



Kaspersky: in Italia il 25% dei responsabili aziendali non comprende il valore strategico della cybersecurity

Descrizione

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE

Milano, 3 novembre 2025

Il nuovo report di Kaspersky "Real talk on cybersecurity: cosa preoccupa, cosa manca e cosa è davvero utile" rivela che il 25% dei responsabili IT in Italia ritiene che i propri colleghi C-level non comprendano pienamente l'importanza della cybersecurity per il business, evidenziando una discrepanza strutturale tra le priorità dei vertici aziendali e la protezione delle PMI italiane. Un terzo (30%) dei decision maker responsabili della cybersecurity in Italia afferma che monitorare le potenziali minacce rappresenta un lavoro a tempo pieno, mentre il 33% dichiara di essere sommerso dagli avvisi e il 10% sostiene di dedicare più tempo alla risoluzione dei problemi legati ai software di sicurezza che alla difesa dalle minacce reali. Inoltre, il 12% segnala che le soluzioni di sicurezza rallentano i flussi di lavoro o la produzione: questi ostacoli operativi si stanno già traducendo in rischi concreti per il business.

Il quadro è chiaro: lo sforzo è elevato, ma l'impatto resta limitato. A complicare ulteriormente la situazione, alcuni decision maker nel campo della cybersecurity segnalano che le stesse soluzioni di sicurezza possono persino rallentare i processi operativi.

Le minacce sono reali, così come lo è la lotta con i C-Level

Il problema è reale, poiché le minacce mettono in evidenza le sfide ancora da affrontare. In alcuni contesti PMI europei, backdoor (24%), trojan (17%) e "not-a-virus: Downloader" (16%) risultano tra le minacce più diffuse.

Le carenze in termini di competenze e leadership aumentano l'esposizione alle minacce, evidenziando una discrepanza tra le priorità dei dirigenti e le procedure di sicurezza applicate in prima

linea. In Italia, il 25% dei responsabili IT afferma che i colleghi C-Level non comprendono appieno l'importanza della cybersecurity per l'azienda, limitando così il raggiungimento degli obiettivi e lo slancio verso il cambiamento. Il 17% segnala una carenza di specialisti qualificati, quindi la maggior parte delle PMI si affida a team IT generici (22%) o a specialisti di sicurezza informatica integrati all'interno di quest'equipe (25%). Solo il 42% delle aziende italiane dispone di un team dedicato esclusivamente alla sicurezza informatica, mentre appena il 12% si affida unicamente a partner esterni per la progettazione e la gestione della cybersecurity. Paradossalmente, il livello di soddisfazione interna risulta molto elevato: il 93% dichiara di essere soddisfatto degli esperti di sicurezza informatica interni, il 77% dei reparti IT in generale e l'80% dei team interni dedicati alla sicurezza. Questo suggerisce un divario significativo tra la percezione delle prestazioni e l'effettiva esposizione ai rischi.

Quello che emerge non è una carenza di strumenti, ma una mancanza di coerenza. I segnali arrivano più velocemente delle decisioni, quindi i processi di controllo e i flussi di lavoro si scontrano tra loro e non è più chiaro a chi spetti la responsabilità proprio nel momento in cui sarebbero necessari passaggi chiari dal rilevamento all'azione. In molte PMI, la sicurezza quotidiana è affidata a team IT generalisti o a singoli specialisti; solo il 42% delle aziende dispone di un team dedicato alla cybersecurity e questa fragilità è evidente in ogni fase e in ogni processo di escalation. La conseguenza è un'esposizione silenziosa: il triage rallenta, il contesto si perde e i problemi che sembrano tattici si accumulano fino a diventare rischi strategici. I decision-maker devono agire subito e fornire ai team di sicurezza strumenti, soluzioni personali adeguati. Soprattutto, devono comprendere la rilevanza della cybersecurity per il business e colmare il divario strutturale tra le priorità del board e la protezione sul campo.», ha affermato Cesare D'Angelo, General Manager Italy, Mediterranean & France di Kaspersky.

Per affrontare la mancanza di know-how e di strategia, Kaspersky consiglia ai leader aziendali e alle imprese di adottare le seguenti misure:

Informazioni su Kaspersky

Kaspersky è un'azienda globale di cybersecurity e privacy digitale fondata nel 1997. Con oltre un miliardo di dispositivi protetti dalle minacce informatiche emergenti e dagli attacchi mirati, la profonda esperienza di Kaspersky in materia di sicurezza e di Threat Intelligence si trasforma costantemente in soluzioni e servizi innovativi per la sicurezza di aziende, infrastrutture critiche, governi e consumatori in tutto il mondo. Il portfolio completo dell'azienda comprende una protezione Endpoint leader, prodotti e servizi di sicurezza specializzati e soluzioni Cyber Immune per contrastare le minacce digitali sofisticate e in continua evoluzione. Aiutiamo oltre 200.000 aziende a proteggere ciò che conta per loro. Per ulteriori informazioni è possibile consultare <https://www.kaspersky.it/>

Seguici su:

[Tweets by KasperskyLabIT](#)

<http://www.facebook.com/kasperskylabitalia>

<https://www.linkedin.com/company/kaspersky-lab-italia>

<https://www.instagram.com/kasperskylabitalia/>

<https://t.me/KasperskyItalia>

default watermark

[1]??Realtalk oncybersecurity?• ?? Per questo report Kaspersky ha commissionato Arlington Research di condurre un sondaggio online auto-compilabile con i decision-maker il cui ruolo coinvolge in modo significativo la sicurezza informatica, che lavorano per aziende con meno di 500 dipendenti in Europa nei mesi di agosto e settembre 2025. Arlington ha condotto un totale di 820 interviste (Europa: 600; 60 interviste ciascuno: Germania, Austria, Svizzera, Regno Unito, Francia, Italia, Spagna, Grecia, Romania, Serbia)

Contatti:

Immediapress

Contatto di redazione:

NoesisKaspersky Italia

kaspersky@noesis.net

COMUNICATO STAMPA ?? CONTENUTO PROMOZIONALE

Responsabilit  editoriale di Immediapress

??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione

Novembre 3, 2025

Autore

redazione

default watermark