

# Cybersecurity, allarme Verizon: "Boom di attacchi nell'ultimo anno"

24 maggio 2022 | 16.43

LETTURA: 3 minuti

Ali Neil all'Adnkronos: "Gli ultimi tre anni hanno messo le aziende di fronte a nuove sfide legate al modo di lavorare e alla gestione dei dati"



(Foto Ufficio Stampa Verizon)

E' un anno "senza precedenti" nella storia della **sicurezza informatica** quello analizzato l'edizione 2022 del **Data Breach Investigations Report di Verizon** appena reso noto e che registra, fra i dati "particolarmente allarmanti", un notevole aumento degli **attacchi ransomware** con un incremento pari al 13% in un solo anno. Si tratta della crescita analizzata da Verizon "maggiore rispetto agli ultimi 5 anni messi insieme". Dal Report, che fa luce su alcune delle principali questioni che interessano il panorama internazionale della **cybersecurity**, emerge che mentre i criminali cercano di sfruttare forme sempre più sofisticate di malware, il ransomware continua a rivelarsi particolarmente efficace nello sfruttamento e nella monetizzazione dell'accesso illegale alle informazioni private.

Anche la **criminalità organizzata**, secondo quanto rilevato dagli analisti di Verizon, continua a essere una forza pervasiva nel mondo della **sicurezza informatica**: circa 4 violazioni su 5

possono essere attribuite al crimine organizzato, e gli attori esterni risultano essere circa 4 volte più propensi a causare **violazioni** in un'organizzazione rispetto agli attori interni. Le crescenti tensioni geopolitiche stanno anche portando a una maggiore sofisticatezza, visibilità e consapevolezza sugli attacchi informatici legati agli stati nazionali. "Gli ultimi tre anni hanno messo le aziende di fronte a nuove sfide legate al modo di lavorare e alla **gestione dei dati**, che i **cybercriminali** si sono dimostrati pronti a trasformare in opportunità di attacco, sfruttando ogni falla dei sistemi informatici" **sottolinea all'Adnkronos Ali Neil**, Director of International Security Solutions di Verizon Business.

"Per molte organizzazioni, in particolare quelle più piccole, l'implementazione di **misure di sicurezza** diffuse non è né conveniente né fattibile", tuttavia Neil osserva che "ogni miglioramento in quest'ambito, non importa quanto piccolo, può avere effetti altamente benefici quando si tratta di rilevare gli attacchi e scoraggiare i criminali informatici". "In un'era sempre più **digitale**, è importante che le aziende sfruttino tutte le misure di **sicurezza** possibili, educino il personale all'identificazione di potenziali minacce, ma - avverte ancora Neil - altrettanto importante è avere una mente aperta alle più recenti tecnologie per essere sempre un passo avanti rispetto ai potenziali aggressori".

Nel **Report di Verizon** gli analisti sottolineano che per molte aziende, l'ultimo anno è stato dominato anche dai problemi della catena di approvvigionamento e questa tendenza si è riflessa anche nel panorama della sicurezza informatica. Il 62% degli **incidenti di System Intrusion** si è verificato tramite il partner di un'organizzazione. La compromissione del partner giusto è un moltiplicatore di forza per i criminali informatici e mette in evidenza le sfide che molte organizzazioni devono affrontare per proteggere la propria catena di approvvigionamento. Parlando nel dettaglio dell'**elemento umano**, le persone rimangono - di gran lunga - **l'anello più debole** nelle difese della sicurezza informatica di un'organizzazione. Il 25% delle violazioni totali rilevate nel report 2022 è stato il risultato di **attacchi di social engineering** e, se si aggiungono **l'errore umano** e l'uso improprio, l'elemento umano rappresenta l'82% delle violazioni analizzate nell'ultimo anno. Dave Hylender, autore principale del Dbir, assicura che "giunto alla sua 15ª edizione, il Data Breach Investigations Report di Verizon rimane la massima autorità in termini di valutazione delle numerose minacce alla **sicurezza informatica** che le organizzazioni continuano a dover affrontare. E mentre il rapporto si è evoluto, i **fondamenti della sicurezza** rimangono gli stessi". "Bisogna valutare la propria esposizione, mitigare il rischio e - sottolinea Dave Hylender - prendere le misure appropriate. Come spesso accade, partire da basi solide è il fattore più importante per il successo". (di Andreana d'Aquino)