IBM Italy News Room

Studio IBM: sempre più difficile difendersi contro i cyber-attacchi

Quasi il 60 percento dei responsabili della sicurezza ritiene che le capacità di difesa delle loro organizzazioni non siano all'altezza degli hacker

Milano - 10 dic 2014: Secondo un recentissimo studio di IBM, più dell'80 percento dei responsabili della sicurezza afferma che le sfide poste dalle minacce esterne siano in aumento, mentre 60 percento ritiene che nella guerra ai crimini informatici gli hacker abbiano la meglio sulla loro organizzazione. Lo studio rivela inoltre che la tecnologia è considerata un elemento critico per affrontare le sfide e le minacce relative alla sicurezza e che i Big data, il cloud e il mobile computing rappresentano le aree di massima priorità. Il terzo studio annuale di IBM dedicato ai Chief Information Security Officer (CISO) è stato condotto dall'IBM Center for Applied Insight, basandosi su 138 interviste rivolte ai massimi responsabili della sicurezza aziendale a livello globale. Le minacce esterne, sempre più sofisticate, sono state individuate come sfida principale dal 40 percento dei responsabili della sicurezza, seguite a distanza dalle normative, in seconda posizione con poco meno del 15 percento: le minacce esterne richiederanno il maggiore sforzo da parte delle organizzazioni nei prossimi tre-cinque anni – pari a quello richiesto complessivamente da normative, nuove tecnologie e minacce interne.

"I CISO hanno finalmente voce nei consigli di amministrazione", commenta Brendan Hannigan, General Manager, IBM Security. "I responsabili della sicurezza devono ora sfruttare questa loro posizione di influencer per fornire risultati migliori, ovvero per meglio definire le priorità nella protezione degli asset critici, focalizzare gli investimenti sull'intelligence e reclutare i migliori talenti del settore".

Le organizzazioni di oggi ripensano alle tattiche di cyber-sicurezza
Scopo dello studio era scoprire e comprendere come le organizzazioni si stanno proteggendo dai cyber-attacchi: il 70 percento dei responsabili della sicurezza ritiene di disporre di tecnologie tradizionali mature, incentrate sulla prevenzione dalle intrusioni di rete (network intrusion prevention), rilevamento di malware (advanced malware detection) e scansione delle vulnerabilità di rete (network vulnerability scanning).

Tuttavia, quasi la metà degli intervistati è concorde nel ritenere che l'adozione di nuove tecnologia di sicurezza sia l'area di principale focalizzazione per la propria organizzazione, individuando nella prevenzione della perdita di dati, nella sicurezza del cloud e nella sicurezza del mobile le tre aree prioritarie di trasformazione.

Dallo studio di IBM è inoltre emerso che:

- **La sicurezza del cloud continua a essere una priorità:** mentre restano forti i timori sulla sicurezza del cloud, quasi il 90 percento degli intervistati ha dichiarato di avere adottato il cloud o di aver pianificato iniziative in tale senso. Di questi, il 75 percento prevede - nei prossimi tre-cinque anni - un aumento, in alcuni casi anche molto significativo, del proprio budget per la sicurezza del cloud.
- **La security intelligence basata sui dati è in primo piano:** oltre il 70 percento dei responsabili della sicurezza afferma che la security intelligence in tempo reale è sempre più importante per la propria organizzazione. Nonostante ciò, lo studio ha riscontrato che aree quali raccolta e classificazione dei dati e analytics per la security intelligence hanno un grado di maturità relativamente basso (54 percento) e presentano spazi di miglioramento o trasformazione.

- **Permangono esigenze significative nella sicurezza *mobile*:** nonostante la crescita della forza lavoro *mobile*, solo il 45 percento dei responsabili della sicurezza afferma di avere un approccio efficace alla gestione dei dispositivi mobili. In effetti, secondo lo studio, la sicurezza del mobile computing e dei dispositivi si trova in fondo alla classifica in termini di maturità (51 percento).

Gestire i rischi a livello governativo

Oltre alle minacce esterne, lo studio indica che i CISO si trovano ad affrontare ulteriori sfide a livello governativo: quasi l'80 percento degli intervistati afferma infatti che il potenziale rischio derivante da normative e standard è aumentato nel corso degli ultimi tre anni. I responsabili della sicurezza manifestano incertezza soprattutto sull'eventualità che le autorità pubbliche gestiscano la governance della sicurezza a livello nazionale o globale e sul livello di trasparenza con cui procederanno al riguardo. Solo il 22 percento ritiene che nei prossimi tre-cinque anni si arriverà a concordare un approccio globale nella lotta al crimine informatico.

Come dare più potere ai responsabili della sicurezza di oggi

Con la continua evoluzione degli attacchi informatici e delle normative, la maggior parte delle organizzazioni ha ridefinito la propria visione della sicurezza negli ultimi tre anni, portando i leader della sicurezza a ruoli di maggiore influenza. Secondo lo studio, il 90 percento dei responsabili della sicurezza concorda fortemente sul fatto di essere influenti per la propria organizzazione e il 76 percento afferma che il proprio grado di influenza è significativamente aumentato negli ultimi tre anni. Inoltre, il 71 percento è fortemente d'accordo sul fatto di ricevere dall'organizzazione il sostegno necessario a svolgere il loro lavoro con efficacia.

Informazioni sulla ricerca

Per avere una fotografia aggiornata sulla situazione attuale vissuta dai responsabili della sicurezza e sulle loro opinioni riguardo al panorama futuro, l'IBM Center for Applied Insights, in collaborazione con IBM Security, ha condotto 138 interviste a leader della sicurezza – dirigenti IT e responsabili di business di più alto livello responsabili della sicurezza nelle rispettive organizzazioni. Il 63 percento con la qualifica di Chief Information Security Officer (CISO); altri, data l'eterogeneità delle strutture aziendali, con qualifiche diverse, tra cui CIO, vice-president della sicurezza IT e direttori della sicurezza. La partecipazione ha riguardato aziende appartenenti a una vasta gamma di settori e a cinque diversi Paesi. Per scaricare lo studio, visitare il sito: www.ibm.com/security/ciso.

Per ulteriori informazioni, visitate il sito www.ibm.com/, seguite @IBMCAI su Twitter, oppure visitate il blog dell'IBM Center for Applied Insights.

Informazioni su IBM Security

La piattaforma di sicurezza di IBM fornisce la security intelligence necessaria per aiutare le aziende a proteggere in modo onnicomprensivo i propri dipendenti, dati, applicazioni e infrastrutture. IBM offre soluzioni per la gestione delle identità e degli accessi, la gestione delle informazioni e degli eventi di sicurezza, la sicurezza dei database, lo sviluppo delle applicazioni, la gestione del rischio, la gestione degli endpoint, la protezione dalle intrusioni di *next generatio*n e molto altro. IBM gestisce una delle maggiori organizzazioni al mondo di ricerca e sviluppo in ambito security, e un'altrettanto vasta organizzazione globale per il delivery dei servizi di sicurezza.

Per ulteriori informazioni, visitate il sito www.ibm.com/security, seguite @IBMSecurity su Twitter, oppure visitate il **blog** di IBM Security Intelligence.

https://it.newsroom.ibm.com/2014-12-10-Studio-IBM-sempre-piu-difficile-difendersi-contro-i-cyber-attacchi