PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5302 di Venerdì 23 dicembre 2022

# La struttura degli attacchi con ransomware

***Gli attacchi con ransomware rappresentano un pericolo crescente per organizzazioni, pubbliche e private, di qualsiasi tipo. Un prezioso documento del General accounting Office analizza la struttura di questi attacchi.***

Ricordiamo ai lettori che si chiama "attacco con ransomware" un attacco informatico, che permette all'attaccante di bloccare l'accesso ai dati del soggetto attaccato e sbloccarne l'accesso, solo a fronte del pagamento di un riscatto, spesso in moneta elettronica.

La crescita esponenziale di queste tipologie di attacchi ha suggerito al General accounting Office degli Stati Uniti di preparare un documento che illustra le modalità dell'attacco.

L'attacco è articolato in quattro fasi, appresso illustrate.



**L'intrusione iniziale**

L'attaccante riesce, in qualche modo, ad entrare nel sistema informatico o perfino in un singolo apparato colpito, come ad esempio un telefono cellulare.

**Lo sviluppo dell'attacco**

L'attaccante acquisisce ulteriori informazioni sulla configurazione del sistema informativo attaccato ed è in grado di iniettare in esso il software, chiamato ransomware.

**La perpetrazione dell'attacco**

Gli attaccanti possono bloccare l'accesso ai dati, da parte del soggetto attaccato, oppure possono estrarre i dati, per un successivo utilizzo criminoso.

**La richiesta di riscatto**

Gli attaccanti mandano al soggetto attaccato la richiesta di riscatto, indicando non solo l'importo richiesto, ma anche il termine ultimo per soddisfare la richiesta.

La difesa da questa tipologia di attacchi è essenzialmente basata sulla adozione di strumenti per la copia frequente dei dati utilizzati dalla potenziale vittima.

Queste copie possono avvenire in forma automatica e possono essere custodite in vari ambienti e su varie strutture. Si va dalla copia custodita nel cloud, alla copia custodita su un supporto di memoria, che viene a sua volta riposto all'interno di una cassaforte od addirittura di un caveau.

In caso di attacco, evidentemente è anche possibile fare riferimento alle strutture della sicurezza nazionale, che possono offrire assistenza in caso di attacco informatico, ma è anche vero che, a fronte di una molteplicità contemporanea di attacchi, le risorse disponibili potrebbero essere insufficienti.

Un altro strumento di difesa, che aiuta soprattutto quando i dati di backup sono disponibili, ma bisogna superare alcuni ostacoli tecnici per la immediata riattivazione del servizio informatico del soggetto attaccato, consiste nell'attivare una specifica protezione assicurativa. Occorre comunque tenere sempre presente il fatto che la copertura assicurativa non rappresenta uno strumento di prevenzione dell'attacco, ma di mitigazione delle conseguenze.

Un'attiva politica di sensibilizzazione dell'azienda, pubblica o privata, sulle modalità di creazione, aggiornamento e protezione dei dati di backup risulta, ancora oggi, una delle più efficaci politiche di protezione.

L'esperienza ha dimostrato che la messa a punto di strumenti di prevenzione dell'intrusione spesso non dà i risultati attesi ed ecco perché solo una efficiente ed efficace strategia di duplicazione dei dati rappresenta la risposta finale a questa tipologia di attacchi.

**Adalberto Biasiotti**



---

**www.puntosicuro.it**