NEWS

Data Breach Scuole: Dati Gruppo Spaggiari in Vendita Online

Data pubblicazione: 25/08/2026

Autore: Giuseppe Daloiso

Contenuto

Maxi data breach colpisce Gruppo Spaggiari, gestore di ClasseViva, il registro elettronico più diffuso nelle scuole. Oltre 6TB di dati di studenti e docenti in vendita online a 50.000 dollari.

Maxi Data Breach: Attacco a Gruppo Spaggiari e Dati in Vendita

Un grave attacco informatico ha colpito Gruppo Spaggiari Parma, la società dietro ClasseViva, il registro elettronico più utilizzato nelle scuole italiane. Rivendicato il 20 agosto dal gruppo hacker xplOitrs, noto per operazioni ransomware, l'intrusione ha portato alla sottrazione di oltre 6 terabyte di dati. Queste informazioni sono state messe in vendita su un forum di hacking per 50.000 dollari. L'incidente, avvenuto a pochi giorni dall'inizio del nuovo anno scolastico, coinvolge un sistema con oltre quattro milioni di utenti, sollevando immediate preoccupazioni sulla sicurezza dei dati personali di studenti e docenti.

La Posizione di Gruppo Spaggiari: 'Solo Moduli Supplenze'?

Nonostante la gravità dell'attacco, Gruppo Spaggiari ha cercato di rassicurare l'opinione pubblica. L'azienda, contattata da Fanpage.it, ha dichiarato che i dati sottratti apparterrebbero a una piattaforma secondaria e consisterebbero 'perlopiù in moduli per le supplenze degli insegnanti'. Questa affermazione, tuttavia, contrasta con la natura delle operazioni ransomware, dove i cybercriminali mirano a sottrarre dati sensibili per chiedere riscatti. La vendita a 50.000 dollari suggerisce un valore percepito dagli hacker ben superiore a semplici moduli amministrativi, alimentando dubbi sulla reale entità e sensibilità delle informazioni compromesse.

Rischi Privacy e Obblighi Legali: Il Ruolo del Garante

L'attacco solleva serie questioni in termini di protezione dei dati personali e conformità al GDPR. Sebbene Gruppo Spaggiari minimizzi, la potenziale compromissione di informazioni relative a studenti e docenti potrebbe esporre milioni di utenti a rischi di furto d'identità, phishing o altre frodi. È fondamentale che l'azienda fornisca piena trasparenza sull'entità e la natura dei dati trafugati. Il Garante per la protezione dei dati personali dovrà avviare un'indagine per accertare eventuali violazioni e garantire misure adeguate per mitigare i rischi. L'episodio sottolinea l'urgente necessità di rafforzare la cybersecurity negli enti che gestiscono dati sensibili, specialmente nel settore scolastico italiano.