Studio IBM & Ponemon Institute: aumentano i costi delle violazioni dei dati, ora 4 milioni di dollari per incidente

I risultati evidenziano che "il tempo è denaro" nella reazione a una violazione dei dati e che i team di risposta agli incidenti possono ottenere significativi risparmi di costi

Milano, 17 giugno 2016 – IBM Security ha annunciato i risultati di uno studio globale che analizza l'impatto economico delle violazioni dei dati sugli utili di un'azienda. Sponsorizzato da IBM e condotto dal Ponemon Institute, lo studio ha rilevato che il costo medio della violazione dei dati per le aziende intervistate è salito a 4 milioni di dollari, con un aumento del 29 percento dal 2013.

Gli incidenti di sicurezza informatica sono sempre più sofisticati e in continua crescita, registrando nel 2015 un incremento del 64 percento rispetto al 2014.[1] Parallelamente all'aumento della complessità delle minacce, anche il costo per le aziende cresce. Lo studio ha infatti quantificato la perdita delle aziende in 158 dollari per record compromesso. Le violazioni nei settori altamente regolamentati sono state ancora più onerose, raggiungendo nella sanità i 355 dollari per record, ben 100 dollari in più rispetto al 2013.

I tempi di risposta e l'assenza di pianificazione costano milioni alle imprese
Secondo lo studio, la presenza di un team di risposta agli incidenti è il fattore che più ha inciso sulla riduzione dei costi di una violazione dei dati - permettendo alle aziende di risparmiare in media quasi 400.000 dollari (o 16 dollari per record). In effetti, le attività di risposta agli incidenti, quali le indagini, le comunicazioni, le spese legali e i mandati delle autorità di regolamentazione, rappresentano il 59 percento del costo di una violazione dei dati[2]. La ragione di questi costi elevati potrebbe essere, in parte, legata al fatto che il 70 percento dei responsabili della sicurezza statunitensi riferisce di non avere in essere piani di risposta agli incidenti.

In assenza di un'adeguata pianificazione, il processo di risposta a una violazione è estremamente complesso e oneroso in termini di tempo. Tra le attività richieste, un'azienda deve:

- Collaborare con esperti della sicurezza interni o esterni per identificare rapidamente l'origine della violazione e arrestare un'ulteriore perdita di dati
- Dichiarare la violazione ai responsabili delle autorità di governo o regolatorie competenti, rispettando scadenze specifiche al fine di evitare potenziali multe
- Comunicare la violazione a clienti, partner e stakeholder
- Allestire l'eventuale supporto telefonico necessario e i servizi di monitoraggio del credito per i clienti interessati

Ciascuno di questi interventi richiede parecchie ore di impegno da parte dei componenti dello staff, sottraendo del tempo alle loro normali responsabilità, con spreco di risorse umane preziose per l'impresa.

I team di risposta agli incidenti possono velocizzare e ottimizzare il processo di risposta a una violazione, dal momento che sanno perfettamente ciò che le aziende devono fare una volta accertata la compromissione dei dati. Questi team affrontano tutti gli aspetti delle attività di sicurezza e del ciclo di vita della risposta, dall'aiuto nella risoluzione dell'incidente, ai problemi specifici per il settore d'industria, fino alla compliance normativa. Inoltre, le tecnologie di risposta agli incidenti possono automatizzare questo processo, per accelerare ulteriormente l'efficienza e i tempi di risposta.

Lo studio ha riscontrato inoltre che tempi più lunghi di rilevamento e contenimento di una violazione dei dati determinano un aumento dei costi di risoluzione. Mentre le violazioni identificate in meno di 100 giorni

[1] X-Force IBM Cyber Security Intelligence Index, April 2016
[2] The Cyber Resilient Organization: Learning to Thrive Against Threats, Ponemon Institute, 2015

costano alle aziende in media 3,23 milioni di dollari, quelle individuate dopo i 100 giorni costano in media 4,38 milioni di dollari, più di 1 milione di dollari aggiuntivi.

Secondo lo studio, il tempo richiesto in media per identificare una violazione è stato stimato in 201 giorni, mentre il tempo medio di contenimento è stato stimato in 70 giorni.

Lo studio ha riscontrato inoltre che le aziende con processi in essere di Business Continuity Management (BCM) hanno rilevato e contenuto le violazioni con maggiore rapidità, scoprendo le violazioni 52 giorni prima e contenendole con 36 giorni in meno rispetto alle aziende prive di un BCM.

Analisi del costo di una violazione dei dati
L'annuale studio Cost of a Data Breach esamina i costi diretti e indiretti a carico delle aziende nella gestione di un singolo incidente di violazione dei dati. Grazie ad approfondite interviste con quasi 400 aziende in varie parti del mondo, lo studio comprende i costi associati alle attività di risposta alle violazioni, nonché il danno d'immagine e il costo di perdita di business.

"Dopo anni di studio di esperienze di violazioni di dati in oltre 2000 organizzazioni in ogni settore, riscontriamo che, nell'era del cybercrime, le violazioni rappresentano un 'costo sistematico per le imprese", spiega il Dr. Larry Ponemon. "Le evidenze dimostrano che si tratta di un costo permanente, con cui le organizzazioni devono essere pronte a confrontarsi e che devono inserire nelle loro strategie di protezione dei dati".

Per maggiori dettagli sullo studio, il rapporto integrale è disponibile sulla IBM X-Force Research Library, dove sono disponibili anche gli studi specifici per i singoli Paesi: Stati Uniti, Regno Unito, Germania, Australia, Francia, Brasile, Giappone, Italia, India, regione araba (Emirati Arabi Uniti e Arabia Saudita), Canada e Sudafrica.

Quest'anno IBM ha aumentato gli investimenti nel mercato delle soluzioni e servizi per la risposta agli incidenti con l'acquisizione di Resilient Systems. La Incident Response Platform (IRP) di Resilient consente ai team della sicurezza di analizzare, rispondere e mitigare gli incidenti in modo più rapido ed efficiente. La nuova versione della piattaforma, annunciata in questi giorni, comprende Resilient Incident Visualization, che visualizza graficamente le relazioni tra gli indicatori di compromissione (Indicators of Compromise, IOC) e gli incidenti nell'ambiente di un'organizzazione.

"La quantità di tempo, impegno e costi dedicata dalle aziende in conseguenza di una violazione dei dati può essere devastante e, sfortunatamente, la maggior parte di esse non dispone ancora di un piano per affrontare con efficienza questo processo", commenta Ted Julian, Vice President di Resilient, IBM Company. "Anche se il rischio è inevitabile, avere un piano di risposta agli incidenti coordinato e automatizzato, nonché l'accesso alle risorse con le giuste competenze, può influire enormemente sull'impatto che un evento di sicurezza ha su un'azienda".

IBM ha annunciato anche X-Force Incident Response Services, che comprende servizi di consulenza e sicurezza gestita, per aiutare i clienti ad affrontare tutti gli aspetti della risposta a una violazione informatica.

IBM Security
IBM Security offre uno dei portafogli di offerta più evoluti e integrati di prodotti e servizi per la sicurezza aziendale. Il portafoglio, supportato dal team di Ricerca noto in tutto il mondo IBM X-Force®, consente alle organizzazioni di gestire con efficacia il rischio e di difendersi dalle minacce emergenti. IBM gestisce una delle più vaste organizzazioni di ricerca, sviluppo e delivery in materia di sicurezza del mondo, monitora 20 miliardi di eventi di sicurezza al giorno in oltre 130 paesi, e detiene più di 3.000 brevetti in materia. Per ulteriori informazioni, visitate il sito www.ibm.com/security, seguite @IBMSecurity su Twitter, oppure visitate il blog di IBM Security Intelligence.

IBM Resiliency Services
IBM Resiliency Services offre un portafoglio innovativo di soluzioni e servizi di resilienza, incluso Business Continuity Management, con un ampio supporto che copre ogni aspetto dell'interruzione dell'attività aziendale. Oggi, più di 6000 professionisti della resilienza IBM progettano, realizzano e gestiscono funzionalità cloud leader di settore, per aiutare le aziende a mantenere la continuità delle attività aziendali e a migliorare la resilienza complessiva dell'organizzazione. Per maggiori informazioni, visitate il sito http://ibm.co/1cqLDOz e seguite @IBMServices.

Ufficio Stampa IBM
Claudia Ruffini, cla@it.ibm.com
02 596 25793; 335 6325093