Il Sole 24 ORE Lombardia
Settimanale

Cybersicurezza, il 78% delle Pmi adotta strategie di protezione

Il report. Un'indagine del Digital Innovation Hub Lombardia insieme a Confindustria rileva il grado di conoscenza e adeguamento delle imprese alla direttiva NIS 2. Complessità e costi i fattori più critici

Giovanna Mancini

L'aumento degli attacchi informatici alle aziende pubbliche e private del nostro Paese non è una percezione, ma un fenomeno certificato dai dati del Rapporto Clusit pubblicato in ottobre, secondo cui il 2024 è stato, a livello globale, il peggior anno di sempre in termini di cybersecurity. E l'Italia non solo non fa eccezione, ma anzi, rappresenta secondo gli esperti che hanno redatto il rapporto un «bersaglio preferenziale». Se a livello globale gli attacchi sono aumentati del 27,4% rispetto al 2023 (arrivando a quota 3.451), nel nostro Paese questi eventi sono cresciuti del 15%: un dato migliore rispetto alla media mondiale, ma comunque allarmante, considerando che l'Italia, «pur rappresentando solo lo 0,7% della popolazione e l'1,8% del Pil mondiale, nel 2024 ha subito il 10% degli attacchi registrati a livello globale», mentre la Francia, ad esempio, è al 4% e la Germania al 3%, così come il Regno Unito.

Un triste primato che sottende, probabilmente, una minor tenuta del sistema o una scarsa preparazione da parte delle imprese. La Lombardia risulta, in questo quadro, particolarmente interessata al fenomeno e non tanto per una questione territoriale, quanto per ragioni intrinseche al suo tessuto imprenditoriale, che concentra numerose realtà specializzate in ambito digitale o connesse a soggetti regolamentati.

La buona notizia è che la maggior parte delle imprese lombarde è consapevole del problema e si sta attrezzando per porre rimedi, come emerge da un'indagine qualitativa sul tema della Cybersecurity realizzata da Digital Innovation Hub (DIH) Lombardia, in collaborazione con Confindustria Lombardia, interrogando le nove associazioni territoriali. Quasi l'80% delle aziende è infatti a conoscenza della Direttiva NIS 2 dell'Unione europea, che introduce requisiti più stringenti in materia di gestione del rischio, segnalazione degli incidenti e governance della sicurezza informatica per un numero maggiore di soggetti, inclusi gli operatori delle filiere industriali, dei servizi essenziali e delle infrastrutture digitali. «Il recepimento nazionale della direttiva ha un impatto significativo anche sulle piccole e medie imprese che operano come fornitori o partner di soggetti regolamentati, chiamate a innalzare i propri standard di sicurezza per mantenere la competitività e l'affidabilità all'interno delle catene del valore», si legge nel rapporto.

Elevata è anche la percentuale di imprese lombarde, tra quelle che rientrano nell'ambito di applicazione della NIS 2, che si sta adeguando alla nuova normativa (il 78%). Rimane tuttavia un 22% di aziende che non si sta attrezzando per adeguarsi.

Tra le misure adottate con maggiore frequenza da queste aziende per proteggersi dai cyberattacchi, l'indagine segnala l'uso di sistemi antivirus e firewall, l'autenticazione a due o più fattori, i backup periodici anche su cloud, sistemi di monitoraggio e rilevamento intrusioni. Per supportare e accelerare l'adeguamento delle imprese lombarde alla NIS 2, l'indagine del Digital Innovation Hub indica un maggiore coordinamento e condivisione tra le iniziative a livello territoriale, una comunicazione più chiara e mirata, incentivi e sostegni economici per le Pmi che investono in cybersecurity.

«Come emerge dalle cronache quotidiane si moltiplicano e si fanno più sofisticati gli attacchi hacker contro infrastrutture digitali, banche dati e segreti aziendali – osserva la segretaria generale di Confindustria Lombardia, Alina Candu –. Per le nostre aziende proteggersi da attacchi deve diventare una priorità al pari della sicurezza del personale». Due gli strumenti a disposizione delle imprese, spiega Candu: «la sensibilizzazione culturale e la formazione di tutto il personale, perché anche chi non è direttamente coinvolto in processi industriali digitalizzati può diventare la porta di accesso di malintenzionati e mettere a repentaglio la sicurezza aziendale. È poi necessario che associazioni imprenditoriali e istituzioni regionali collaborino per supportare e aggiornare costantemente le aziende su rischi e contromisure, con l'obiettivo di proteggere le infrastrutture critiche aziendali e di filiera in quella che è ormai diventata una priorità strategica per la competitività del sistema produttivo».

Il Sole 24 ORE Lombardia
Settimanale

I numeri

2024

L'anno nero
L'aumento degli attacchi informatici alle aziende pubbliche e private del nostro Paese non è una percezione, ma un fenomeno certificato dai dati del Rapporto Clusit pubblicato in ottobre, secondo cui il 2024 è stato, a livello globale, il peggior anno di sempre in termini di cybersecurity

10%

Gli attacchi subiti
Se a livello globale gli attacchi sono aumentati del 27,4% rispetto al 2023 (arrivando a quota 3.451), nel nostro Paese questi eventi sono cresciuti del 15%: un dato migliore rispetto alla media mondiale, ma comunque allarmante, considerando che l'Italia ha subito il 10% degli attacchi registrati a livello globale

80%

Le aziende informate
Quasi l'80% delle aziende è a conoscenza della Direttiva NIS 2 dell'Unione europea, che introduce requisiti più stringenti in materia di gestione del rischio, segnalazione degli incidenti e governance della sicurezza informatica per un numero maggiore di soggetti, inclusi gli operatori delle filiere industriali

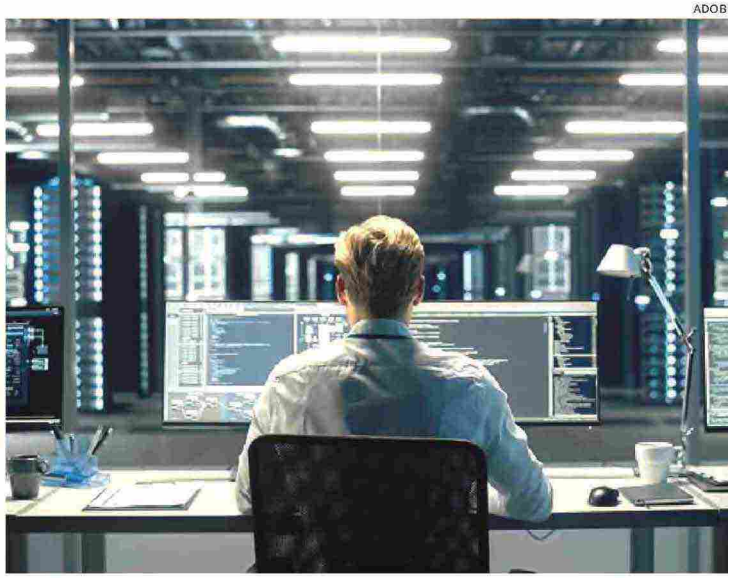
3%

Violazioni in Germania
L'Italia pur rappresentando solo lo 0,7% della popolazione e l'1,8% del Pil mondiale, nel 2024 ha subito il 10% degli attacchi registrati a livello globale. La cifra è molto alta soprattutto se rapportata a quanto accaduto in Francia (4% degli attacchi globali) e in Germania così come il Regno Unito (3%)

2023

LA DIRETTIVA EUROPEA
La Direttiva NIS 2 (Network and Information Security Directive 2) è la nuova normativa europea sulla cybersecurity, emanata per rafforzare la sicurezza delle reti e dei sistemi informativi nella Ue, entrata in vigore nel gennaio 2023. In Italia il decreto di recepimento è già stato approvato, ma la piena applicazione è in corso.

ADOB



Affidabilità.
Le Pmi devono innalzare i propri standard di sicurezza per mantenere l'affidabilità all'interno delle catene del valore


Cybersicurezza, il 78% delle Pmi adotta strategie di protezione