Studio IBM: il costo delle violazioni dei dati ha raggiunto un picco record durante la pandemia

• Le aziende pagano in media 4.24 milioni di dollari per incidente, il costo più alto mai registrato in 17 anni • In Italia, rubati quasi 24mila record nel 2020 e il costo complessivo per le violazioni è salito a €3,03 milioni • L'adozione di intelligenza artificiale, cloud ibrido e approccio "Zero Trust" aiuta ad abbassare i costi

28 luglio 2021 – Le violazioni dei dati costano alle aziende 4,24 milioni di dollari in media per ogni incidente: questa la principale evidenza dell'ultimo Cost of a Data Breach Report, rilasciato oggi da IBM Security. Si tratta del costo più alto per singola violazione emerso dal 2004, anno in cui è stato pubblicato il primo report. Lo studio, basato su un'analisi approfondita di reali violazioni di dati subite da oltre 500 organizzazioni, suggerisce dunque che gli incidenti di security sono diventati più costosi, con un aumento della spesa del 10% rispetto all'anno precedente, e più difficili da contenere, soprattutto a causa dei drastici cambiamenti indotti dalla pandemia.

Nel 2020, le aziende sono state costrette a modificare rapidamente il proprio approccio alla tecnologia, incoraggiando o obbligando i dipendenti a ricorrere al lavoro da remoto durante la pandemia e il 60% delle imprese si è spostato verso un approccio cloud-based per condurre le proprie attività[1]. I dati pubblicati oggi evidenziano, però, che la security potrebbe non essersi adeguata altrettanto velocemente, ponendo un freno alla capacità delle organizzazioni di rispondere alle violazioni dei dati.

Lo studio annuale Cost of a Data Breach, condotto da Ponemon Institute e promosso da IBM Security, che ne ha analizzato i dati, ha identificato alcuni trend significativi:

- **Impatto del lavoro a distanza.** Il rapido passaggio delle attività lavorative verso lo smart-working sembrerebbe aver causato data breach più costosi: oltre 1 milione di dollari in più in media quando il lavoro remoto è stato indicato come causa dell'evento dalle aziende analizzate, rispetto alle violazioni con altri vettori (4,96 dollari contro 3,89 milioni di dollari per ogni violazione) [2].
- **I costi delle violazioni in ambito sanitario sono aumentati:** i settori che hanno affrontato enormi cambiamenti operativi durante la pandemia (tra cui sanità, vendita al dettaglio, produzione e distribuzione di prodotti di consumo) hanno anche sperimentato un crescente aumento della spesa per i data breach. Il settore sanitario è quello che paga il prezzo di gran lunga più caro, con 9,23 milioni di dollari per incidente - un aumento di 2 milioni di dollari rispetto all'anno precedente.
- **Credenziali compromesse portano a dati compromessi:** Le credenziali utente rubate sono state la causa principale delle violazioni. Allo stesso tempo, i dati personali degli utenti (come nome, e-mail, password) sono stati tra le informazioni più comunemente esposte, presenti nel 44% delle violazioni analizzate. La combinazione tra questi fattori potrebbe causare un effetto a spirale in futuro, con username e password rubate che diventano potenziali agganci per portare a termine ulteriori aggressioni.
- **Approcci più evoluti nella mitigazione delle violazioni ne hanno ridotto i costi** : AI, security analytics e crittografia sono stati i primi tre fattori di mitigazione delle violazioni, dimostrando come queste tecnologie possano ridurre i costi per singolo attacco. Le aziende che si sono dotate preventivamente di questi strumenti hanno risparmiato tra 1,25 e 1,49 milioni di dollari rispetto alle organizzazioni che non ne hanno fatto un uso significativo. Per quanto riguarda i data breach basati sul cloud, le imprese con una strategia hybrid cloud hanno dovuto affrontare una spesa inferiore (3,61 milioni di dollari) rispetto alle organizzazioni che avevano adottato un approccio principalmente di cloud pubblico (4,80 milioni di dollari) o privato (4,55 milioni di dollari).

“L'aumento dei costi di data breach è un’altra spesa che si aggiunge a quelle che le aziende hanno dovuto affrontare, sulla scia dei rapidi cambiamenti causati dalla pandemia”, ha affermato Chris McCurdy, Vice President e General Manager, IBM Security. “*Tuttavia, sebbene i costi delle violazioni abbiano raggiunto un livello record nell’ultimo anno, lo studio ha anche mostrato segnali positivi rispetto all’adozione di tecnologie e approcci innovativi di cybersecurity, come l'AI, l'automation e l’approccio ‘Zero Trust’, che possono contribuire a ridurre il costo degli incidenti con ritorni anche per il futuro*.”

L’impatto del lavoro a distanza e della migrazione al cloud sui data breach

Con l’aumento delle interazioni digitali portato dalla pandemia, le organizzazioni hanno adottato il lavoro da remoto e il cloud per soddisfare la crescente domanda di attività online. Lo studio ha rilevato che tali fattori hanno avuto un impatto significativo sulle violazioni di dati: quasi il 20% delle organizzazioni analizzate dallo studio ha riferito che lo smart working è stato un fattore chiave nelle violazioni dei dati e che le violazioni causate da smart-working sono costate alle aziende 4,96 milioni di dollari, il 15% in più rispetto al costo medio.

Inoltre, le aziende intervistate che hanno subito una violazione durante un progetto di migrazione al cloud hanno affrontato un costo superiore del 18,8% rispetto alla media. Tuttavia, l’indagine ha anche rilevato che le organizzazioni più “mature” nella strategia di modernizzazione del cloud sono state in grado di identificare e rispondere più efficacemente agli incidenti, impiegando circa 77 giorni in meno rispetto alle imprese in fase iniziale di adozione. Infine, per le violazioni di dati avvenute sul cloud, le organizzazioni che hanno adottato un approccio hybrid cloud hanno dovuto affrontare una spesa più contenuta (3,61 milioni di dollari) rispetto alle imprese che avevano adottato un approccio principalmente di cloud pubblico (4,80 dollari) o privato (4,55 milioni di dollari).

Credenziali compromesse: un rischio crescente

Il rapporto ha anche fatto luce su un problema crescente: i dati dei consumatori, incluse le credenziali, compromessi durante un data breach possono poi diventare leva per propagare ulteriori attacchi. Se si considera che l’82% delle persone intervistate ammette di riutilizzare le password tra gli account, le credenziali compromesse sono sia la causa che l’effetto principale delle violazioni, un problema che rappresenta un rischio crescente per le aziende.

- **Dati personali esposti:** quasi la metà (44%) delle violazioni analizzate ha esposto i dati personali dei clienti, come nome, e-mail, password, o anche dati sanitari, rappresentando dunque il tipo più comune di informazione rubata.
- **Le informazioni personali costano di più:** la perdita di PII (Personal Identifiable Information) dei clienti è stata anche il tipo di violazione più costosa (180 dollari per record perso o rubato contro 161 dollari di media).
- **Metodo di attacco più comune**: le credenziali utente compromesse sono state il metodo più comune utilizzato come punto d'ingresso dagli aggressori (20% delle violazioni studiate).
- **Più lunghi da rilevare e contenere:** le violazioni frutto di credenziali compromesse sono state quelle che hanno richiesto più tempo per essere rilevate, 250 giorni contro i 212 di media.

Le aziende che si sono modernizzate hanno avuto costi di violazione inferiori

Se da un lato gli interventi informatici indotti dalla pandemia hanno portato ad un aumento dei costi dei data breach, dall’altro la mancanza di progetti di trasformazione digitale volti a modernizzare le business operations ha portato le aziende a sostenere costi effettivamente superiori per singola violazione di dati: 750.000 dollari in più nelle organizzazioni che non hanno avviato percorsi di trasformazione digitale a causa del COVID-19 (pari al 16,6% rispetto alla media).

Le aziende analizzate che hanno adottato un approccio alla security di tipo Zero Trust si sono trovate in una posizione privilegiata al momento di affrontare le violazioni dei dati. L'approccio Zero Trust opera sul presupposto che le identità degli utenti, o la rete stessa, possano essere già compromesse e si affida invece all'AI e agli analytics per convalidare continuamente le connessioni tra utenti, dati e risorse. Per le organizzazioni con una strategia matura Zero Trust, una violazione di dati è costata in media 3,28 milioni di dollari, 1,76 milioni di dollari in meno rispetto alle aziende che non avevano sviluppato questo approccio.

Il rapporto ha inoltre messo in luce un aumento dell'adozione della security automation rispetto agli anni precedenti, un trend che condurrà ad un risparmio significativo sui costi dei data breach. Circa il 65% delle aziende intervistate ha riferito di aver introdotto parzialmente o completamente soluzioni di automazione nei propri ambienti security, rispetto al 52% di due anni fa. Per le organizzazioni che hanno completato il processo di adozione di una strategia di security automation, ogni violazione è costata in media solo 2,90 milioni di dollari, mentre chi non ha adottato questo approccio ha pagato più del doppio, 6,71 milioni di dollari.

Gli investimenti in piani di risposta agli incidenti e team specializzati sono anche tra gli elementi che hanno contribuito alla riduzione dei costi di violazione dei dati. Le aziende con un team dedicato alla risposta agli incidenti e con un piano di risposta testato hanno riportato un costo medio di violazione di 3,25 milioni di dollari, mentre quelle che non avevano nessuno dei due hanno riportato un costo medio di 5,71 milioni di dollari (con una differenza del 54,9%).

Altri risultati del Report 2021 includono:

- **Tempo di risposta:** il tempo medio per rilevare e contenere una violazione dei dati è stato di 287 giorni (212 per rilevare, 75 per contenere), una settimana in più rispetto all'anno precedente.
- **Per settore:** il settore sanitario ha subito i data breach più costosi (9,23 milioni di dollari), seguito dal settore finanziario (5,72 milioni di dollari) e farmaceutico (5,04 milioni di dollari). Sebbene i costi complessivi siano inferiori, altri settori come retail, media e il settore pubblico hanno registrato un forte aumento dei costi rispetto all'anno precedente.
- **Per paese/regione:** le violazioni di dati più costose si sono verificate negli Stati Uniti con 9,05 milioni di dollari per incidente, seguiti dal Medio Oriente (6,93 milioni di dollari) e dal Canada (5,4 milioni di dollari).

Metodologia e altre statistiche

Il 2021 Cost of a Data Breach Report di IBM Security e Ponemon Institute si basa sull'analisi approfondita di violazioni di dati reali relativi a 100.000 record, subite da oltre 500 organizzazioni in tutto il mondo tra maggio 2020 e marzo 2021. Lo studio prende in considerazione centinaia di fattori di costo causati dagli incidenti di violazione dei dati, come quelli relativi alle attività legali, normative e tecniche e quelli dovuti alla perdita di brand equity, clienti e produttività dei dipendenti.

Il report completo è disponibile al seguente link: ibm.com/databreach

Iscriviti al webinar 2021 Cost of a Data Breach Report il 12 agosto alle 11 AM ET, qui: ibm.biz/CODBwebinar

IBM Security

IBM Security offre uno dei portfoli 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 Security X-Force, consente alle organizzazioni di gestire con efficacia i rischi cyber e difendersi dalle minacce emergenti. IBM gestisce una delle organizzazioni di ricerca, sviluppo e delivery di soluzioni di sicurezza più grandi al mondo, monitora oltre 150 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] IBM Institute for Business Value: COVID-19 and the future of business

[2]Costo medio di 4.96 milioni di dollari per le aziende intervistate per le quali il lavoro da remoto è stato un fattore vs. 3.89 milioni di dollari quando il lavoro da remote non è indicato come fattore

For further information: Ufficio stampa IBM Claudia Ruffini – cla@it.ibm.com – 335 6325093