IN CIFRE:

Il moderno panorama delle vulnerabilità

ninjaOne

I CVE sono aumentati del

275% dal 2024

Verizon ha segnalato un sorprendente aumento del 180% degli sfruttamenti riusciti delle vulnerabilità nel 2024 e il loro report pubblicato il 23 aprile 2025 ha mostrato un ulteriore aumento del 34%.

Questo si traduce in 132 nuovi CVE ogni giorno con il 33% dei CVE classificati come ad alta o critica gravità

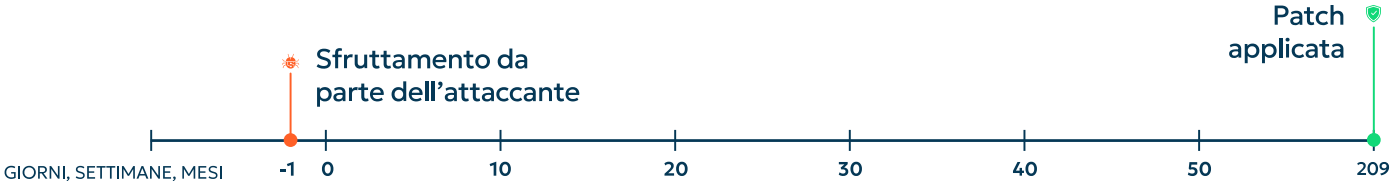
Verizon riferisce che:

solo il 54% delle vulnerabilità viene corretto entro 32 giorni,

ma la cosa più preoccupante è che il tempo medio di patching è di 209 giorni

I software enterprise hanno rappresentato il 44% degli zero-days nel 2024 e il 48% nel 2025.

Tra il 50% e il 61% delle nuove vulnerabilità viene sfruttato entro 48 ore dalla divulgazione



Il "tempo zero" qui si riferisce a quando una patch diventa disponibile. Gli attaccanti spesso sfruttano le vulnerabilità prima che esistano le patch, mentre le organizzazioni impiegano fino a **209 giorni** per distribuirle.

Vettori di attacco

Lo sfruttamento delle vulnerabilità è diventato comune come gli attacchi di phishing o di estrazione delle password. In effetti, Verizon ha segnalato che:

Lo sfruttamento delle vulnerabilità è cresciuto

x 8 passando dal **3%** al **22%**.

Un approccio migliore

NinjaOne Vulnerability Management, con la valutazione in tempo reale, elimina completamente i cicli di scansione, fornendo informazioni sempre aggiornate sulle vulnerabilità, senza interrompere le attività degli endpoint. Utilizzalo insieme al Patch Management autonomo di NinjaOne per creare un sistema di correzione a ciclo chiuso. Le informazioni sulle vulnerabilità, in questo modo, confluiscono direttamente nei flussi di lavoro di patching guidati da AI, accelerando la correzione e riducendo il rischio operativo.

Per saperne di più:
https://www.ninjaone.com/it/gestione-delle-vulnerabilita/