italia ha investito 29,4 miliardi di euro in ricerca e sviluppo, registrando un incremento del 7,7% rispetto all'anno precedente, mentre per il 2025 si è verificato un boom nelle certificazioni di credito d'imposta con 6577 progetti registrati. Tuttavia, questo scenario di innovazione tecnologica si scontra con una realtà preoccupante: la maggior parte delle organizzazioni non è ancora strutturata per gestire gli incidenti cyber nei tempi imposti dalla nuova normativa.

«Con l'introduzione della NIS2», spiega Riccardo Petricca, ingegnere e certificatore accreditato Mimit, «la cybersecurity diventa governance: gli organi apicali devono approvare, sovraintendere e rispondere delle violazioni, non possono più semplicemente delegare come accadeva fino a qualche anno fa. Oggi un incidente cyber rappresenta un rischio operativo, economico e legale con impatti sui cittadini, sulla continuità operativa, e la finestra di notifica di 24-72 ore impone decisioni immediate con responsabilità e risorse che fanno capo direttamente a sindaci, giunte e amministratori delegati»•.

La normativa prevede sanzioni particolarmente severe: «Ci sono responsabilità dirette, quindi civili e penali. Non esiste più il «non lo sapevo» oppure «avevo delegato». È un obbligo scritto e sancito dalla NIS2 con sanzioni veramente pesanti», avverte Petricca. La legge impone espressamente che i vertici seguano una formazione specifica e la promuovano nell'organizzazione, mentre l'amministratore delegato deve essere pienamente consapevole dei rischi concreti. Il problema più grave emerge dall'approccio ancora troppo superficiale delle aziende verso questa trasformazione. «L'errore più grave», sottolinea, «è sottovalutare un inventario serio e corretto, una classificazione del ruolo e del rischio, trattando la cybersecurity come un tema esclusivamente legale o solo IT. Molte aziende non distinguono bene se sono provider o deployer, ruoli fondamentali che cambiano gli obblighi e le responsabilità, e non impostano per tempo evidenze, controlli del ciclo di vita, documentazione, tracciabilità e monitoraggio degli incidenti»•.

La situazione diventa ancora più¹ critica considerando l'effetto domino che un attacco informatico può² generare. Come evidenzia Petricca: «Il paradigma fondamentale è che il fermo di un'azienda ha risvolti economici enormi perché fermi macchine, servizi, persone, con perdite economiche e reputazionali. Ma soprattutto può² bloccare chi sta a monte e a valle della filiera». Settori vitali come energia, telecomunicazioni, sanità e alimentare rischiano di paralizzare intere catene produttive, con conseguenze che si estendono ben oltre i confini aziendali.

La prevenzione diventa quindi l'unica strategia vincente. «Bisogna implementare» suggerisce «misure minime: ruoli e deleghe formalizzate, incident commander, compliance, comunicazione IT security con reperibilità, piano di gestione degli incidenti con criteri già definiti, flussi di raccolta evidenze, canali di escalation, esercitazioni, formazione e presidio della supply chain». Come membro della catena, devo accertarmi che anche i miei fornitori stiano seguendo queste best practice».

L'impatto della NIS2 va oltre la semplice compliance normativa, trasformandosi in un fattore competitivo decisivo. Le aziende che sapranno adeguarsi tempestivamente non solo eviteranno sanzioni milionarie, ma costruiranno un vantaggio strategico basato sulla fiducia e sulla continuità operativa. Al contrario, quelle che continueranno a sottovalutare la portata di questa rivoluzione normativa rischiano di trovarsi escluse da mercati sempre più attenti alla sicurezza informatica e alla gestione responsabile dei dati. La strada verso la compliance NIS2 richiede un cambio di paradigma culturale: dalla cybersecurity vista come costo tecnico alla cybersecurity come investimento strategico, dalla delega alla responsabilità diretta, dalla reazione alla prevenzione. Solo così le imprese italiane potranno trasformare quello che oggi appare come un obbligo normativo in un'opportunità di crescita sostenibile e sicura.

»

economia

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione

Maggio 12, 2026

Autore

redazione