Riassunto Dettagliato del *2024 Data Breach Investigations Report*

Il *2024 Data Breach Investigations Report* (DBIR) di Verizon offre una panoramica dettagliata sullo stato della cybersecurity a livello globale, analizzando incidenti e violazioni di dati avvenuti tra il 2022 e il 2023. Il report si basa su oltre 23.000 incidenti di sicurezza, di cui più di 5.000 confermati come violazioni di dati. La pubblicazione mira a fornire una comprensione profonda delle tendenze emergenti, dei metodi di attacco più comuni e delle vulnerabilità che gli attaccanti sfruttano per colpire le organizzazioni.

Analisi Generale delle Minacce

- **Ransomware**: Continua a essere una delle principali minacce, rappresentando oltre il 25% delle violazioni analizzate. Gli attaccanti utilizzano spesso ransomware per cifrare i dati delle vittime e richiedere un riscatto in cambio della chiave di decrittazione. Il report evidenzia un aumento significativo degli attacchi che combinano ransomware e esfiltrazione dei dati, in cui gli aggressori minacciano di rendere pubblici i dati sensibili se il riscatto non viene pagato.
- **Zero-Day Exploits**: Gli exploit zero-day, ovvero vulnerabilità non ancora note al pubblico o non corrette dai fornitori, sono diventati una delle tecniche più utilizzate per ottenere un accesso iniziale alle reti aziendali. Questo tipo di attacco è spesso visto in combinazione con altre tecniche di social engineering, come il phishing, per massimizzare l'efficacia dell'attacco.
- **Attacchi di Estorsione**: Cresce la tendenza verso gli attacchi di estorsione che non si limitano a cifrare i dati, ma puntano anche a ottenere pagamenti sotto la minaccia di rilasciare informazioni compromettenti al pubblico o alla concorrenza. Questo tipo di attacco ha un impatto reputazionale

significativo per le organizzazioni colpite, oltre che un impatto finanziario.

Il Ruolo del Fattore Umano

Il report evidenzia che il "fattore umano" è implicato nel 68% delle violazioni di dati analizzate. Questo dato include errori umani, come l'invio di dati sensibili ai destinatari sbagliati, ma soprattutto attacchi che sfruttano la psicologia degli utenti per ottenere accesso ai sistemi. Di seguito, un approfondimento sui principali tipi di attacchi che sfruttano il fattore umano:

Focus su Phishing e Social Engineering

- **Phishing**:
    - Il phishing rimane una delle tecniche più efficaci per compromettere le credenziali degli utenti e ottenere un accesso iniziale. Nel report si evidenzia che il phishing rappresenta oltre il 40% dei metodi di ingresso iniziale utilizzati dagli attaccanti in violazioni confermate.
    - La maggior parte degli attacchi di phishing analizzati si svolge tramite e-mail, dove gli attaccanti inducono i destinatari a cliccare su link dannosi o a scaricare allegati infetti. Questi link possono reindirizzare le vittime a pagine web che imitano i portali aziendali, raccogliendo le credenziali di login.
    - Il report mette in evidenza un dato preoccupante: il tempo mediano impiegato da un utente per cliccare su un link di phishing dopo aver aperto un'e-mail sospetta è di soli 21 secondi. Successivamente, la maggior parte degli utenti inserisce le proprie credenziali entro i 28 secondi successivi. Questo dimostra quanto sia veloce la compromissione di un account se gli utenti non sono adeguatamente formati.
    - **Phishing Simulation Reports**: Le esercitazioni di phishing condotte dalle organizzazioni, menzionate nel

report, rivelano che solo il 20% dei dipendenti è in grado di riconoscere e segnalare correttamente i tentativi di phishing durante queste simulazioni. Questo dimostra la necessità di migliorare i programmi di formazione e sensibilizzazione.

- **Tecniche di Social Engineering più ampie**:
  - **Pretexting**: Questo tipo di attacco prevede che l'attaccante costruisca uno scenario credibile (pretesto) per ingannare la vittima e ottenere informazioni sensibili. Il pretexting è spesso utilizzato per compromettere account aziendali tramite Business Email Compromise (BEC). Ad esempio, un attaccante può fingersi un fornitore per convincere il reparto contabile a modificare i dettagli di pagamento, dirottando fondi verso conti controllati dagli aggressori.
  - Il pretexting è responsabile di circa il 25% degli attacchi finanziari analizzati nel report, con una perdita mediana di circa 50.000 dollari per incidente. Questo tipo di attacco sfrutta la fiducia dei dipendenti, che sono indotti a credere che l'interlocutore sia legittimo.
  - **BEC e Frodi Finanziarie**: Il Business Email Compromise (BEC) rappresenta una minaccia crescente. Gli attaccanti riescono a compromettere l'account e-mail di un dirigente o di un responsabile finanziario e utilizzano tale accesso per inviare messaggi falsi ai dipendenti, richiedendo trasferimenti di fondi. Questo metodo ha un impatto economico significativo, in quanto le vittime spesso non si rendono conto dell'inganno fino a quando i fondi non sono stati trasferiti.

Impatto Economico e Risposta delle Organizzazioni

- **Costo delle Violazioni**: Il report rileva che le violazioni di dati e gli attacchi ransomware comportano costi elevati per le aziende, non solo in termini di riscatto richiesto, ma anche per i costi legati al ripristino dei sistemi, alla perdita di produttività

e al danno reputazionale. Il costo mediano di un riscatto richiesto negli attacchi ransomware analizzati è di 200.000 dollari, ma può superare il milione di dollari per le organizzazioni di grandi dimensioni.
- **Preparazione e Risposta agli Incidenti**: Le organizzazioni che avevano un piano di risposta agli incidenti sono state in grado di mitigare i danni più rapidamente, limitando la propagazione del ransomware e riducendo i tempi di inattività. Tuttavia, molte organizzazioni si sono trovate impreparate, soprattutto di fronte ad attacchi che combinano tecniche avanzate di social engineering e attacchi zero-day.

Raccomandazioni per la Mitigazione

Il report fornisce anche una serie di raccomandazioni per migliorare la sicurezza e la resilienza delle organizzazioni contro minacce come phishing, pretexting e ransomware:

- **Formazione Continua**: Implementare programmi di formazione regolari per i dipendenti, incentrati sul riconoscimento delle e-mail di phishing e delle tecniche di social engineering.
- **Multi-Factor Authentication (MFA)**: Abilitare l'autenticazione a più fattori su tutte le applicazioni critiche per ridurre il rischio di compromissione degli account.
- **Simulazioni di Phishing**: Eseguire esercitazioni di phishing regolari per valutare la preparazione dei dipendenti e identificare eventuali lacune nella consapevolezza della sicurezza.
- **Rafforzamento delle Politiche di Sicurezza**: Migliorare le politiche di gestione degli accessi e assicurarsi che i software siano aggiornati, riducendo le possibilità di sfruttamento di vulnerabilità conosciute.

Conclusione del Report

Il *2024 Data Breach Investigations Report* sottolinea che, nonostante i progressi tecnologici nella difesa contro le minacce informatiche, il fattore umano rimane una delle principali debolezze sfruttate dai cybercriminali. La capacità di un’organizzazione di rispondere rapidamente a un attacco dipende dalla consapevolezza dei propri dipendenti e dalla prontezza delle sue misure di sicurezza. Il report enfatizza l'importanza di un approccio proattivo alla sicurezza informatica, che combina tecnologie avanzate con una solida cultura della sicurezza all'interno dell'azienda.