IBM Italy News Room

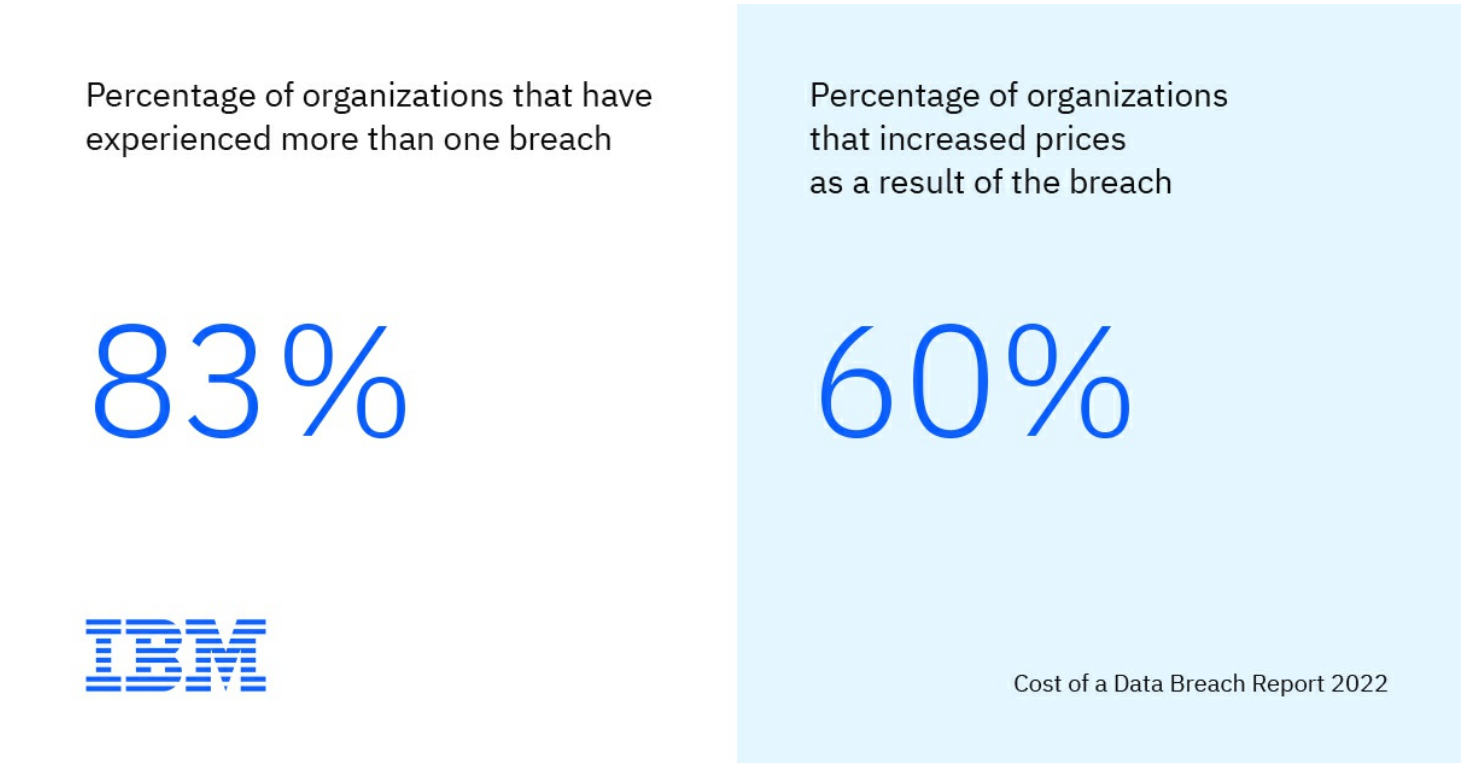
Report IBM: il costo delle violazioni dei dati ha raggiunto il suo massimo storico e a pagarne il prezzo sono i consumatori

• Il 60% delle aziende che hanno subito dei data breach ha aumentato i prezzi di beni e servizi dopo la violazione;

• La maggioranza delle imprese che operano in infrastrutture critiche è in ritardo nell'adozione di un approccio zero trust;

• Le aziende che non hanno personale sufficientemente preparato pagano $550.000 in costi supplementari;

• In Italia, il costo medio di ogni singolo dato rubato è di €143, mentre quello globale è di $164. Tra le 17 aree geografiche analizzate, l'Italia si colloca all'ottavo posto, e l'industria farmaceutica è quella ad aver pagato di più: ogni dato rubato è costato €182. Seguono il settore tecnologico (€174) e quello dei servizi finanziari (€173). Il primo vettore di attacco è il phishing mentre quello che comporta i costi maggiori è la perdita accidentale di dati o device (€4,92 milioni).



CAMBRIDGE, Mass.,27 luglio 2022 – IBM Security ha pubblicato l'annuale Cost of a Data Breach Report,[1] che rivela violazioni dei dati senza precedenti sia in termini di costo sia di impatto. Il costo medio globale dei data breach ha raggiunto il massimo storico di $4,35 milioni, un aumento di circa il 13% rispetto agli ultimi due anni analizzati dal report. Questi risultati potrebbero contribuire all'aumento dei costi di beni e servizi: il 60% delle organizzazioni prese in considerazione ha infatti aumentato i prezzi a seguito delle violazioni, un aumento che si somma alla crescita dei prezzi, già elevata in tutto il mondo, dovuta a inflazione e problemi della supply chain.

Il susseguirsi degli attacchi informatici sta inoltre facendo luce sull' “effetto persecutorio” dei data breach nelle aziende. Il report IBM rileva che l'83% delle organizzazioni analizzate ha subito più di una violazione di dati nel corso della propria attività. Inoltre, le violazioni continuano ad avere effetti sempre più a lungo termine: circa il 50% dei costi dei data breach viene sostenuto più di un anno dopo la violazione.

Il report Cost of a Data Breach del 2022 si basa su un'analisi approfondita delle violazioni dei dati subite da 550 organizzazioni di tutto il mondo tra marzo 2021 e marzo 2022. La ricerca, promossa e analizzata da IBM Security, è stata condotta dal Ponemon Institute.

Alcuni dei risultati chiave nel report IBM 2022 includono:

- **Ritardi delle infrastrutture critiche in Zero Trust -** Circa l'80% delle organizzazioni che operano in infrastrutture critiche non adotta strategie zero trust, con i costi medi delle violazioni che aumentano fino a $5,4 milioni - un aumento di $1,17 milioni rispetto alle aziende che adottano tali strategie. Il 28% dei data breach verso queste organizzazioni è costituito da ransomware o attacchi distruttivi.
- **Pagare non paga -** Le vittime di ransomware che hanno scelto di pagare le richieste di riscatto degli autori delle minacce hanno risparmiato solo $610.000 in media rispetto alle organizzazioni che hanno scelto di non pagare, un risparmio da cui va detratto il costo del riscatto. Considerando le richieste di pagamento elevate, il costo finanziario potrebbe crescere ancora, suggerendo che il semplice pagamento del riscatto potrebbe non essere una strategia efficace.
- **Immaturità della sicurezza nel cloud -** Il 43% delle organizzazioni prese in esame è nella fase iniziale o non ha ancora iniziato ad applicare pratiche di security nei propri ambienti cloud, subendo in media costi di violazione più elevati di circa $660.000 rispetto alle organizzazioni con una security più matura.
- **Automazione e AI per la security sono i principali fattori di risparmio** - Le organizzazioni che hanno adottato completamente l'automazione e l'AI per la security hanno pagato mediamente circa $3,05 milioni in meno rispetto alle organizzazioni che non hanno adottato queste tecnologie - il più grande risparmio osservato nello studio.

"Le aziende devono concentrare le proprie difese di sicurezza sugli attacchi e battere gli aggressori sul tempo. È ora di impedire agli avversari di raggiungere i propri obiettivi e di iniziare a ridurre al minimo l'impatto degli attacchi. Più le aziende provano a perfezionare il proprio perimetro di difesa invece di investire in rilevazione e risposta, più le violazioni finiscono con l’alimentare l'aumento del costo della vita.” ha affermato Charles Henderson, Global Head di IBM Security X-Force. "Questo report mostra che le giuste strategie, abbinate alle giuste tecnologie, fanno la differenza quando le aziende vengono attaccate".

Eccessiva fiducia nella gestione delle infrastrutture critiche

Nell’ultimo anno, è aumentata in tutto il mondo la preoccupazione per le infrastrutture critiche, sempre più bersaglio dei cybercriminali. Molte agenzie governative per la sicurezza informatica hanno sollecitato allerta contro gli attacchi malevoli. Infatti, il report di IBM rivela che i ransomware e gli attacchi distruttivi costituiscono il 28% delle violazioni verso organizzazioni parte di settori infrastrutturali critici – finanziario, manifatturiero, sanitario e dei trasporti tra gli altri – evidenziando come gli autori delle minacce stiano cercando di innescare una rottura delle supply chain globali, che si affidano a queste organizzazioni.

Nonostante l’invito alla cautela, e un anno dopo che l'Amministrazione Biden ha emesso un ordine esecutivo

sulla sicurezza informatica incentrato sull'importanza dell'adozione di un approccio zero trust per rafforzare la sicurezza informatica della nazione, il report ha evidenziato che solo il 21% di questo tipo di imprese adotta un modello di sicurezza zero trust. A ciò si aggiunge che il 17% delle violazioni dirette a infrastrutture critiche è stato causato dalla compromissione iniziale di un business partner, evidenziando che i rischi per la security spesso derivano da una fiducia eccessiva negli ambienti di collaborazione.

Le aziende che pagano il riscatto non fanno un "affare"

Secondo il report, le aziende che hanno pagato le richieste di riscatto hanno speso circa $610.000 in meno come costo medio di una violazione rispetto a quelle che hanno scelto di non pagare, senza considerare l'importo del riscatto pagato. Tuttavia, considerando il costo medio del riscatto, che secondo Sophos ha raggiunto $812.000 nel 2021, le imprese che decidono di pagare il riscatto potrebbero sostenere costi totali più elevati. Inoltre, questi capitali vanno a finanziare inconsapevolmente futuri attacchi di ransomware, mentre potrebbero essere destinati a interventi di remediation e recovery e alla ricerca di potenziali reati federali.

La persistenza del ransomware, nonostante il significativo impegno globale per bloccarlo, è alimentata dall'industrializzazione dei crimini informatici. IBM Security X-Force ha scoperto che la durata degli attacchi di ransomware diretti alle aziende è diminuita del 94% negli ultimi tre anni – passando da oltre due mesi a poco meno di quattro giorni. Un ciclo di vita dell'attacco così esponenzialmente breve può condurre ad attacchi di impatto maggiore, poiché lascia agli addetti alla security una finestra di tempo molto piccola per rilevarli e contenerli. Con un "tempo di riscatto" che scende a poche ore, è fondamentale che le aziende diano priorità ad una verifica rigorosa dei manuali di incident response. Tuttavia, il report indica che il 37% delle organizzazioni prese in esame che hanno piani di incident response non li controlla regolarmente.

Vantaggi del cloud ibrido

Il report indica anche che gli ambienti cloud ibridi costituiscono le infrastrutture più diffuse (45%) tra le organizzazioni esaminate. Con una media pari a $3,8 milioni, le aziende che hanno adottato un modello di cloud ibrido hanno sostenuto costi di violazione inferiori rispetto alle aziende con un modello di cloud esclusivamente pubblico o privato, che hanno registrato rispettivamente una media di $5,02 e $4,24 milioni. Infatti, le aziende che hanno adottato il cloud ibrido sono state in grado di identificare e contenere le violazioni dei dati in circa 15 giorni in meno rispetto alla media globale di 277 giorni.

Il report evidenzia che il 45% delle violazioni esaminate si è verificata nel cloud, sottolineando l'importanza della security nel cloud. Tuttavia, un significativo 43% delle organizzazioni indicate nel report ha dichiarato di essere solo nelle prime fasi di adozione del cloud o di non aver iniziato ad implementare pratiche di security per proteggere i propri ambienti cloud, sostenendo così costi di violazione più elevati[2]. Le aziende che non hanno adottato pratiche di security nei propri ambienti cloud hanno richiesto in media 108 giorni in più per identificare e contenere un data breach rispetto a quelle che applicano le pratiche di security in modo coerente in tutti i propri domini.

Ulteriori risultati nel report IBM 2022 includono:

- **Il phishing diventa la causa di violazione più costosa -** Sebbene le credenziali compromesse continuino a rappresentare la causa di violazione più comune (19%), il phishing rappresenta la seconda

(16%) e più costosa causa, portando a $4,91 milioni i costi di violazione medi.

- **Per la prima volta, i costi delle violazioni del settore sanitario raggiungono la doppia cifra** - Per il dodicesimo anno consecutivo, le imprese del settore sanitario hanno assistito alle violazioni più costose rispetto agli altri settori, sostenendo un aumento del costo medio di quasi $1 milione, che ha raggiunto un record di $10,1 milioni.
- **Il personale addetto alla security è insufficiente** - Il 62% delle organizzazioni intervistate ha dichiarato di non disporre di personale sufficiente per soddisfare le proprie esigenze di security, sostenendo in media $550.000 di costi per le violazioni in più rispetto a quelle che affermano di disporre di personale sufficiente.

Ulteriori fonti

- Il report Cost of a Data Breach del 2022 è disponibile qui: https://www.ibm.com/security/data-breach.
- Iscriviti al webinar 2022 IBM Security Cost of a Data Breach di mercoledì, 3 agosto 2022, alle 11:00 ET qui.

IBM Security

IBM Security offre un portfolio ampio e integrato di prodotti e servizi per la sicurezza aziendale tra i più all'avanguardia nel settore. Il portfolio, supportato dalla ricerca IBM Security X-Force®, consente alle organizzazioni di gestire efficacemente il rischio e di difendersi dalle minacce emergenti. IBM gestisce una delle organizzazioni di ricerca, sviluppo e distribuzione di security più grandi del mondo, monitora oltre 150 miliardi di eventi di security al giorno in più di 130 paesi, e ha ottenuto più di 10.000 brevetti di security in tutto il mondo. Per ulteriori informazioni, visitare il sito www.ibm.com/security, @IBMSecurity suTwitter o il blog IBM Security Intelligence.

---

[1] Cost of a Data Breach Report 2022, condotto da Ponemon Institute, promosso e analizzato da IBM

[2] Costo medio di $4.53M, rispetto al costo medio di $3,87 milioni delle organizzazioni partecipanti con pratiche di sicurezza cloud in fase matura

Per ulteriori informazioni: Claudia Ruffini, IBM Communications Italia, cla@ibm.com, +39 335 6325093
