

Studio IBM: migliora la capacità di predisporre piani per la sicurezza ma il rischio di attacchi cyber resta elevato

Oltre 50 tool utilizzati risultano non essere particolarmente efficaci. La maggior parte delle organizzazioni non dispone di piani specifici volti a contrastare gli attacchi informatici più comuni e le minacce emergenti

CAMBRIDGE, Mass., 10 Luglio 2020 -- IBM (NYSE: IBM) IBM Security ha reso noti i risultati del "Cyber Resilient Organization Report", lo studio annuale volto a rilevare e analizzare il livello di preparazione delle aziende nei confronti dei rischi legati agli attacchi informatici. Negli ultimi 5 anni è migliorata la capacità di pianificare, rilevare e rispondere agli attacchi informatici ma, contestualmente, è diminuita del 13% quella di fronteggiarli. Lo studio, condotto a livello globale da Ponemon Institute e promosso da IBM Security, ha evidenziato che l'utilizzo di un numero eccessivo di tool di sicurezza e la mancanza di linee guida specifiche per contrastare gli attacchi informatici più diffusi rendono le organizzazioni vulnerabili.

Se da un lato è lievemente migliorata la capacità di attuare piani di sicurezza, dall'altro la stragrande maggioranza delle organizzazioni intervistate (74%) dispone di piani inefficaci o non ha alcun piano. Ciò può influire negativamente non solo sulla capacità di fronteggiare gli attacchi ma anche sui costi: le aziende che dispongono di piani strutturati e risorse dedicate ed effettuano test periodici, infatti, spendono in media 1,2 milioni di dollari in meno, in caso di violazione dei dati, rispetto a quelle che scelgono di rimanere destrutturate per ridurre i costi[1].

Queste le principali evidenze dell'ultimo "Cyber Resilient Organization Report":

- **Miglioramento lento:** negli ultimi 5 anni molte delle organizzazioni intervistate hanno adottato piani di security strutturati: dal 18% nel 2015 si è passati al 26% nell'ultimo anno, con una crescita complessiva del 44% in 5 anni.
- **Manuali di sicurezza:** tra le aziende che hanno adottato un piano strutturato, solo un terzo (il 17% del totale) ha anche realizzato manuali specifici con le indicazioni per fronteggiare gli attacchi informatici più diffusi; le stesse risultano meno preparate nei confronti di minacce emergenti, come il ransomware.
- **La complessità ostacola la capacità di contrastare gli attacchi:** disporre di troppi tool di security crea complessità. Le organizzazioni che ne utilizzano più di 50 hanno una capacità di rilevare un attacco inferiore dell'8% e una capacità di fronteggiarlo inferiore al 7%.
- **Pianificazione efficace, minori problemi:** le aziende che dispongono di piani di sicurezza strutturati hanno meno probabilità di subire interruzioni significative in caso di attacco informatico. Negli ultimi due anni, solo il 39% di queste organizzazioni ha subito un attacco significativo, rispetto al 62% di quelle con piani destrutturati.

"Molte organizzazioni hanno compreso l'importanza di disporre di piani di sicurezza, che presuppongono un insieme di attività strutturate", ha affermato Wendi Whitmore, Vice President IBM X-Force Threat Intelligence. "Le organizzazioni devono anche pianificare regolarmente test, simulazioni e verifiche per essere sempre efficienti. Facendo leva sull'interoperabilità delle tecnologie e sull'automazione è possibile vincere le sfide della complessità ed essere più rapidi nel contenere un attacco informatico."

Aggiornamento dei manuali per fronteggiare le minacce emergenti

Lo studio ha rilevato che anche tra le organizzazioni che hanno implementato un piano di cybersecurity strutturato (CSIRP, cybersecurity incident response plan), solo il 33% disponeva di procedure dedicate a specifiche tipologie di minacce. Attacchi diversi possono essere contrastati da metodologie univoche, pertanto è sicuramente utile prevedere procedure predefinite che illustrino operazioni standard da attuare per fronteggiare gli attacchi più comuni.

Le procedure più diffuse sono quelle dedicate agli attacchi DDoS (64%) e ai malware (57%), ossia quelli

storicamente più comuni, anche se lo studio rivela il ransomware quale minaccia in crescita. Negli ultimi anni gli attacchi ransomware sono infatti aumentati di quasi il 70%^[2], ciò nonostante solo il 45% degli intervistati ha dichiarato di disporre di piani specifici volti a contrastare queste nuove minacce.

Inoltre, oltre la metà (52%) di coloro che hanno predisposto piani di sicurezza ha dichiarato di non averli mai aggiornati o, comunque, di non aver previsto collaudi o verifiche periodiche. Inoltre, rapidi cambiamenti nei processi aziendali, come l'introduzione del lavoro da remoto, facilitano la creazione di nuove tecniche di attacco e aumentano i rischi per le organizzazioni che fanno affidamento su piani di security obsoleti, non allineati ai nuovi e mutati scenari.

La molteplicità di strumenti porta ad una minore efficacia

Il rapporto mette anche in evidenza come la complessità abbia un impatto negativo sulle capacità di risposta agli attacchi. Le aziende intervistate hanno stimato di utilizzare in media più di 45 diversi dispositivi di sicurezza e che ciascun attacco ha richiesto, mediamente, il coordinamento di 19 tool. Tuttavia, lo studio ha anche rivelato che il ricorso ad un numero eccessivo di strumenti può effettivamente ostacolare la capacità di proteggersi. Secondo il report, le aziende che utilizzano più di 50 tool hanno una capacità ridotta - l'8% in meno - nel rilevare un attacco e nel fronteggiarlo - 7%. Il ricorso a più tool non porta necessariamente a una maggiore protezione. Di contro, l'utilizzo di piattaforme aperte, interoperabili e di tecnologie di automazione può aiutare a ridurre la complessità: il 63% delle organizzazioni con elevate performance ha affermato che l'interoperabilità è un fattore abilitante nel fronteggiare gli attacchi informatici.

Migliore pianificazione, maggiore efficacia

Il report mette in evidenza come investire in piani strutturati consenta di contrastare in modo più efficace gli attacchi informatici. Tra gli intervistati, coloro che dispongono di un CSIRP applicato correttamente, solo il 39% ha subito un attacco che ha provocato un'interruzione significativa delle attività negli ultimi due anni, rispetto al 62% di coloro che non hanno predisposto un piano strutturato.

In questo contesto, disporre di personale qualificato, con competenze specifiche, è un requisito fondamentale per sviluppare resilienza agli attacchi informatici, secondo il 61% degli intervistati. Il 41% delle organizzazioni ha dichiarato di non essere particolarmente resiliente a causa della mancanza di risorse qualificate.

La tecnologia è risultata un altro elemento differenziante nell'aiutare le organizzazioni a essere più cyber-resilienti, soprattutto in presenza di particolari complessità. I due principali fattori abilitanti sono l'opportunità di accesso ad applicazioni e dati (57%) e il ricorso a procedure automatizzate (55%). In conclusione, le tecnologie più avanzate permettono una maggiore resilienza.

Il Report

Condotto da Ponemon Institute e promosso da IBM Security, il Cyber Resilient Organization Report, giunto alla quinta edizione, analizza la preparazione e la capacità di fronteggiare gli attacchi informatici. La ricerca ha coinvolto oltre 3,400 IT e security manager a livello mondiale, in particolare in questi Paesi: Stati Uniti, India, Germania, Gran Bretagna, Brasile, Giappone, Australia, Francia, Canada, ASEAN, e Medio Oriente.

Il report completo è disponibile qui: <https://www.ibm.com/account/reg/us-en/signup?formid=urx-45839>

È possibile prendere parte ad un webinar dedicato in programma il 23 luglio, h 11:00 AM ET:

<https://event.on24.com/wcc/r/2448121/9297B87DE7A378D816846835989BD762>

IBM Security

IBM Security offre uno dei portfolio di offerta più completi e integrati di prodotti e servizi per la protezione aziendale. Il portfolio, supportato dal team di ricerca di fama mondiale IBM X-Force®, consente alle organizzazioni di gestire con efficacia il rischio e difendersi dalle minacce emergenti. IBM dirige una delle organizzazioni di ricerca, sviluppo e delivery di soluzioni di sicurezza più grandi al mondo, monitora 70 miliardi di eventi di security al giorno in più di 130 Paesi e ha ottenuto oltre 10.000 brevetti di sicurezza. Per maggiori informazioni, visita il sito www.ibm.com/security, segui @IBMSecurity su Twitter o visita il [blog di IBM Security Intelligence](#).

Contatti

Claudia Ruffini, IBM Media Relations
335 6325093 cla@it.ibm.com

[1] IBM Security and Ponemon Institute: *2019 Cost of a Data Breach Report*

[2] IBM Security, *2020 X-Force Threat Intelligence Index*, (2020), p. 15

<https://it.newsroom.ibm.com/IBMPonemomStudy>