IBM & Ponemon Institute: nel 2017 il costo di una violazione dei dati è sceso del 10% a livello globale

Il costo negli Stati Uniti ha continuato a crescere, mentre in Europa è sceso; le differenze normative possono influire drasticamente sui costi di violazione

Cambridge - 20 giu 2017: IBM Security ha annunciato oggi i risultati di uno studio globale che esplora le implicazioni e gli effetti delle violazioni dei dati sulle aziende di oggi. Sponsorizzato da IBM Security e condotto da Ponemon Institute, lo studio ha rilevato che il costo medio di una violazione dei dati è di 3,62 milioni di dollari a livello mondiale^[1], in calo del 10% rispetto ai risultati del 2016. Questa è la prima volta da quando è stato creato questo studio globale che si è registrata una diminuzione complessiva del costo. Secondo lo studio, queste violazioni costano alle aziende in media 141 dollari per record di dati perso o rubato.

Analizzando gli 11 Paesi e le 2 regioni presenti nel rapporto, [IBM Security](#) ha individuato una stretta correlazione tra la risposta ai requisiti normativi in Europa e il costo totale di una violazione dei dati. I Paesi europei hanno registrato un calo del 26% del costo totale di una violazione dei dati rispetto allo studio dello scorso anno. Le imprese in Europa operano in un contesto regolamentato centralmente, mentre negli Stati Uniti hanno esigenze diverse, con 48 dei 50 Stati con proprie leggi in materia di violazione dei dati. Rispondere a una moltitudine di requisiti normativi e segnalare il problema potenzialmente a milioni di consumatori può essere un compito estremamente costoso anche in termini di risorse.

Secondo lo studio [2017 Cost of Data Breach Study](#), "i vizi di conformità alle normative" e "la fretta di informare" le vittime senza aver ben compreso la portata della violazione sono tra i cinque principali motivi per cui il costo della violazione dei dati è aumentato negli Stati Uniti. Un confronto tra questi fattori suggerisce che le attività di normazione negli Stati Uniti potrebbero avere per le imprese un costo per ogni record superiore rispetto all'Europa. Ad esempio, le mancate conformità costano alle aziende statunitensi il 48% in più rispetto alle aziende europee, mentre la "fretta di informare" costa alle imprese statunitensi il 50% in più rispetto alle aziende europee. Inoltre, le società statunitensi hanno riferito di aver pagato in media oltre 690.000 dollari per le spese di notifica relative a una violazione, che è più del doppio rispetto a qualsiasi altro Paese esaminato nel rapporto.

"I nuovi requisiti normativi come il GDPR in Europa rappresentano una sfida e un'opportunità per le aziende che cercano di gestire meglio la loro risposta alle violazioni dei dati", ha dichiarato Wendi Whitmore, Global Lead, IBM X-Force Incident Response & Intelligence Services (IRIS). "Oggi più che mai è importante identificare rapidamente ciò che è successo, a cosa l'attaccante ha accesso, e come contenere e rimuovere il loro accesso è più importante che mai. È quindi fondamentale che le organizzazioni abbiano in essere un piano completo per rispondere rapidamente ed efficacemente agli incidenti qualora si verificano".

Il costo di una violazione di dati si riduce, ma non ovunque

Nello studio globale del 2017, il costo totale di una violazione dei dati è sceso, rispetto al 2016, a 3.62 milioni di dollari - in calo del 10 per cento da 4 milioni di dollari dello scorso anno. I Paesi europei hanno mediamente registrato una riduzione del costo di una violazione di dati rispetto al costo medio dei quattro anni precedenti. Così anche l'Australia, il Canada e il Brasile.

Tuttavia, altre regioni o Paesi hanno sperimentato un aumento di tali costi - ad esempio, il costo di una violazione dei dati negli Stati Uniti è stato di 7,35 milioni di dollari, in aumento del cinque per cento rispetto al 2016. E anche Medio Oriente, Giappone, Sudafrica e India hanno riportato un aumento rispetto al costo medio dei quattro anni precedenti.

Il tempo è denaro, le violazioni dei dati vanno arginate

Per il terzo anno consecutivo, emerge che avere un team di risposta a incidenti di sicurezza (IR) ha ridotto significativamente il costo di una violazione dei dati, permettendo di risparmiare più di 19 dollari per record perso o rubato. La velocità con cui una violazione può essere identificata e arginata è in gran parte dovuta all'utilizzo di un team IR e a un piano formale di risposta agli incidenti. I team IR possono aiutare le organizzazioni a muoversi correttamente per contenere una violazione e mitigare le possibili perdite.

Secondo lo studio, la rapidità con cui un incidente di violazione dei dati può essere arginato ha un impatto diretto sulle conseguenze finanziarie. Il costo di una violazione dei dati è stato di circa 1 milione di dollari inferiore alla media per le organizzazioni che hanno potuto contenere una violazione di dati in meno di trenta giorni rispetto a quelli che hanno impiegato più di 30 giorni. La velocità di risposta sarà sempre più critica in quanto il GDPR, attuato nel maggio 2018, richiederà alle organizzazioni che operano in Europa di segnalare le violazioni dei dati entro 72 ore, con il rischio di sostenere ammende fino al quattro per cento del loro fatturato annuo globale.

Secondo lo studio, le organizzazioni hanno impiegato, in media, più di sei mesi per identificare una violazione e almeno altri 66 giorni per contenere una violazione una volta scoperta.

Ulteriori risultati chiave dal rapporto “2017 Cost of Data Breach”

- **Le violazioni sanitarie sono le più costose:** per il settimo anno consecutivo, l'Healthcare si è rivelato come il settore d'industria più costoso con un costo pari a 380 dollari per ogni record violato, più che 2,5 volte la media globale di tutti i settori (141 dollari per ogni record).
- **Fattori principali che incidono sul maggiore costo di una violazione :** il ricorso a terze parti rappresenta il fattore principale che contribuisce ad aumentare il costo di una violazione dei dati. L'incidenza è di 17 dollari per record. Le organizzazioni devono quindi valutare la posizione di sicurezza dei loro fornitori esterni - che siano fornitori di servizi di payroll, di cloud o di CRM - per garantire la sicurezza dei dati dei propri dipendenti e clienti.
- **Fattori principali che riducono il costo di una violazione:** la risposta agli incidenti di sicurezza, la crittografia e una adeguata formazione del personale sono i fattori che hanno il maggior impatto sulla riduzione del costo di una violazione dei dati. Avere un team di risposta agli incidenti ha portato una riduzione del costo di 19 dollari per ogni record perso o rubato, seguito da un ampio uso della crittografia (riduzione di 16 dollari per ogni record) e la formazione dei dipendenti (riduzione di 12,50 dollari per ogni record).
- **Impatto positivo anche della resilienza:** i programmi di business continuity riducono notevolmente i costi di una violazione dei dati. Secondo lo studio di quest'anno, il costo complessivo medio di violazione dei dati giornalieri è stimato a 5.064 dollari. Le aziende che hanno un processo di disaster recovery gestito manualmente hanno registrato un costo medio stimato di 6.101 dollari al giorno. Al contrario, le

aziende che implementano un processo di disaster recovery automatizzato e che orchestrano la loro resilienza hanno registrato un costo medio molto più basso al giorno, pari a 4.041 dollari con una differenza netta del 39 per cento (o un risparmio sui costi di 1.969 dollari al giorno).

Scopri il costo di una violazione dei dati

Lo studio annuale Cost of Data Breach esamina i costi diretti e indiretti che le aziende sostengono per affrontare un singolo incidente di violazione dei dati. Attraverso interviste a oltre 400 aziende in 13 paesi, lo studio considera i costi associati alle attività di risposta alle violazioni, nonché i danni di immagine e il costo corrispondente alla perdita di business.

Il rapporto [2017 Cost of Data Breach Study: Global Overview](https://www.ibm.com/security/data-breach/) è disponibile al sito <https://www.ibm.com/security/data-breach/>

Sono inoltre disponibili rapporti specifici per i seguenti Paesi: Stati Uniti, Regno Unito, Germania, Australia, Francia, Brasile, Giappone, Italia, India, Arabia (Emirati Arabi Uniti e Arabia Saudita), Canada, Sudafrica e per la prima volta, la regione del Sud-Est asiatico (Singapore, Indonesia, Filippine e Malesia).

Per esplorare e interagire con i risultati dello studio 2017, utilizzate [IBM Security Data Breach Calculator](#), uno strumento interattivo che consente di analizzare i dati del rapporto e visualizzare il costo di una violazione di dati in specifici Paesi e settori e comprendere come diversi fattori influenzano i costi di ogni violazione.

Per iscriversi al seminario web di IBM Security e Ponemon Institute "Comprendere le violazioni della sicurezza di oggi: 2017 Cost of data breach study" che si terrà il 26 giugno 2017 alle ore 11:00 EDT visita il sito <https://ibm.co/2ssR8qz>.

Informazioni su IBM Security

IBM Security offre uno dei portafogli più avanzati e integrati di prodotti e servizi di sicurezza aziendale. Il portafoglio, in continua evoluzione grazie al team di Ricerca mondiale IBM X-Force®, consente alle organizzazioni di gestire efficacemente il rischio e di difendersi dalle minacce emergenti. IBM dispone di una delle più grandi organizzazioni al mondo di ricerca, sviluppo e delivery di servizi e soluzioni di sicurezza informatica, gestisce 35 miliardi di eventi di sicurezza al giorno in più di 130 paesi e ha ottenuto più di 3.000 brevetti di sicurezza in tutto il mondo. Per ulteriori informazioni, visitare il sito www.ibm.com/security, seguire [@ibmsecurity](#) su Twitter visitare il blog [IBM Security Intelligence](#).

[1] Ai fini dello studio Globale, le valute locali sono state convertite in dollari americani.

Contatti

Claudia Ruffini

IBM Media Relations +39 335 6325093 cla@it.ibm.com

<https://it.newsroom.ibm.com/2017-06-20-IBM-Ponemon-Institute-nel-2017-il-costo-di-una-violazione-dei-dati-e-sceso-del-10-a-livello-globale>