Ransomware, troppe imprese vittime del sequestro digitale

13 aprile 2017

Il 93% degli IT reseller italiani ha dovuto effettuare almeno un intervento a causa del **ransomware**. Questi i risultati allarmanti di una ricerca condotta da **Achab** su oltre 200 fornitori di servizi IT che hanno dichiarato la loro esperienza con il ransomware.

C'è anche da considerare che meno di un incidente su 4 viene denunciato alle autorità. Il fenomeno è inarrestabile e vale un miliardo di dollari a livello globale.

Per ransomware, o **cryptolocker**, si intende quell'attacco informatico che cifra e tiene **in ostaggio** i dati delle aziende finché non viene pagato un **riscatto**.

Per via della sua natura e delle conseguenze che comporta, il ransomware è diventato un problema prioritario per chi si occupa di sicurezza informatica e di IT.

Considerando come oggi i dati vengono trattati nelle aziende e la centralità che rivestono in ogni tipo di attività, prendendoli in ostaggio il ransomware ha la capacità di distruggere qualsiasi realtà, anche grande, nel giro di pochi minuti.

E benché alcune aziende abbiano iniziato a utilizzare sistemi antivirus di nuova generazione e soluzioni di business continuity, sono ancora **troppe le impres**e impreparate all'eventualità di attacchi di questo tipo.

È il caso delle **piccole e medie imprese** dove spesso non c'è una figura dedicata a gestire l'IT e dove spesso si utilizzano sistemi informatici obsoleti e quindi inefficaci.

E di queste mancanze approfittano consapevolmente i cybercriminali che guadagnano milioni di dollari mettendo in ginocchio le aziende a cui il **downtime** genera delle perdite complessive per migliaia di dollari. Non meno drammatici i numeri relativi alle denunce che ne conseguono: stando ai dati del **Clusit** meno di 1 incidente su 4 viene riportato alle autorità.

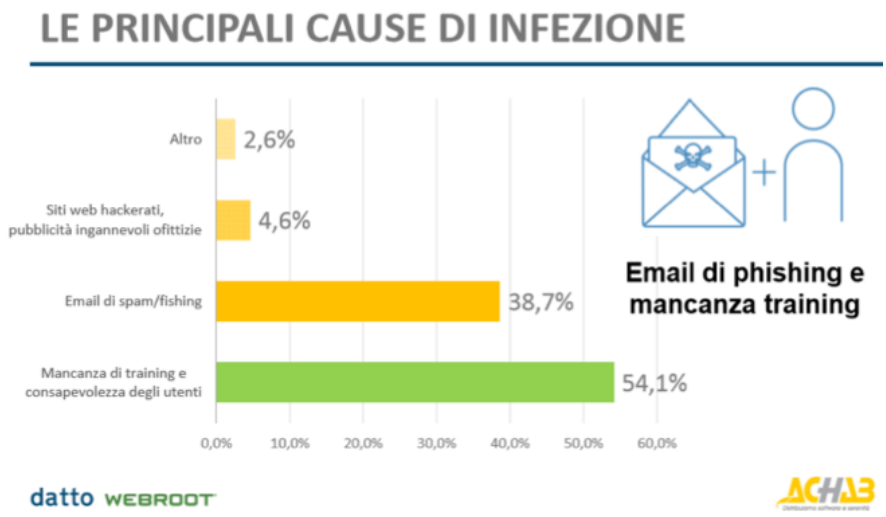
Come si reagisce al ransomware

Per essere pronti a resistere al ransomware è necessario innanzitutto che le imprese siano **consapevoli** di questi rischi, e solo in seguito possono provvedere a mettere in atto **best practice** e sistemi di ripartenza post attacco affidandosi a fornitori di serviti IT e consulenti preparati.

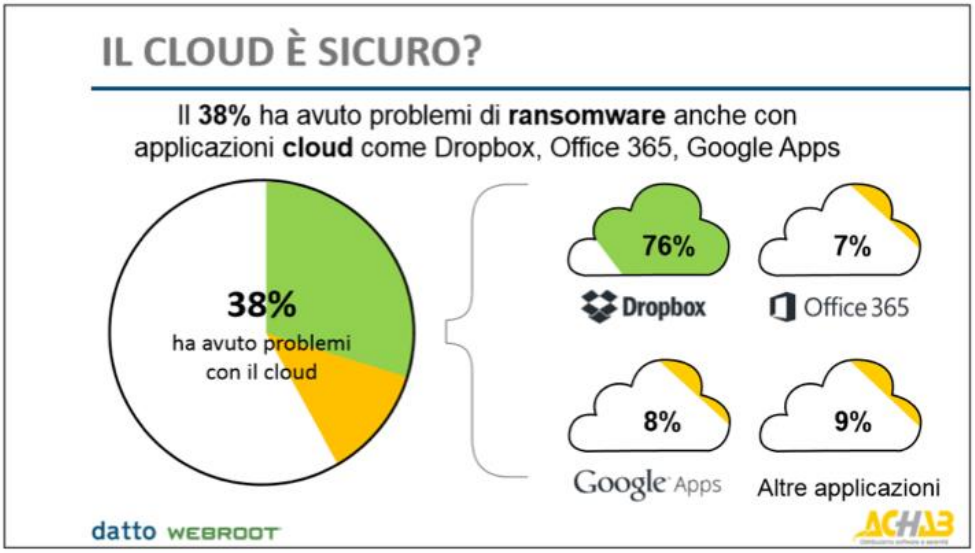
Entrando nel dettaglio della ricerca condotta da Achab, è emerso che il 93% dei fornitori di servizi IT negli ultimi 12 mesi ha effettuato interventi tecnici a causa del ransomware e purtroppo si tratta di un dato che non può che continuare a crescere nei prossimi due anni.

«*C'è una grande differenza di consapevolezza sui rischi del ransomware fra chi si occupa di IT e i clienti* - dice Andrea Veca, CEO di Achab - *Solo il 24% dei clienti è consapevole*».

Come mostra l'immagine seguente, la scarsa consapevolezza degli utenti, la mancanza di training e le email di **phishing** e **spam** sono le principali cause di infezione che nel 93% del casi ha determinato downtime e/o perdita di dati.



«*Inoltre il pagamento del riscatto* – racconta Claudio Panerai, CTO di Achab – *non garantisce il recupero dei dati: il 37% dei fornitori di servizi IT ha pagato il riscatto almeno una volta e di questi in 1 caso su 3 è successo di non riavere i dati anche dopo aver pagato. Le richieste di riscatto per l'81% dei casi non supera i 1.000 euro, ma si sono verificati casi in cui le richieste abbiano superato i 10.000 euro. Tuttavia, benché il tipico riscatto non sia generalmente una somma elevata da prosciugare il conto in banca, il costo del downtime e della perdita di dati conseguente a un attacco ransomware è il danno maggiore da sostenere*».



«*Anche il **cloud*** – ci spiega Andrea Veca – n*on è al riparo dal ransomware: il 38% dei fornitori di servizi IT ha visto infezioni anche su diffuse applicazioni cloud come Dropbox (76%), Office 365 (7%) e Google Apps (8%)*».

Come difendersi?

Secondo Veca le soluzioni di sicurezza tradizionali non sono in grado di arginare gli attacchi di ransomware. Ecco che sul fronte tecnologico la risposta migliore, oltre a un sistematico **aggiornamento dei sistemi**, applicazioni e antivirus, è l'adozione di un sistema di **disaster recovery e business continuity**.

Per tenere sotto controllo l'evoluzione dei ransomware, Achab ha messo a disposizione una risorsa online (**raggiungibile cliccando qui**) che contiene tutte le novità in merito e le tecniche di reazione.