Cybersicurezza, Petricca su direttiva NIS2: â??Per ad responsabili di incidenti obbligo di formazioneâ?•

Descrizione

(Adnkronos) â?? Le aziende italiane si trovano di fronte a una rivoluzione normativa che sta ridefinendo completamente il concetto di responsabilitÃ in materia di cybersecurity. Con lâ??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 lâ??obbligo tassativo di notificare qualsiasi violazione entro 72 ore alle autoritÃ competenti. Secondo i dati piÃ¹ recenti, nel 2023 lâ??Italia ha investito 29,4 miliardi di euro in ricerca e sviluppo, registrando un incremento del 7,7% rispetto allâ??anno precedente, mentre per il 2025 si Ã¨ verificato un boom nelle certificazioni di credito dâ??imposta con 6577 progetti registrati. Tuttavia, questo scenario di innovazione tecnologica si scontra con una realtÃ preoccupante: la maggior parte delle organizzazioni non Ã¨ ancora strutturata per gestire gli incidenti cyber nei tempi imposti dalla nuova normativa.

â??Con lâ??introduzione della NIS2 â?? spiega Riccardo Petricca, ingegnere e certificatore accreditato Mimit â?? la cybersecurity diventa governance: gli organi apicali devono approvare, sovraintendere e rispondere delle violazioni, non possono piÃ¹ 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 continuitÃ operativa, e la finestra di notifica di 24-72 ore impone decisioni immediate con responsabilitÃ e risorse che fanno capo direttamente a sindaci, giunte e amministratori delegatiâ?•.

La normativa prevede sanzioni particolarmente severe: â??Ci sono responsabilitÃ dirette, quindi civili e penali. Non esiste piÃ¹ il â??non lo sapevoâ?? oppure â??avevo delegatoâ??. Eâ?? un obbligo scritto e sancito dalla NIS2 con sanzioni veramente pesantiâ?•, avverte Petricca. La legge impone espressamente che i vertici seguano una formazione specifica e la promuovano nellâ??organizzazione, mentre lâ??amministratore delegato deve essere pienamente consapevole dei rischi concreti. Il problema piÃ¹ grave emerge dallâ??approccio ancora troppo superficiale delle aziende verso questa trasformazione. â??Lâ??errore piÃ¹ grave â?? sottolinea â?? Ã¨ 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 responsabilitÃ , e non impostano per tempo evidenze, controlli del ciclo di vita, documentazione, tracciabilitÃ e monitoraggio degli incidentiâ?•.

La situazione diventa ancora piÃ¹ critica considerando lâ??effetto domino che un attacco informatico puÃ² generare. Come evidenzia Petricca: â??Il paradigma fondamentale Ã¨ che il fermo di unâ??azienda ha risvolti economici enormi perchÃ© fermi macchine, servizi, persone, con perdite economiche e reputazionali. Ma soprattutto puÃ² bloccare chi sta a monte e a valle della filieraâ?•. Settori vitali come energia,telecomunicazioni, sanitÃ e alimentare rischiano di paralizzare intere catene produttive, con conseguenze che si estendono ben oltre i confini aziendali.

La prevenzione diventa quindi lâ??unica strategia vincente. â??Bisogna implementare â?? suggerisce â?? misure minime: ruoli e deleghe formalizzate, incident commander, compliance, comunicazione IT security con reperibilitÃ , piano di gestione degli incidenti con criteri giÃ definiti, flussi di raccolta evidenze, canali di escalation, esercitazioni, formazione e presidio della supply chainâ??. Come membro della catena, devo accertarmi che anche i miei fornitori stiano seguendo queste best practiceâ?•.

Lâ??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 continuitÃ operativa. Al contrario, quelle che continueranno a sottovalutare la portata di questa rivoluzione normativa rischiano di trovarsi escluse da mercati sempre piÃ¹ 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 responsabilitÃ diretta, dalla reazione alla prevenzione. Solo cosÃ¬ le imprese italiane potranno trasformare quello che oggi appare come un obbligo normativo in unâ??opportunitÃ di crescita sostenibile e sicura.

â??

economia

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione
Maggio 12, 2026
Autore
redazione