# Il costo della violazione dei dati a livello mondiale aumenta del 15 percento, secondo il Ponemon Institute

**Milano - 08 mag 2014:** Il Ponemon Institute ha pubblicato il suo studio annuale *Cost of Data Breach Study: Global Study,* sponsorizzato da IBM. Secondo lo studio, condotto su 314 aziende in 10 Paesi, nell'ultimo anno il costo totale medio per la violazione dei dati delle aziende è aumentato del 15%, raggiungendo i 3,5 milioni di dollari (le valute locali sono state convertite in dollari USA ai fini di comparazione). Lo studio ha rilevato inoltre che il costo sostenuto per ogni record perso o rubato, contenente informazioni riservate e sensibili, è aumentato di più del 9%, toccando i 145 dollari. Lo studio annuale di Ponemon, giunto alla nona edizione, è basato sulla raccolta di informazioni dettagliate sulle conseguenze finanziarie causate dalla violazione di dati. Ai fini di questa ricerca, una violazione dei dati si verifica quando dati sensibili, protetti o riservati vengono persi o rubati e messi a rischio. Il Ponemon Institute ha condotto 1.690 interviste con professionisti dell'IT, della compliance e della sicurezza delle informazioni, in rappresentanza di 314 organizzazioni, nei 10 Paesi seguenti: Stati Uniti, Regno Unito, Germania, Australia, Francia, Brasile, Giappone, Italia, India e, per la prima volta, la regione araba (un insieme di organizzazioni degli Emirati Arabi Uniti e dell'Arabia Saudita).

"L'obiettivo di questa ricerca non è solo aiutare le aziende a comprendere i tipi di violazioni dei dati che potrebbero pregiudicare la loro attività d'impresa, ma anche i costi potenziali e il modo migliore per assegnare le risorse alla prevenzione, al rilevamento e alla soluzione di un incidente", spiega il Dr. Larry Ponemon, presidente e fondatore del Ponemon Institute. "Il *Cost of Data Breach Study* di quest'anno fornisce inoltre un orientamento sulla probabilità che le imprese hanno di subire una violazione dei dati e sui possibili interventi per ridurne le conseguenze finanziarie".

Tutti gli intervistati sono figure che, per ruolo, conoscono le violazione dei dati subite dalle rispettive organizzazioni e i costi associati alle relative risoluzioni. Tutte le organizzazioni partecipanti hanno subito violazioni dei dati, da un livello minimo di circa 2.400 record compromessi a poco più di 100.000. Si definisce record compromesso quello che identifica il soggetto le cui informazioni sono state perse o rubate in una violazione dei dati.

"Le minacce per la cyber-sicurezza sono chiaramente motivo di preoccupazione crescente per le imprese, soprattutto se consideriamo quanto sono diventati persistenti i dati nell'era del cloud e del mobile computing", spiega Kris Lovejoy, General Manager, IBM Security Services Division. "Una violazione dei dati può comportare un danno enorme per l'impresa che la subisce, e va ben oltre gli aspetti finanziari. In gioco ci sono infatti la fidelizzazione dei clienti e la reputazione del marchio".

**I punti chiave emersi dallo Studio *Global Cost of Data Beach***

§ Le violazioni più onerose si sono verificate negli Stati Uniti e in Germania, con un costo rispettivamente di $201 e $195 per record compromesso. Le violazioni dei dati meno costose sono state in India e Brasile, rispettivamente a $51 e $70.

§ Le cause principali delle violazioni dei dati sono variano da Paese a Paese e possono influire sul costo della violazione. I Paesi nella Regione Araba e la Germania hanno avuto un maggior numero di violazioni dei dati causate da attacchi malevoli o di organizzazioni criminali. L'India ha avuto il maggior numero di violazioni dei dati causate da anomalie di sistema o di processo. L'errore umano è stato la causa più comune nel Regno Unito e in Brasile.

§ Le violazioni dei dati più onerose sono state quelle causate da attacchi malevoli o di organizzazioni criminali. Gli Stati Uniti e la Germania hanno sostenuto i costi più elevati.

§ L'approccio alla sicurezza è stato essenziale per ridurre il costo della violazione dei dati. In media, le aziende che hanno dichiarato di avere un solido livello di sicurezza sono riuscite a ridurre il costo addirittura di $14 per record.

§ L'integrazione della gestione della business continuity ha ridotto il costo della violazione dei dati, in media, di quasi $9 per record.

§ La nomina di un Chief Information Security Officer (CISO) alla guida di un team di gestione della violazione dei dati ha ridotto il costo di una violazione di oltre $6.

§ I Paesi che hanno perso il maggior numero di clienti in seguito a una violazione dei dati sono stati la Francia e l'Italia. Le aziende nella Regione Araba e in Brasile hanno subito la perdita di clienti minore.

§ La probabilità per un'azienda di subire una violazione dei dati che coinvolga 10.000 o più record riservati è del 22% nell'arco di due anni. I Paesi che hanno la maggiore probabilità di subire una violazione dei dati sono India, Brasile e Francia.

In linea con i precedenti studi *Cost of Data Breach*, la causa più comune di una violazione dei dati è l'attacco malevolo da parte di soggetti interni all'azienda o di un'organizzazione criminale. Nello studio di quest'anno, abbiamo chiesto alle aziende che cosa le preoccupa di più degli incidenti di sicurezza, quali investimenti stanno effettuando e l'eventuale esistenza di una strategia al riguardo.

Di seguito sono riportati alcuni dei risultati chiave:

§ Le minacce più grandi per le aziende partecipanti sono il malware e i tentativi di accesso subiti. Secondo lo studio, queste due minacce sono in aumento.

§ Solo il 38% delle aziende ha una strategia di sicurezza per proteggere la propria infrastruttura IT. Una percentuale più elevata (45%) ha in essere una strategia di sicurezza per proteggere il proprio patrimonio di informazioni.

§ Codice maligno e *probe* subiti hanno registrato il massimo aumento. Le aziende stimano che dovranno confrontarsi con una media di 17 codici maligni e 12 probe subiti ogni mese. Gli incidenti legati agli accessi non autorizzati sono rimasti sostanzialmente invariati e le aziende stimano che dovranno confrontarsi con una media di 10 incidenti di questo tipo ogni mese.

§ La maggior parte delle aziende (50%) ha scarsa o nessuna fiducia rispetto all'adeguatezza degli investimenti effettuati in risorse umane, processi e tecnologie per affrontare le minacce potenziali ed effettive.

§ Idealmente, le aziende vorrebbero investire 14 milioni di dollari nei prossimi 12 mesi per realizzare la propria strategia di sicurezza. Tuttavia, nell'arco dei prossimi 12 mesi, le aziende prevedono di disporre in media di circa metà di tale cifra, ovvero 7 milioni di dollari, da investire in strategia di sicurezza.

**Lo studio *The State of Advanced Persistent Threats***

Il Ponemon Institute ha pubblicato anche lo studio *The Economic Consequences of an APT Attack*, sponsorizzato da Trusteer, una società IBM. Questo nuovo rapporto fa parte di una ricerca più vasta, dal titolo *The State of Advanced Persistent Threats*, pubblicato nel dicembre 2013. La ricerca originale, condotta tra 755 professionisti della sicurezza IT statunitensi, conferma i risultati dello studio *The Cost of Data Breach*, nel quale gli attacchi mirati di organizzazioni criminali sono considerati dalla maggior parte degli intervistati la più grande minaccia per la rispettiva organizzazione. Un altro fatto avvalorante è la rilevazione che i danni in termini di reputazione rappresentano la componente o conseguenza più onerosa degli attacchi criminali, in particolare quelli che comportano il furto o l'uso improprio del patrimonio di informazioni. Gli intervistati di questo studio stimano che il costo medio di un'azienda per ristabilire la propria reputazione sia pari a 9,4 milioni di dollari.

**Ponemon Institute**

Il Ponemon Institute si dedica alla ricerca indipendente e alla formazione in materia di sicurezza delle informazioni, protezione dei dati,  privacy e prassi di gestione responsabile delle informazioni per imprese pubbliche e private di tutto il mondo. La sua missione è condurre studi empirici di alta qualità su tematiche critiche, che concernono la protezione del patrimonio di informazioni e l'infrastruttura IT. In qualità di membro del Council of American Survey Research Organizations (CASRO), è tenuto al rispetto di severi standard di riservatezza dei dati, privacy e ricerca etica. www.ponemon.org.

**About IBM Security**

IBM, con il suo ampio portfolio di soluzioni di sicurezza e di security intelligence, aiuta le aziende a proteggere in modo completo ed integrato il proprio patrimonio di persone, dati applicazioni e infrastrutture.  Tale portfolio comprende soluzioni di identity and access management, security information e event management, database security, application development, risk management, endpoint management, next-generation intrusion protection e altro ancora. IBM vanta uno delle maggiori gruppi al mondo per la ricerca e sviluppo in ambito sicurezza e un'importante rete di delivery globale per i servizi di sicurezza. IBM monitora 15 miliardi di eventi giornalieri relative alla sicurezza in più 130 paesi e detiene più di  3,000 brevetti in questo ambito.

Per maggiori informazioni, visitate : www.ibm.com/security.