

Cohesity: team IT e di sicurezza devono collaborare di più (e meglio)

https://www.hwupgrade.it/i/n/cohesity_720.jpg,



La scarsa collaborazione fra i responsabili IT e i SecOps, i team che si occupano delle operazioni di cybersecurity, aumenta il rischio di incidenti informatici. L'indagine di Cohesity e i suggerimenti su come potenziare la cooperazione fra i due ruoli

di [Alberto Falchi](#) pubblicata il **10 Giugno 2022**, alle **14:01** nel canale [Security](#)

[CohesityCloud Security](#)

Qual è la principale minaccia per la sicurezza informatica delle aziende? Secondo un'indagine di **Cohesity** non bisogna guardare solo a phishing, ransomware o mancanze di competenze, ma ai processi interni: **la mancata collaborazione fra i team IT e quelli delle Security Operations (SecOps)**.

La sicurezza deve essere una responsabilità condivisa: l'indagine di Cohesity

I team IT e quelli che si occupano delle operazioni relative alla sicurezza informatica, i SecOps, sembrano due mondi distanti, che hanno difficoltà a comunicare in maniera efficace pur lavorando nella stessa azienda. È quanto emerge da un sondaggio commissionato da **Cohesity** a Censuswide e basato su un campione di 2.000 decisioni maker operanti in ambito IT e SecOps in US, UK, Australia e Nuova Zelanda. Il campione è suddiviso in maniera praticamente identica fra le due figure.

L'IT e la sicurezza differiscono anche sulle funzionalità critiche

Alla domanda su come l'azienda abbia dato priorità a backup e protezione dati come item della postura di security o come risposta a un attacco informatico



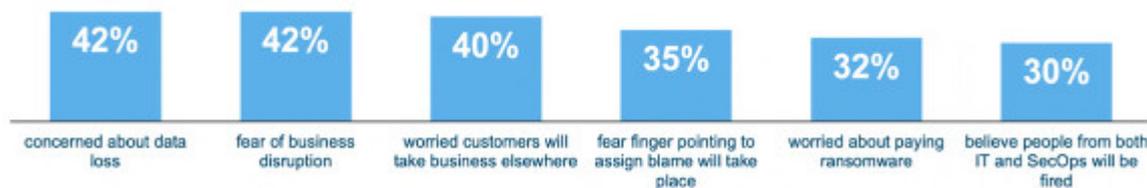
Ha dichiarato che si tratta di una priorità assoluta e di una funzionalità cruciale

Quasi tutti (81% del campione) convergono sul fatto che la cybersecurity dovrebbe essere una responsabilità condivisa, ma nella pratica la collaborazione non è così stretta e, in certi

casi, anche le priorità non sono sempre le stesse. Per fare un esempio concreto, **il 54% dei responsabili IT indica i backup e la protezione dei dati una priorità assoluta, mentre rivolgendo lo stesso quesito ai SecOps solo il 38% risponde lo stesso.**

*“Se i team SecOps non pensano al backup e al ripristino e non dispongono di capacità di gestione innovativa dei dati come parte di una strategia di sicurezza globale, c’è un problema”, spiega **Albert Zammar**, Regional Director Southern Europe di Cohesity. “I team IT e SecOps devono collaborare prima che si verifichi un attacco, guardando in modo olistico alla situazione e prendendo come riferimento il NIST Cyber Security Framework, che comprende cinque capacità fondamentali: identificare, proteggere, rilevare, rispondere e ripristinare. Se per collaborare aspettano il momento in cui si verifica una violazione dei dati, è troppo tardi e i risultati potrebbero rivelarsi catastrofici per le aziende”.*

I timori sono legati alla mancanza di collaborazione tra sicurezza e IT (agli intervistati è stato chiesto di sceglierne fino a tre)

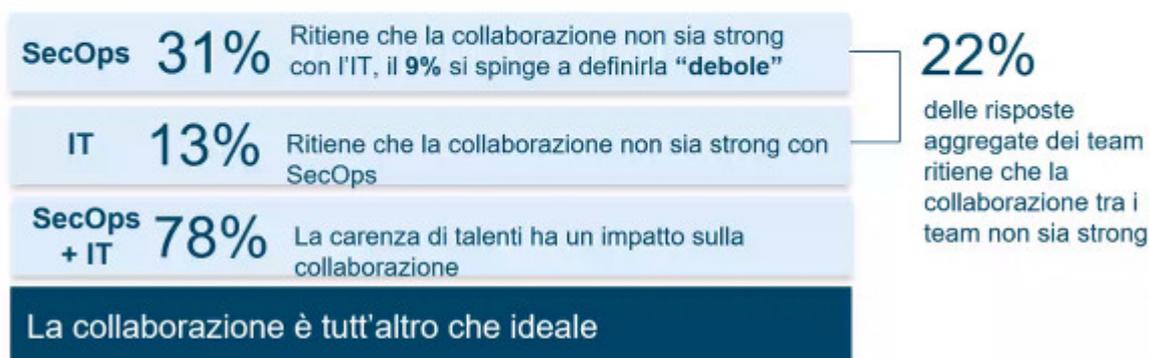


Questa scarsa collaborazione ha due effetti: da un lato incrementa il rischio di incidenti di sicurezza, dall’altro anche sulle prospettive di carriera dei responsabili. Sotto il profilo del rischio informatico, **i principali timori riguardano la perdita di dati, l’interruzione del business**, ma anche che i clienti possano scegliere altre realtà. Quasi **un intervistato su tre (30%), inoltre, teme anche di venire licenziato**: le minacce nell’ultimo anno sono aumentate di molto, soprattutto per quanto riguarda il ransomware (quasi la

metà, 47%, afferma che la propria azienda è stata vittima di un attacco di questo tipo negli ultimi sei mesi), e questa scarsa collaborazione non aiuta certo a reagire in maniera efficace. Questo nonostante 8 persone su dieci sostengano la necessità di una maggiore cooperazione fra team IT e SecOps.

Ma, IT e SecOps Collaborano Bene?

Dipende a chi lo chiediamo



Ma di chi è la colpa di una collaborazione poco efficace? Diciamo che i due mondi presi in esame non si scaricano la colpa a vicenda e il **78% sostiene che sia dovuta a una carenza di talenti.**

Migliorare la collaborazione fra team IT e SecOps: i consigli di Cohesity

Secondo Cohesity per potenziare la collaborazione fra IT e team di sicurezza è necessario che entrambi i gruppi siano co-responsabili dei successi relativi alla resilienza dell'infrastruttura, e debbano anche pianificare in maniera congiunta gli investimenti. Soprattutto, però, dovrebbero coordinare la propria risposta agli incidenti e non agire come

entità separate. Per questo motivo, anche le esercitazioni e i gruppi di lavoro dovrebbero essere strutturati così da facilitare la collaborazione fra le parti.

[Read More](#)