Rapporto Cisco: cloud e automazione sono le sfide della security

Apr 24, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario 1

L'indagine del colosso statunitense mette in luce le priorità delle aziende in tema di sicurezza informatica. Dalle esigenze alle strategie di difesa: ecco il quadro che emerge.

Si parla in continuazione del mutato panorama in ambito cyber security, della sua rilevanza a livello aziendale e dei cambiamenti avvenuti sia a livello di minacce, sia a livello di approccio da parte di chi queste minacce deve affrontare.

Più raramente, però, si ha l'occasione di verificare tutto questo sul campo, attraverso i feedback di chi si occupa tutti i giorni di sicurezza. Il report di **Cisco**, intitolato **2020 CISO Benchmark Study**, rappresenta da questo punto di vista uno strumento per avere una mappatura di ciò che sta accadendo a livello di cyber security attraverso la lente degli esperti del settore.

Lo studio, oltre a confermare alcuni elementi di ciò che sta accadendo nel settore, accende anche i riflettori sulle differenze tra l'Italia e il resto del mondo, evidenziando un livello di percezione decisamente diverso nel nostro paese rispetto ad altre realtà.

A partire, per esempio, dal tema dell'omologazione degli strumenti di difesa. Un problema che riguarda sempre più aziende, che per proteggere i loro sistemi IT arrivano a

utilizzare soluzioni specifiche di differenti produttori (fino a 20) che rendono estremamente complessa la loro gestione.

Un fenomeno che, secondo gli analisti di Cisco, è alla base di quello che hanno battezzato come "cybersecurity fatigue", cioè la rinuncia a stare al passo con le minacce e i criminali informatici.

Un problema che, nel nostro paese, sembra incidere meno che altrove, visto che viene indicato solo dal 29% degli intervistati contro il 42% del campione estero. Il tema, secondo gli esperti di Cisco, non è però da sottovalutare.

"Per supportare il percorso di trasformazione digitale che sta affrontando gran parte delle aziende, i CISO stanno dando sempre più importanza all'adozione di tecnologie di sicurezza per ridurre l'esposizione alle minacce informatiche. Spesso, molte di queste soluzioni non sono integrate, creando così una sostanziale complessità nella gestione del loro ambienti di sicurezza," spiega **Steve Martino**, **Senior Vice President and Chief Information Security Officer di Cisco**. "Per risolvere tale problema, i professionisti della sicurezza devono continuare verso il consolidamento dei vendor, aumentando al contempo la fiducia nella sicurezza e nell'automazione nel cloud per rafforzare il loro livello di sicurezza e ridurre il

rischio di violazioni”.

Ma quali sono gli ambiti in cui le aziende incontrano le maggiori difficoltà? Secondo la ricerca, uno dei temi più spinosi riguardala protezione dei dispositivi mobile e personali, che per il 52% degli intervistati (il 32% in Italia) continuano a rappresentare un problema.

Percepito come problematica anche **la gestione dei datacenter**, con il 41% delle aziende intervistate (il 23% in Italia) che ritiene estremamente difficile proteggerli, mentre il 39% (il 25% in Italia) dichiara di avere difficoltà nel garantire l’integrità delle applicazioni.

Altra criticità sarebbe rappresentata dal **cloud pubblico**, con il 52% (il 30% in Italia) che ritiene tale attività molto o estremamente difficile, e il 50% (il 36% in Italia) secondo il quale l’infrastruttura cloud privata è stata una delle principali sfide in termini di sicurezza.

Insomma: a guardare i dati, sembrerebbe che nel nostro paese ci sia una percezione decisamente diversa. Il dubbio, inutile negarlo, è che più che un minore livello di criticità, ci sia un’inferiore consapevolezza dei rischi e, in definitiva, una

minore sensibilità sul tema.

Dallo studio, però, emergono anche alcuni dati rassicuranti per il nostro paese. Il primo riguarda l'adozione di sistemi di autenticazione multi-fattore. Secondo quanto registrato nella ricerca, il 38% delle aziende italiane utilizzerebbe un approccio **Zero Trust** basato su MFA per l'accesso alle reti, contro il 27% a livello globale.

Anche il numero di attacchi subiti a causa di vulnerabilità non corrette (46% delle aziende a livello globale, 30% in Italia) lascerebbe pensare a una situazione che, per una volta, colloca il nostro paese in una posizione migliore rispetto ad altre realtà.

La tendenza nel settore, però, conferma l'attenzione degli esperti al tema dell'automazione nei sistemi di sicurezza, in cui l'adozione di strumenti di intelligenza artificiale e machine learning rappresenta una priorità assoluta.

Soprattutto per quanto riguarda la protezione dei servizi cloud, che vengono percepiti come un fattore abilitante ma richiedono strumenti specifici per garantirne la sicurezza.

Condividi l'articolo

Allarme dell'NSA sulla diffusione delle Web Shell Pasticcio sulle falle di sicurezza per IBM: online 4 zero-day

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/24/rapporto-cisco-cloud-e-automazione-sono-le-sfide-della-

security/?utm_source=rss&utm_medium=rss&utm_campaign=rapporto-cisco-cloud-e-automazione-sono-le-sfide-della-security