# Data Breach Investigations Report 2019 (DBIR) di Verizon - Download

**Author :** Redazione

**Date :** 8 Luglio 2019


I C-Level - ovvero i dirigenti di alto livello, che hanno accesso ai dati aziendali più sensibili - sono diventati il bersaglio principale degli attacchi di social engineering, avverte il Data Breach Investigations Report 2019 (DBIR) di Verizon.

Rispetto agli anni precedenti, i senior executive corrono molto di più il rischio di essere vittime del social engineering: infatti, i dirigenti hanno 12 volte più probabilità di essere il target di incidenti correlati a questa tipologia di attacchi e 9 volte più probabilità di essere il target di vere e proprie violazioni - e la motivazione finanziaria rappresenta ancora il fattore determinante. Gli attacchi di social engineering a scopo economico (il 12% di tutte le violazioni analizzate) sono un elemento chiave del rapporto di quest'anno, evidenziando la necessità critica di garantire che i dipendenti di ogni livello vengano sensibilizzati sull'impatto potenziale della criminalità informatica.

"Le aziende utilizzano sempre più applicazioni edge-based per fornire informazioni e esperienza credibili. Dati della supply chain, video e altri dati critici, spesso personali, verranno assemblati e analizzati a una velocità sorprendente, cambiando il modo in cui le applicazioni utilizzano funzionalità di rete sicure" commenta George Fischer, presidente di Verizon Enterprise Solutions. " La sicurezza deve sempre avere un ruolo di primo piano quando si implementano queste nuove applicazioni e architetture".

"La manutenzione delle strumentazioni e la sicurezza delle reti sono fattori determinanti quando si tratta di ridurre i rischi. Tutto inizia con la comprensione della posizione di rischio e del panorama delle minacce, in modo da poter sviluppare e attuare un piano solido per proteggere la propria azienda dalla realtà del cybercrime. La conoscenza è potere, e il DBIR di Verizon offre alle organizzazioni grandi e piccole una panoramica completa sullo scenario delle minacce informatiche di oggi in modo che possano sviluppare rapidamente strategie di difesa efficaci".

Un attacco pretexting rivolto ai top manager può raccogliere grandi dividendi a causa dell’autorità - spesso incontrastata – dei dirigenti e del loro accesso privilegiato ai sistemi critici.

Con pochissimo tempo a loro disposizione e costantemente sotto pressione per le consegne, i senior executive esaminano rapidamente e fanno clic su un’email prima di passare alla successiva (o hanno assistenti che gestiscono la posta elettronica per conto loro), rendendo più probabile l’apertura di email sospette.

Il crescente successo di attacchi di ingegneria sociale come quelli tramite BEC (Business Email Compromise) - che rappresentano 370 incidenti, di cui 248 sfociati in violazioni accertate - può essere collegato alla malsana combinazione di un ambiente di lavoro stressante unito ad una mancanza di formazione mirata sui rischi del cyber crime.

I risultati di quest'anno evidenziano anche come la crescente tendenza a condividere e archiviare le informazioni all'interno di soluzioni basate su cloud stia esponendo le aziende a ulteriori rischi per la sicurezza. L'analisi ha rilevato un sostanziale orientamento verso la violazione degli account e-mail su cloud attraverso l'uso di credenziali rubate. Inoltre, gli “errori di configurazione” nel cloud sono in aumento anno dopo anno.

L'errata configurazione ha infatti portato a una serie di massicce violazioni dello storage di file basato su cloud, esponendo almeno 60 milioni di casi analizzati nel dataset del DBIR, pari al 61% delle violazioni causate da errori.

Bryan Sartin, executive director security professional services di Verizon, ha dichiarato " Le aziende stanno adottando nuove modalità di lavoro digitale, tuttavia molte società non sono consapevoli dei nuovi rischi per la sicurezza a cui sono esposte. È importante poter accedere a strumenti di cyber detection per ottenere una panoramica quotidiana della loro posizione di sicurezza, supportata da statistiche sulle più recenti minacce informatiche. La sicurezza deve essere vista come una risorsa strategica flessibile e intelligente che supporta costantemente le aziende e che ha un impatto sui risultati economici.”

## Un riassunto dei dati più scottanti

Il DBIR offre un’analisi esaustiva e basata sui dati del panorama delle minacce informatiche. Tra i dati più significativi dell’edizione 2019 del report:

- **Nuove analisi dell’FBI Internet Crime Complaint Center (IC3):** questa sezione fornisce un'analisi approfondita dell'impatto degli attacchi Business Email Compromises (BEC) e Computer Data Breaches (CDB). I risultati evidenziano come la Compromissione delle Mail aziendali possa essere risolta. Infatti, nei casi in cui il Recovery Asset Team di IC3, in collaborazione con la banca di destinazione, è intervenuto in episodi di Business Email Compromise, metà degli indirizzi e-mail commerciali con sede negli Stati Uniti ha recuperato o congelato il 99% del denaro, mentre solo nel 9% dei casi non è stato possibile recuperare nulla.
- **Gli attacchi al personale delle Risorse Umane sono diminuiti rispetto all'anno scorso:** I risultati hanno evidenziato come quest'anno l'impatto sul settore HR sia diminuito di 6 volte rispetto all'anno scorso. Sono infatti diminuite e quasi scomparse dal dataset del DBIR le truffe che sfruttano i moduli fiscali W-2 (*ndt:* utilizzati negli Stati Uniti per riportare i salari corrisposti ai dipendenti e le imposte trattenute).

- **Le tecnologie di pagamento Chip e Pin hanno raggiunto livelli di sicurezza significativi**: Il numero di violazioni relative alle carte di pagamento realizzate tramite la compromissione dei terminali fisici è in diminuzione rispetto a quelle relative alle applicazioni web.
- **Gli attacchi Ransomware sono ancora numerosi:** rappresentano quasi il 24% degli incidenti in cui è stato utilizzato un malware. Il Ransomware è diventato così comune che viene menzionato meno frequentemente nei media specializzati, a meno che non vi sia un target di alto profilo.
- **I tanto decantati attacchi di cripto-mining sono stati praticamente inesistenti:** Questo tipo di attacchi non sono rientrati tra le 10 principali varietà di malware e hanno rappresentato solo il 2% circa degli incidenti.
- **Le minacce provenienti dall'esterno rimangono quelle più diffuse**: gli attori esterni alle organizzazioni rappresentano ancora il principale motore degli attacchi (69% delle violazioni), contro un valore delle minacce provenienti dall'interno pari al 34%.

## I rischi più temibili, analizzati settore per settore

Anche quest'anno il report rivela le più temibili minacce che le aziende, settore per settore, si ritrovano a dover affrontare, e propone alcune linee guida per arginarle.
"Ogni anno analizziamo i dati e mettiamo in guardia le aziende sulle ultime tendenze del cybercrime, per consentire loro di rivedere le proprie strategie di sicurezza e proteggere in modo proattivo le attività dalle minacce informatiche. Tuttavia, anche se vediamo che i bersagli specifici e i luoghi degli attacchi cambiano, alla fine le tattiche utilizzate dai criminali rimangono invariate. È imperativo che le aziende, grandi e piccole, diano la priorità alla sicurezza della loro attività e alla protezione dei dati dei clienti. Spesso anche le pratiche di sicurezza di base e il buon senso scoraggiano la criminalità informatica", commenta Sartin.

I dati principali, relativi ai diversi settori, includono:

- **Istruzione:** si registra un considerevole cambio di rotta verso i crimini compiuti prevalentemente per ragioni economiche (80%). Il 35% delle violazione è dovuto ad errori umani e, circa un quarto è sorto da attacchi derivanti da applicazioni web, la maggior parte dei quali attribuibili all'utilizzo di credenziali rubate e utilizzate per accedere alle email su cloud.
- **Sanità:** Questo settore continua ad essere il solo a mostrare un incremento del numero di attacchi interni rispetto a quelli esterni (rispettivamente 60 e 40%). Non sorprende che i dati medici siano18 volte più a rischio di essere compromessi in questo settore, e quando un attore interno è coinvolto, è 14 volte più probabile che sia un professionista come un medico o un infermiere.
- **Manifatturiero:** per il secondo anno consecutivo, gli attacchi per ragioni economiche superano il cyber-spionaggio come ragione principale delle violazioni nel settore manifatturiero, e quest' anno con una percentuale ancor più significativa (68%).
- **Settore pubblico:** lo spionaggio informatico è aumentato quest'anno, tuttavia circa il 47% delle violazioni sono state scoperte solo anni dopo l'attacco inziale.
- **Retail:** dal 2015 le violazioni dei terminali di pagamento (PoS) sono diminuite di 10 volte, mentre oggi le violazioni delle applicazioni Web sono 13 volte più probabili.

(I risultati derivanti dall'analisi degli altri settori possono essere consultati all'interno del Report completo.)

**Più dati da un numero sempre più ampio di organizzazioni equivale ad avere ancora più insight**

"Siamo onorati quest'anno di avere incluso i dati provenienti dal numero più ampio di collaboratori rispetto a quanto fatto in passato, e abbiamo il piacere di dare per la prima volta il benvenuto all'FBI nel nostro Report", aggiunge Sartin. "Siamo in grado di fornire le preziose informazioni della nostra ricerca del DBIR come risultato della partecipazione dei nostri importanti collaboratori. Vorremmo a tal proposito ringraziarli tutti per il loro continuo supporto e dare il benvenuto a tutte le altre possibili collaborazioni da tutto il mondo che vorranno unirsi a noi per le prossime edizioni dello studio".

Questa è la 12esima edizione dei DBIR ed è, al momento, l'edizione con il maggior numero di collaboratori globali – 73 organizzazioni. Contiene le analisi di 41.686 incidenti relativi alla sicurezza che comprendono 2.013 violazioni accertate. Con l'aumento dei collaboratori, Verizon ha visto un aumento significativo di dati a disposizione, totalizzando circa 1,5 miliardi di data points of non-incident data.

Il rapporto di quest'anno introduce anche nuove metriche e ragionamenti che aiutano ad identificare quali settori possono essere considerati più redditizi per i criminali sia per l'aggressione sia per gli attacchi su larga scala. Questa analisi è basata su honeypot e dati di scansione Internet.

Il Report completo insieme all'Executive Summary, sono disponibili alla pagina del DBIR. Qualsiasi azienda che desideri diventare un collaboratore e apportare il suo contributo al DBIR, può contattare il seguente indirizzo e-mail: dbir@verizon.com per ricevere ulteriori informazioni.