

Studio IBM: dimezzato il numero di attacchi informatici diretti al settore retail

In calo l'attività dei ladri informatici nei due principali giorni dello shopping dell'anno, ma ammontano a 61 milioni i dati clienti sottratti nel 2014

Milano - 08 gen 2015: Secondo risultati recentemente pubblicati da IBM, nonostante la riduzione del 50 per cento degli attacchi informatici perpetrati nei confronti dei retailer statunitensi, il numero di dati rubati si continua a mantenere a livelli di record. I ricercatori di IBM Security riferiscono che, nel 2014, gli hacker sono riusciti comunque a rubare alle aziende del retail più di 61 milioni di dati clienti, nonostante la diminuzione degli attacchi, a dimostrazione del crescente grado di sofisticatezza e di efficienza del crimine informatico. Contrariamente alle attese, nel 2014 la maggior parte degli hacker ha ridotto gli attacchi intorno al Black Friday e al Cyber Monday, i giorni di maggiore picco di spesa nel retail. Gli studi IBM [2014 Retail Research and Intelligence Report](#) e [Holiday Trends: Black Friday/Cyber Monday Research and Intelligence Report](#) sono stati condotti dagli analisti del team Managed Security Services di IBM, che monitorano più di 20 miliardi di incidenti di sicurezza ogni giorno.

Secondo queste ricerche, gli hacker stanno diventando sempre più sofisticati e utilizzano nuove tecniche per ottenere enormi quantità di dati riservati con modalità sempre più efficienti. Dal 2012 il numero di violazioni segnalate dai retailer è sceso del 50 per cento. Nonostante questo calo, gli autori dei cyber-attacchi sono riusciti a colpire, con ogni singolo attacco, un numero molto maggiore di vittime.

“La minaccia proveniente dalla criminalità informatica organizzata rimane la principale sfida di sicurezza per il settore retail”, commenta Kris Lovejoy, General Manager, IBM Security Services. “È essenziale che i responsabili della sicurezza, e i Chief Information Security Officer (CISO) in particolare, si assicurino di disporre delle persone, dei processi e della tecnologia necessarie per affrontare queste minacce in espansione”.

Black Friday e Cyber Monday

Anziché intensificarla, i cyber-criminali hanno ridotto la loro attività in tutti i settori durante il Black Friday e il Cyber Monday, i due principali giorni di shopping dell'anno secondo il [Digital Analytics Benchmark](#) di IBM. Se si osserva il periodo di due settimane che va dal 24 novembre al 5 dicembre, i dati evidenziano, rispetto a tutti i settori di industria, quanto segue:

- Il numero di cyber-attacchi giornalieri è risultato pari a 3.043, quasi un terzo in meno rispetto alla media di 4.200 registrata nello stesso periodo del 2013.
- Dal 2013 al 2014, il numero di violazioni è diminuito di oltre il 50 per cento per il Black Friday e il Cyber Monday.
- Nel 2013 vi sono state più di 20 violazioni divulgate, incluse diverse violazioni di grandi dimensioni, determinando un netto aumento del numero di dati compromessi, che ha sfiorato i 4 milioni.
- Nello stesso periodo del 2014, sono state divulgate 10 violazioni, che si sono tradotte in poco più di 72.000 dati compromessi.

Nonostante questa diminuzione nei crimini informatici, i settori delle vendite al dettaglio e delle vendite all'ingrosso sono stati i principali bersagli degli hacker nel 2014, conseguenza dell'ondata di incidenti di alto

profilo che hanno colpito rivenditori di marca. Nei due anni precedenti, il settore manifatturiero è risultato il primo dei cinque settori presi di mira, mentre quelli delle vendite al dettaglio e all'ingrosso si trovavano in ultima posizione. In quest'ultimo anno, la modalità di attacco principale è stata l'accesso non autorizzato tramite attacchi di tipo "Secure Shell Brute Force", che hanno superato i codici malevoli, la scelta di punta nel 2012 e nel 2013.

Le violazioni principali mettono in ombra una tendenza in crescita

Gli hacker sono riusciti a impossessarsi di più di 61 milioni di dati nel 2014, in calo rispetto ai quasi 73 milioni nel 2013. Tuttavia, se si restringono i dati ai soli incidenti che coinvolgono meno di 10 milioni di record (ossia escludendo i due attacchi principali nel corso di questo periodo, Target Corporation e The Home Depot), questi ci raccontano una storia diversa: il numero di record del retail compromessi nel 2014 è aumentato di più del 43 per cento, rispetto al 2013.

Metodi di attacco sofisticati

Anche se vi è stato un aumento del numero di attacchi di malware ai Point of Sale (POS), la grande maggioranza di incidenti diretti al settore delle vendite al dettaglio è stata causata da Command Injection o SQL injection. La complessità delle istruzioni SQL e la mancata validazione dei dati da parte degli amministratori della sicurezza hanno reso i database del settore retail un bersaglio primario. Nel corso del 2014, il metodo di Command Injection è stato usato in quasi 6.000 attacchi nei confronti di retailers. Tra gli altri metodi figurano Shellshock, oltre a malware per POS come BlackPOS, Dexter, vSkimmer, Alina e Citadel.

I dati relativi al numero di record compromessi e alle violazioni divulgate sono stati analizzati dagli esperti della sicurezza IBM e resi pubblici attraverso il Privacy Rights Clearinghouse. Altri dati provenivano dal team Managed Security Services di IBM. Per il rapporto completo, [cliccare qui](#).

IBM Security

La piattaforma di sicurezza di IBM fornisce la security intelligence necessaria per aiutare le aziende a proteggere in modo onnicomprensivo i propri dipendenti, dati, applicazioni e infrastrutture. IBM offre soluzioni per la gestione delle identità e degli accessi, la gestione delle informazioni e degli eventi di sicurezza, la sicurezza dei database, lo sviluppo delle applicazioni, la gestione del rischio, la gestione degli endpoint, la protezione dalle intrusioni di *next generation* e molto altro. IBM gestisce una delle maggiori organizzazioni al mondo di ricerca e sviluppo in ambito security, e un'altrettanto vasta organizzazione globale per il delivery dei servizi di sicurezza.

Per ulteriori informazioni, visitate il sito www.ibm.com/security, seguite @IBMSecurity su Twitter, oppure visitate il [blog](#) di IBM Security Intelligence.

Informazioni su IBM Security

Per ulteriori informazioni, visitate il sito www.ibm.com/security, seguite @IBMSecurity su Twitter, oppure visitate il [blog](#) di IBM Security Intelligence.
