Studio IBM: i costi della violazione dei dati sono in aumento con impatti finanziari prolungati per anni

Le violazioni rappresentano un rischio crescente per le piccole imprese, con un costo pari a quasi il 5% del fatturato annuo

Cambridge, MA - 23 lug 2019: IBM ha annunciato i risultati del suo studio annuale che esamina l'impatto finanziario delle violazioni di dati sulle aziende. Secondo il rapporto, il costo di una violazione di dati è aumentato del 12% negli ultimi 5 anni e corrisponde oggi a 3,92 milioni di dollari in media. La crescita è rappresentativa dell'impatto finanziario pluriennale delle violazioni, dell'aumento delle regolamentazioni e del complesso processo di risoluzione degli attacchi criminali .

Le conseguenze finanziarie di una violazione di dati possono essere particolarmente gravi per le piccole e medie imprese. Secondo la ricerca, le aziende con meno di 500 dipendenti hanno subito perdite di oltre 2,5 milioni di dollari in media, un importo fortemente penalizzante per questa categoria di imprese.

Per la prima volta, quest'anno è stato esaminato anche l'impatto finanziario a lungo termine di una violazione di dati, che è risultato essere prolungato nel tempo. Circa il 67% dei costi della violazione di dati viene registrato entro il primo anno, il 22% nel secondo anno e un altro 11% si estende oltre i due anni dalla violazione. I costi sono risultati più elevati nel secondo e terzo anno per le aziende operanti in ambienti altamente regolamentati, come la sanità, i servizi finanziari, l'energia e l'industria farmaceutica.

"Il cybercrime è fonte di guadagno per i criminali informatici e a questo corrispondono perdite significative per le aziende colpite", ha affermato Wendi Whitmore, Global Lead di IBM X-Force Incident Response and Intelligence Services. "Considerando che le organizzazioni hanno dovuto affrontare la perdita o il furto di oltre 11,7 miliardi di dati solo negli ultimi 3 anni, le imprese devono essere pienamente consapevoli dell'impatto finanziario che una violazione dei dati può avere sui loro profitti e, quindi, concentrarsi su come è possibile ridurre questi costi."

Il rapporto annuale "Cost of a Data Breach" (Costo di una violazione di dati) sponsorizzato da IBM Security e condotto dal Ponemon Institute, si basa su interviste approfondite condotte con più di 500 aziende in tutto il mondo che hanno subito una violazione nell'ultimo anno3]. L'analisi tiene conto di centinaia di fattori di costo, tra cui attività legali, normative e tecniche dovute a perdite di valore del brand e di produttività dei dipendenti.

Tra i principali risultati dello studio di quest'anno è possibile elencare:

- **le violazioni malevole sono le più comuni e costose**: Oltre il 50% delle violazioni di dati analizzate nello studio è stato causato da attacchi cyber malevoli ed è costato alle aziende in media 1 milione di dollari in più rispetto a quelli derivanti da cause accidentali.

- **le "Mega violazioni" comportano Mega-perdite**4[4]: anche se meno comuni, le violazioni di più di 1 milione di dati costano alle aziende circa 42 milioni di dollari di perdite; quelle da 50 milioni di dati, circa 388 milioni di dollari.
- **sbagliando si impara**: le aziende con un team di risposta agli incidenti dedicato e con un piano di risposta ampiamente testato hanno registrato dei costi di violazione di dati inferiori di 1,23 milioni di dollari in media rispetto a quelle che non avevano messo in atto nessuna delle due misure.
- **le violazioni negli Stati Uniti costano il doppio**: il costo medio di una violazione negli Stati Uniti è di 8,19 milioni di dollari, più del doppio della media mondiale.
- **le violazioni in ambito sanitario costano di più**: per il nono anno consecutivo, le aziende sanitarie hanno subito il costo più alto di una violazione: circa 6,5 milioni di dollari in media (oltre il 60% in più rispetto ad altri ambiti presi in considerazione nello studio).

Le violazioni malevole sono una minaccia crescente e quelle accidentali sono ancora comuni

Dalla ricerca è emerso che le violazioni di dati derivanti da attacchi informatici malevoli sono non solo le più comuni, ma anche le più costose.

Alle aziende coinvolte nello studio, una violazione malevola costa in media 4,45 milioni di dollari, cioè circa 1 milione in più rispetto a una violazione dovuta a cause accidentali, come anomalie nei sistemi o errori umani. Queste violazioni rappresentano una minaccia crescente: la percentuale di attacchi malevoli o criminali come causa principale di una violazione di dati è passata dal 42% al 51% nei sei anni presi in considerazione nello studio (con un aumento del 21%).

Tuttavia, le violazioni accidentali dovute a errori umani o anomalie nei sistemi sono risultate essere la causa di quasi metà (49%) delle violazioni di dati, comportando un costo per le aziende rispettivamente di 3,50 e 3,24 milioni di dollari. Queste violazioni dovute a errori umani o meccanici rappresentano però un'occasione di miglioramento, che può essere implementato attraverso corsi di security awareness, investimenti in strumenti tecnologici e servizi volti a identificare in anticipo le violazioni accidentali. Una particolare area di interesse è l'errata configurazione dei server cloud che, secondo la IBM X-Force Threat Intelligence Index[5] ha comportato un'esposizione di 990 milioni di dati nel 2018, rappresentando il 43% della totalità dei dati persi di tutto l'anno.

La risposta alle violazioni rimane il miglior modo di risparmiare

Durante gli ultimi 14 anni, il Ponemon Institute ha analizzato i fattori che incidono sull'aumento o la

diminuzione del costo di una violazione ed è stato rilevato che la velocità e l'efficienza di risposta di un'azienda a una violazione ha un grandissimo impatto sui costi complessivi.

Lo studio condotto quest'anno ha rilevato che il ciclo di vita medio di una violazione è di 279 giorni. Le aziende ne impiegano 206 per identificare una violazione dopo che è avvenuta, e altri 73 sono necessari per contenere i danni. Tuttavia, le aziende coinvolte nello studio che sono state in grado di rilevare e contenere una violazione in meno di 200 giorni hanno speso 1,2 milioni in meno rispetto al costo totale medio di una violazione.

Concentrarsi subito sulla risposta agli incidenti può quindi aiutare a ridurne i tempi e, inoltre, sempre secondo lo studio, queste misure hanno anche una correlazione diretta con i costi complessivi. Poter contare su un team e su piani di risposta agli incidenti sono due dei maggiori fattori di risparmio che emergono dallo studio. Le aziende che avevano messo in atto entrambe le misure hanno speso in media 1,23 milioni in meno rispetto alle aziende che non potevano contare su nessuna delle due (3,51 milioni contro 4,74 milioni).

Altri fattori che hanno avuto un impatto sui costi di una violazione sostenuti dalle aziende nello studio sono:

- numero di dati compromessi: ogni dato perso o rubato a causa di una violazione costa alle aziende in media 150 dollari;
- le aziende che avevano messo pienamente in atto tecnologie per l'automazione della sicurezza hanno dovuto sostenere circa la metà dei costi di una violazione (in media 2,65 milioni di dollari) rispetto a quelle che non utilizzavano questo tipo di tecnologie (in media 5,16 milioni di dollari);
- anche l'utilizzo dell'encryption è risultato essere uno dei maggiori fattori di risparmio, riducendo il costo totale di una violazione di 360.000 dollari;
- le violazioni derivanti da terze parti, come partner o fornitori, costano alle aziende 370.000 dollari in più della media, il che evidenzia l'importanza di controllare attentamente la sicurezza delle aziende con cui si collabora, di allineare gli standard di sicurezza e monitorare attivamente l'accesso di terzi.
-

Trend nazionali e di settore

All'interno dello studio 2019 Cost of a Data Breach Report si possono esaminare anche i costi di violazioni di dati in diversi settori e nazioni.

IBM Security

IBM Security offre uno dei portfolio 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 soluzione 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.

[1]Confronto tra il costo medio globale di una violazione di dati del Rapporto Cost of Data Breach del 2019 rispetto a quello del 2014.

[2] Analisi di IBM basate sui dati del Report Cost of a Data Breach Report

[3] Il perimetro del report e le metodologie impiegate sono descritte all'interno del rapporto.

[4] I calcoli dei costi di Mega breach si basano su un'analisi di 14 aziende, applicando un approccio analitico Monte-Carlo per simulare risultati di maggiore rilevanza statistica.

[5] IBM X-Force Threat Intelligence Index 2019

Contatti

Claudia Ruffini

IBM Media Relations +393356325093cla@it.ibm.com

Alessandro Ferrari

IBM Media Relations +393484554535ale_federferrari@it.ibm.com