PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4804 di Mercoledì 28 ottobre 2020

Come prevenire e contrastare fenomeni di ransomware

Questo tipo di attacco rappresenta ancora una forma temibile di danno alle attività produttive. In genere le aziende di minori dimensioni sono quelle più facilmente colpite perché sono meno sensibili all'adozione di adeguate provvedimenti di mitigazione.

Un recente studio, pubblicato da una autorevole azienda di consulenza, ha messo in evidenza come i rischi legati a ransomware sono ancora presenti e gravi. Ad esempio, vi è un'elevata probabilità che, anche se l'azienda colpita paga il riscatto, non tutti i dati colpiti dalla protezione criptografica possano essere integralmente recuperati.

Le aziende che più facilmente solo colpite sono quelle con un numero di dipendenti che varia da 100 a 1000, con un giro d'affari dell'ordine dei 50 milioni di dollari. Molte di queste aziende non hanno un budget specifico per la sicurezza del sistema informativo od un responsabile della sicurezza delle informazioni. Le modalità con cui un'azienda può rispondere a un attacco ransomware variano in funzione di parametri locali. Come regola generale, le forze dell'ordine suggeriscono sempre caldamente di non sottostare al ricatto, ma vi sono situazioni estreme nelle quali l'azienda si può trovare, che non offrono alternative.

Ad esempio, se l'azienda non ha messo a punto un piano di disponibilità di copie di backup dei dati, il pagamento del riscatto potrebbe essere l'unica soluzione possibile per riprendere l'attività.

L'importo medio del riscatto, che è stato richiesto nel primo quadrimestre del 2020, è pari a 178.000 $ ma questo riguarda solo il costo del riscatto e non i costi legati al fermo dell'azienda, in attesa del ripristino dei dati. Vale tuttavia la pena di segnalare che la cifra indicata presenta un incremento drammatico rispetto agli 8000 $ circa che sono stati pagati come riscatto nell'ultimo quadrimestre del 2018. L'aumento degli attacchi nel 2020, rispetto all'anno precedente, ad oggi è pari al 148%, il che dimostra come il pagamento del riscatto rappresenta un incentivo notevole perché gli attaccanti coltivino la loro attività criminosa.

Un altro elemento interessante riguarda il fatto che il 76% degli attacchi di ransomware è stato perpetrato durante le ore di chiusura dell'azienda, a dimostrazione del fatto che spesso l'azienda tiene attivi i sistemi informativi, di cui forse non potrebbe aver bisogno durante le ore di chiusura.

La presentazione di questi specialisti di tutela dell'azienda si chiude con un elenco di quali siano gli otto passi che possono essere intrapresi per mitigare la possibilità di un attacco o prevenirla.

1. Attivate politiche di isolamento del sistema informativo
2. identificate i punti di ingresso e, se non necessari, chiudeteli
3. identificate l'orario nel quale si è verificato l'attacco
4. preparate per tempo un piano di contrasto
5. analizzate regolarmente i backup per garantire che non vi sia presente un'infezione
6. ripristinate i file utilizzando un modello di riferimento precedente al periodo dell'infezione
7. indagati attentamente tutte le risorse del sistema che avrebbero potuto essere coinvolte nell'attacco
8. effettuate un'accurata analisi dell'accaduto dopo aver ripristinato le funzionalità operative

Infine, è il caso di ricordare ancora una volta che una adeguata politica di protezione dei dati di backup consiste nell'avere una costante disponibilità di almeno tre copie di backup, di cui una conservata in luogo fisico esterno all'azienda.

Adalberto Biasiotti

---

www.puntosicuro.it