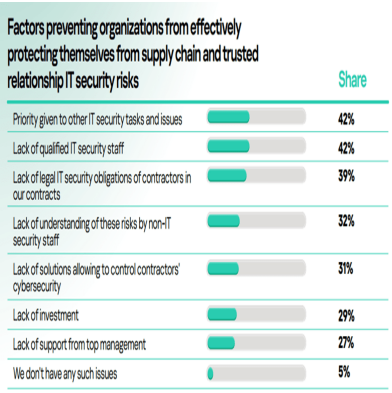

La carenza di esperti in cybersecurity ostacola la riduzione dei rischi nella supply chain

Descrizione

default watermark

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Un nuovo studio globale condotto da Kaspersky evidenzia la carenza di personale qualificato nel settore della sicurezza informatica e la necessitÃ , per le aziende internazionali, di dare prioritÃ a diverse attivitÃ di sicurezza per mitigare i rischi legati alla supply chain e alle relazioni di fiducia. Entrambi questi fattori sono stati indicati da quasi la metÃ degli intervistati (42%).

Lo studio di Kaspersky[1] sui rischi legati alla supply chain e alle relazioni di fiducia ha evidenziato che gli attacchi alla supply chain sono diventati una delle principali minacce per le aziende: unâ??azienda su tre ha subito un attacco di questo tipo nellâ??ultimo anno. La gravitÃ e la frequenza di tali episodi rendono fondamentale individuare le cause che impediscono alle imprese di gestire efficacemente questi rischi.

Secondo lâ??indagine, uno degli ostacoli principali Ã¨ proprio la carenza di personale qualificato, che limita la capacitÃ delle organizzazioni di monitorare in modo sistematico le vulnerabilitÃ dei soggetti terzi allâ??interno dei propri ecosistemi. Il bisogno di professionisti in grado di affrontare queste sfide Ã¨ particolarmente elevato in Vietnam, negli Emirati Arabi Uniti, in Messico e in Spagna.

Tra le altre criticitÃ emerge la difficoltÃ di gestire contemporaneamente molteplici prioritÃ di cybersecurity, un aspetto particolarmente sentito in India, Vietnam, Singapore ed Egitto. Questo riflette il sovraccarico dei team di sicurezza, spesso impegnati su troppe attivitÃ , con il rischio che le minacce alla supply chain non ricevano la necessaria attenzione.

Oltre alla carenza di risorse, gli intervistati segnalano anche problematiche strutturali: il 39% dichiara che i contratti non includono obblighi chiari in materia di sicurezza informatica per gli appaltatori, con

lacune particolarmente evidenti in Vietnam, Turchia, Spagna e Messico. Inoltre, il 32% rileva che il personale non specializzato in cybersecurity non comprende pienamente tali rischi.

A livello globale, lâ??85% delle aziende ammette la necessitÃ di rafforzare la protezione contro i rischi legati alla supply chain e alle relazioni di fiducia, mentre solo il 15% considera efficaci le misure di sicurezza attualmente adottate. Questo livello di fiducia scende ulteriormente in economie chiave come Germania (6%), Turchia (7%), Italia (8%), Brasile (8%), Russia (8%) e Arabia Saudita (9%).

Allo stesso tempo, le pratiche di mitigazione dei rischi legati a terzi risultano ancora frammentarie: nessuna misura di protezione supera il 40% di diffusione tra gli utilizzatori. Anche lâ??autenticazione a due fattori, la piÃ¹ adottata, Ã¨ utilizzata solo dal 38% degli intervistati.

Inoltre, appena il 35% delle aziende effettua controlli periodici sul livello di sicurezza informatica dei propri fornitori. Di conseguenza, quasi due terzi delle organizzazioni non dispongono di una visibilitÃ costante sulla sicurezza dei partner, esponendosi a vulnerabilitÃ in continua evoluzione allâ??interno dei propri ecosistemi.

default watermark

Ã? interessante notare che le aziende giÃ colpite da attacchi alla supply chain o da violazioni delle relazioni di fiducia tendono ad adottare misure piÃ¹ rigorose. In particolare, le organizzazioni coinvolte in incidenti legati alla supply chain sono piÃ¹ propense a richiedere i risultati dei penetration test (56%), mentre quelle vittime di violazioni delle relazioni di fiducia danno prioritÃ alla verifica della conformitÃ agli standard di settore (56%) e alle policy della supply chain dei fornitori (53%).

â??Quando i team di sicurezza sono sovraccarichi, con risorse limitate e costretti a privilegiare le urgenze rispetto alla resilienza di lungo periodo, le aziende restano esposte a minacce che possono diffondersi silenziosamente lungo lâ??intero ecosistema dei fornitori. Per interrompere questo circolo vizioso, Ã¨ necessario adottare strategie di mitigazione piÃ¹ integrate e coerenti, che includano valutazioni standardizzate dei fornitori e una maggiore consapevolezza tra i diversi team. La sicurezza della supply chain deve diventare una responsabilitÃ condivisa e diffusa in tutta la rete aziendaleâ?•, ha commentato Sergey Soldatov, Head of Security Operations Center di Kaspersky.

Solo attraverso lâ??adozione di misure preventive a tutti i livelli e un approccio strategico nella gestione dei rapporti con fornitori e appaltatori, le aziende possono ridurre i rischi legati alla supply chain e garantire la resilienza del proprio business.

Per proteggersi da queste minacce, Kaspersky consiglia di:

Ulteriori raccomandazioni e altre conclusioni relative alla mitigazione dei rischi della supply chain sono disponibili al link.

[1] Ai fini del report, il centro di ricerche di mercato interno di Kaspersky ha commissionato un sondaggio che ha coinvolto 1.714 esperti tecnici, tra cui dirigenti di alto livello, vicepresidenti, responsabili di team e specialisti senior provenienti da aziende con oltre 500 dipendenti. Lo studio ha riguardato 16 paesi, tra cui Germania, Spagna, Italia, Brasile, Messico, Colombia, Singapore, Vietnam, Cina, India, Indonesia, Arabia Saudita, Turchia, Egitto, Emirati Arabi Uniti e Russia.

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

default watermark

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Marzo 18, 2026
Autore
redazione