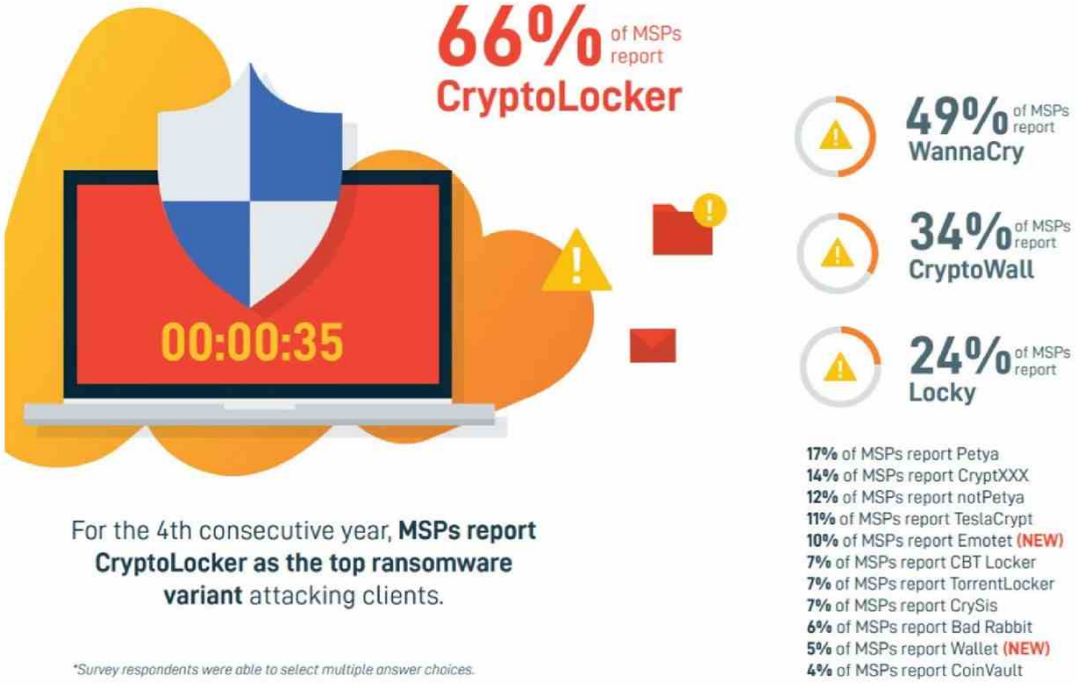
# Ransomware ai danni delle PMI: costi in crescita del 200%

securityopenlab.it/news/143/ransomware-ai-danni-delle-pmi-costi-in-crescita-del-200-.html

Una ricerca condotta da Datto rivela l'aumento degli attacchi ransomware e dei costi di interruzione dei servizi, che ora è 23 volte superiore alla richiesta di riscatto.

Gli attacchi di ransomware, già additati come principale minaccia del 2019, non accennano a smorzarsi. Una nuova analisi si concentra sui **costi alle aziende** causati da queste minacce informatiche. Comportano blocchi delle attività con costi e danni ingenti in termini di produttività, oltre che di reputazione.

A fare i conti dei danni è Datto, produttore di soluzioni per Managed Service Provider, nella relazione annuale "Global State of the Channel Ransomware Report". L'indagine ha coinvolto oltre 1.400 MSP, tra responsabili e decision maker, che gestiscono i sistemi IT di piccole e medie imprese. Emerge che la crescente frequenza degli attacchi ransomware nel 2019 ha portato a un **aumento dei costi pari al 200%** rispetto allo scorso anno.

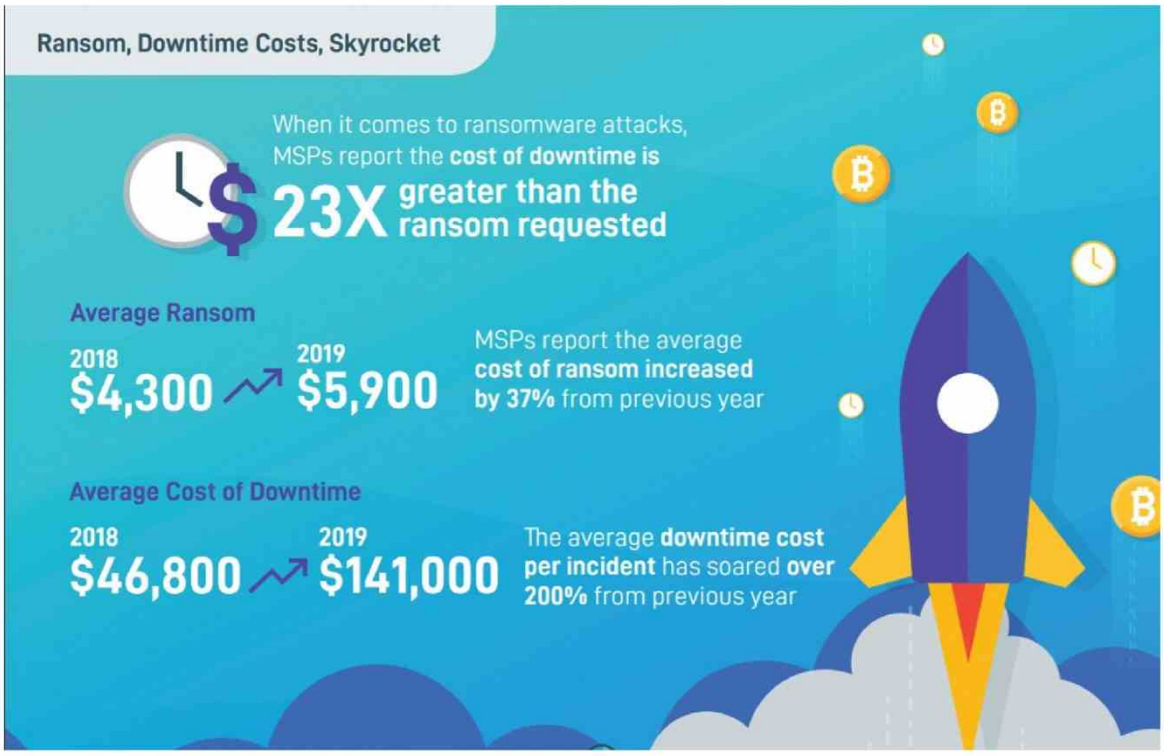



Il ransomware è un tipo di malware che rende inaccessibili i dati finché non viene corrisposto il pagamento di un riscatto. Sono prese di mira aziende di ogni dimensione, ma le PMI sono diventate il principale obiettivo dei criminali informatici.

Secondo i dati raccolti da Datto, l'85% degli MSP segnala attacchi contro le PMI negli ultimi due anni. Il dato è in aumento rispetto al 79% riferito nel 2018. Nonostante i dati, non tutti percepiscono il ransomware come minaccia. L'89% degli MSP afferma che il ransomware dovrebbe mettere le PMI in una posizione di allerta. Solo il 28% degli MSP dichiara consapevolezza e preoccupazione da parte delle PMI.

Preoccupazione o meno, il costo del ransomware è ingente. Il 64% degli MSP segnala perdite da mancata produttività da parte dei clienti (PMI). Il 45% segnala tempi di inattività potenzialmente pericolosi per il business. **Il costo medio di un downtime è 141.000 dollari**, in aumento di oltre il 200% rispetto al tempo medio di interruzione dello scorso anno, pari a 46.800 dollari.

Altro dato rilevante è che il costo dei tempi di inattività è **23 volte superiore alla richiesta media di riscatto**, pari a 5.900 dollari.




Per difendersi, la soluzione più efficace resta il Business Continuity e Disaster Recovery (BCDR). Secondo il 95% degli MSP, i clienti con soluzioni BCDR attive hanno meno probabilità di subire significativi fermi in caso di attacco. Per quattro MSP su cinque i clienti dotati di strumenti BCDR che hanno subito attacchi si sono ripresi in massimo 24 ore.

Il problema del downtime, infatti, è che la criticità aumenta quanto più si allungano i tempi di ripresa. È quindi vitale disporre di strumenti per affrontare un blocco e far ripartire i sistemi in tempi brevi. La proposta di Datto per le PMI comprende la soluzione di backup Datto BDR, e la piattaforma cloud Datto RMM per gestire il parco macchine.

In Italia l'adozione di queste soluzioni, distribuite da Achab, è ampia. All'evento europeo DattoCon 19 erano presenti 30 esponenti del Belpaese. Due sono stati premiati come migliori MSP: Kartenia e Sinergy Studio, entrambi partner di Achab.

Andrea Veca, CEO di Achab, commenta: “oggi gli MSP si trovano in una posizione unica per educare le PMI su come proteggersi da un attacco. I tempi di inattività dell'IT possono paralizzare una piccola impresa, è fondamentale avere un approccio proattivo alla sicurezza informatica. Proteggere i clienti SMB da attacchi come il ransomware richiede una comprensione della loro attività. Oltre a una preparazione dettagliata e al giusto mix di tecnologie. Man mano che gli

attacchi ransomware continuano ad aumentare di frequenza e raffinatezza, lavoreremo a stretto contatto con gli MSP. E con i partner come Datto per ridurre sia il rischio che l'impatto di un attacco."