Il **2024 Data Breach Investigations Report** (DBIR) di Verizon fornisce un'analisi approfondita sulle violazioni dei dati e sugli incidenti di sicurezza informatica a livello globale. Di seguito sono riportati i punti chiave del rapporto:

1. Statistiche globali sulle violazioni

- Nel periodo analizzato (novembre 2022 - ottobre 2023), sono stati esaminati 30.458 incidenti di sicurezza, di cui 10.626 violazioni confermate, un record storico.
- Gli attacchi sono avvenuti in 94 paesi e hanno coinvolto una vasta gamma di settori e dimensioni aziendali.

2. Principali vettori di attacco

- Circa un terzo delle violazioni ha coinvolto ransomware o tecniche di estorsione, che rappresentano una crescente minaccia. Sebbene gli attacchi puramente ransomware siano leggermente diminuiti (dal 23% al 32% delle violazioni complessive quando combinati con estorsioni), rappresentano ancora un rischio significativo per il 92% delle industrie.
- L'**exploit delle vulnerabilità** è aumentato del 180% rispetto all'anno precedente, con attacchi che sfruttano principalmente applicazioni web, VPN e condivisione desktop come vettori.

3. Fattori umani e terze parti

- Il **fattore umano** ha contribuito al 68% delle violazioni, evidenziando l'importanza della formazione sulla sicurezza.
- Le violazioni legate a **fornitori esterni** o a catene di fornitura software hanno visto una crescita significativa (15% delle violazioni, +68% rispetto all'anno precedente).

4. Minacce principali

- Il ransomware continua a dominare la scena, non solo con la crittografia dei dati ma anche con tecniche di estorsione senza crittografia. I criminali informatici hanno adottato nuove strategie per massimizzare i guadagni, con richieste di riscatto che rappresentano mediamente l'1,34% delle entrate dell'azienda vittima.
- Gli **errori umani** rappresentano il 28% delle violazioni, principalmente a causa di errori di configurazione o perdita di dati.

5. Settori e impatti regionali

- Tutti i settori sono stati colpiti, ma in particolare quello della **sanità**, delle **amministrazioni pubbliche** e dei **servizi finanziari**.
- Gli **attacchi statali** hanno rappresentato il 7% delle violazioni, con un focus particolare sulla raccolta di informazioni e spionaggio.

6. Tendenze emergenti

- La crescente diffusione di attacchi che sfruttano vulnerabilità zero-day (es. MOVEit) e le difficoltà di mitigazione tempestiva delle vulnerabilità stanno mettendo sotto pressione le organizzazioni.
- Gli attori malevoli statali e organizzazioni criminali continuano a utilizzare tattiche sofisticate, tra cui il furto di credenziali e la compromissione di applicazioni critiche.

In sintesi, il rapporto evidenzia come la cybercriminalità stia evolvendo con minacce sempre più sofisticate, con ransomware ed estorsioni che rimangono tra le maggiori preoccupazioni per le organizzazioni di tutto il mondo.