Deloitte.

Michele Pozzi
Ufficio Stampa Deloitte
Tel: +39 342 154 0357
Email: mpozzi@deloitte.it

Tommaso Filippi, Michele Cartisano,
Tel: +39 3240021567, +39 3408524741
Email: deloitte-ita@omnicomprgroup.com

Deloitte: aziende nel mirino dei cyber criminali, il 98% delle italiane ha subito attacchi nel 2022

Otto aziende su 10 stanno ripensando la composizione dei loro Consigli di Amministrazione per includervi conoscenze tecnico-specialistiche cyber

- *Due terzi del campione prevedono di aumentare i propri investimenti in cybersecurity, un trend più marcato in Italia rispetto alla dinamica rilevata a livello globale (55%)*
- *Secondo gli intervistati una strategia di cybersecurity contribuisce a generare valore per le aziende, soprattutto in termini di brand reputation (92%), fiducia dei clienti (92%), resilienza (82%) e agilità (80%)*
- *Circa 2 dirigenti su 3 credono che la formazione in ambito cyber sia la chiave per coltivare i talenti che, secondo 4 intervistati su 10, oggi sono scarsamente disponibili*

Milano, 18 ottobre 2023 – In Italia il 98% delle aziende ha sperimentato almeno una violazione informatica nell'ultimo anno, con danni di entità grave o estremamente grave in circa 2 casi su 3. È quanto emerge dal report di Deloitte "Future of Cyber: una visione cyber-first per la sicurezza e la creazione di valore – Il punto di vista delle aziende italiane". Il report presenta i risultati emersi dalle interviste a un campione di dirigenti italiani, condotte nell'ambito di uno studio globale di Deloitte, appartenenti a organizzazioni con almeno 1.000 dipendenti e 500 milioni di dollari di fatturato annuo.

«L'analisi dei dati relativi allo scenario attuale in materia di cybersecurity nel nostro Paese mette chiaramente in evidenza una crescente consapevolezza che queste violazioni impattano le aziende da molteplici punti di vista», dichiara **Matthew Holt**, **Cyber Strategy and Transformation Leader di Deloitte**.

Le conseguenze delle violazioni informatiche per le aziende

Secondo quanto emerge dalle evidenze del report Deloitte, le conseguenze delle violazioni informatiche non si limitano solamente alla perdita di fatturato o alla riduzione del valore di mercato dell'azienda, come sostengono rispettivamente il 40% e il 36% dei dirigenti italiani intervistati, ma possono incidere sulle organizzazioni anche dal punto di vista normativo, comportando multe e sanzioni per inadempienza rispetto alle procedure in essere o per le violazioni dei regolamenti sulla cybersecurity, come riportato dal 52% degli intervistati. Grave anche il rischio reputazionale, in termini di ripercussioni negative sull'immagine dell'azienda, secondo il 44%, con il possibile crollo della fiducia da parte della clientela paventato dal 46%. Una medesima percentuale (46%) sottolinea il rischio tecnologico, ovvero la possibilità di minore fiducia nella "tech integrity" dell'azienda. Infine, un 42% segnala le conseguenze strategiche ed operative, come il rischio di minori budget a supporto delle iniziative strategiche o le possibili interruzioni delle *operation*.

Gli investimenti in cybersecurity delle aziende italiane

I dati che emergono dallo studio condotto da Deloitte mostrano come la cybersecurity stia progressivamente assumendo un ruolo fondamentale all'interno delle aziende, garantendo sempre più il raggiungimento degli obiettivi di business e la creazione di valore per i propri stakeholder. Tutto questo si riflette anche sulle

strategie d'investimento delle aziende stesse: due terzi del campione intervistato da Deloitte in Italia prevede di investire di più in cybersecurity, segnalando un trend più marcato nel nostro Paese rispetto alla dinamica rilevata a livello globale (55%). Tali investimenti sono necessari anche per implementare con successo le iniziative di trasformazione digitale: nei prossimi 3 anni, infatti, le soluzioni tecnologiche considerate prioritarie saranno quelle di Cloud Computing, come dichiara più di un'azienda su 2, e a seguire quelle di Intelligenza Artificiale (38%), IoT (38%) e Data Analytics (36%).

Cresce l'importanza della cybersecurity nei CdA delle aziende italiane

Inoltre, 9 dirigenti italiani intervistati su 10 hanno dichiarato che le questioni legate alla cybersecurity sono regolarmente all'ordine del giorno del loro CdA, con cadenza settimanale (36%), mensile (30%) o trimestrale (24%). I CdA delle aziende desiderano infatti essere sempre più coinvolti sul tema tanto che, come emerge nel report, in 3 casi su 4 il Board riceve aggiornamenti regolari in merito allo stato dei programmi di cybersecurity. Questo approccio consente all'organo direttivo di poter definire efficacemente le strategie e investimenti futuri, integrando al meglio il Risk Management nei processi aziendali. Non è un caso che addirittura 8 aziende su 10 stiano rivedendo la composizione del loro CdA per garantire all'interno dell'assemblea la presenza di professionalità con solide conoscenze tecnico-specialistiche in ambito cyber e con forti capacità di interazione nelle discussioni consiliari in grado di comprendere lo scenario attuale e futuro delle minacce cyber e le loro ricadute sul business.

L'importanza di una visione "cyber-first" integrata nella strategia aziendale

Un'adeguata strategia di cybersecurity supporta le aziende nel generare valore, non solo in termini di crescita dei ricavi, come indicato dal 78% dei rispondenti, ma anche e soprattutto di "brand reputation" (92%), fiducia dei clienti (92%) e modello di business resiliente (82%) e agile (80%). Sfruttare appieno tale potenziale, rendendo la cybersecurity un vero e proprio fattore abilitante per il raggiungimento degli obiettivi aziendali, è possibile solo se questa viene integrata nella più ampia strategia di business.

Secondo il 62% dei dirigenti italiani coinvolti nell'indagine, l'integrazione della cybersecurity all'interno delle strategie aziendali migliora l'efficienza nella gestione delle priorità di business sotto il profilo del risk management (94%), dal punto di vista della creazione di digital trust (92%), ma anche ai fini della trasformazione digitale (88%), poiché permette alle aziende di intraprendere percorsi di digitalizzazione con una maggiore sicurezza. Al di là dell'impatto sulle priorità di business, l'adozione di un approccio strategico e integrato alla cybersecurity, secondo gli intervistati, affina la capacità delle organizzazioni di anticipare l'identificazione dei rischi (54%), di prendere decisioni in modo rapido e agile (48%) e di adattarsi prontamente all'evoluzione del contesto competitivo (46%).

«Per vincere la sfida della cybersecurity, è cruciale sviluppare una visione "cyber-first" che permei l'organizzazione e tutte le attività aziendali: dallo sviluppo della strategia alla pianificazione, dall'avvio di nuove iniziative di trasformazione digitale alla progettazione di nuovi prodotti e servizi, dal coinvolgimento di terze parti nel proprio ecosistema alla gestione dei talenti. Ma l'adozione di questa prospettiva va al di là dell'implementazione tecnologica: si tratta di una vera e propria trasformazione aziendale e culturale», afferma **Holt**. *«È anche importante sottolineare che l'adozione di un approccio cyber-first agevola anche le organizzazioni nel percorso di conformità rispetto alle nuove normative, come nel caso del Regolamento DORA per il settore finanziario. Sviluppare una visione cyber-first, quindi, può assicurare un vantaggio competitivo rilevante»*, continua **Holt**.

Pianificazione strategica e operativa determinanti per un approccio cyber-first

La cybersecurity richiede un'attenta pianificazione strategica: secondo lo studio di Deloitte, infatti, 8 aziende italiane su 10 rivedono e aggiornano i propri piani di cybersecurity su base annua. A tal proposito, la quasi totalità delle aziende italiane (94%) ha già definito o sta definendo un piano olistico per la protezione da minacce cyber. Le imprese italiane affermano di sviluppare e implementare piani operativi che valutano le

Deloitte.

modalità di protezione dai rischi cyber in ogni fase della gestione del trattamento di dati sensibili (96%) e dichiarano di includere in ogni valutazione, o di essere quasi pronte a farlo, la più ampia rete di stakeholder, monitorando ad esempio la "security posture" di partner e fornitori per i propri programmi di valutazione del rischio cyber (92%).

«La formulazione di strategie di cybersecurity in grado di mitigare efficacemente i rischi e generare valore aziendale passa necessariamente da una solida pianificazione. Da questo punto di vista le aziende italiane si stanno dimostrando particolarmente consapevoli. Quella della pianificazione è una fase essenziale per sviluppare e implementare strategie "zero-trust" rispetto alla cybersecurity, in grado di rafforzare la sicurezza degli ambienti aziendali digitali, semplificandone la gestione e migliorando la customer experience», commenta **Holt**.

L'importanza della formazione cyber e la carenza di talenti

Il tema della formazione delle professionalità qualificate nel campo della cybersecurity è centrale per le aziende italiane. La mancanza di talenti in questa area, riconosciuta da 4 leader italiani su 10 intervistati, richiederà la collaborazione di attori pubblici e privati per la sua soluzione. Non a caso, la quasi totalità delle aziende italiane ritiene la formazione delle proprie risorse e dichiara di aver già implementato dei programmi di training per i dipendenti (92%). Affinché questi risultino efficaci, le organizzazioni devono però garantire che tale formazione sia erogata in modo continuativo, sia sempre aggiornata, sia coerente al "risk appetite" dell'azienda e offra percorsi differenziati e personalizzati. Circa 2 aziende italiane su 3 indicano che i programmi di formazione sono sì utili per dotare le aziende delle giuste competenze, ma sono anche uno dei principali strumenti per coinvolgere, trattenere e sviluppare i talenti.

«Investire nel talento è necessario per far fronte all'attuale carenza di professionalità qualificate e dotare l'organizzazione delle competenze necessarie per gestire le iniziative di cybersecurity, sempre più centrali per il successo e la generazione di valore. Affinché ciò possa risultare efficace, è opportuno che le aziende abbiano ben chiari quali sono i ruoli e le competenze più rilevanti in grado di garantire una consistente riduzione del complessivo rischio cyber a cui è esposta», conclude **Holt**.