PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5721 di Venerdì 25 ottobre 2024

Quando siete colpiti da ransomware: pagare o non pagare?

Gli attacchi ransomware stanno diventando sempre più frequenti e più volte i dirigenti aziendali coinvolti si sono posti una domanda critica: pagare o non pagare? Ecco il parere di alcuni esperti.

Cominciamo a descrivere brevemente che cosa è un attacco per ransomware. L'attaccante può introdurre nel sistema informativo aziendale un applicativo, che impedisce l'accesso ai dati presenti nel sistema. Successivamente sullo schermo appare un messaggio, che informa il responsabile dell'attacco in corso e offre indicazioni su come pagare il riscatto. Una volta che questo attacco si verifica, non è quasi mai possibile attivare alcuna immediata contromisura e i dipendenti sono impossibilitati ad operare.

Sulla base dell'esperienza attuale, il problema non riguarda tanto il fatto che si rimanga o meno vittima di questo attacco, ma quando si potrebbe rimanere vittima. Anche i responsabili dei sistemi informativi, di elevato livello, possono trovarsi in difficoltà nell'attuare misure preventive sufficientemente efficaci.

Infine, non dimentichiamo che anche se la vostra azienda non viene direttamente coinvolta, potrebbe esserlo perché fornisce servizi ad un'altra azienda, che invece è rimasta coinvolta in questo attacco. Recentemente questo attacco ha colpito un rivenditore di auto negli Stati Uniti. Poiché quasi il 60% dei rivenditori di auto usano lo specifico applicativo, coinvolto nell'attacco, la maggior parte dei rivenditori è stata bloccata.

A questo punto si pone il problema di base: pagare o non pagare il riscatto?

L'esperienza dimostra che in genere i criminali informatici sono molto "corretti", nel senso che se il pagamento viene effettuato, il sistema viene riattivato. L'azienda, tuttavia, a fronte di questa situazione, può crearsi un'immagine negativa, in quanto altri criminali informatici possono ritenere di trovarsi davanti a un'azienda che, in caso di difficoltà, tende a pagare il riscatto; essa diventa pertanto facile bersaglio di nuovi attacchi. Al proposito, è bene tener presente che oggi alcune polizze assicurative informatiche possono anche coprire questo rischio e questo fatto rappresenta un elemento fondamentale di valutazione, circa l'opportunità o meno di pagare riscatto.

Per quanto riguarda le misure di prevenzione, l'esperienza ormai ha dimostrato che esse si devono articolare in tre fasi:

- effettuare un backup frequente e sicuro di tutti i dati aziendali,
- effettuare un backup frequente e sicuro di tutti gli applicativi utilizzati,
- adottare procedure di accesso ai terminali di elevato livello, con autenticazione a due o più fattori.

Con ormai tutti ben sanno, i criminali informatici preferiscono concentrare i loro attacchi sui sistemi più deboli, che possono garantire un ritorno economico soddisfacente, rispetto al grande dispiego di energie, che potrebbe essere necessario per penetrare i sistemi più sicuri.

Ancora una volta, un'oncia di prevenzione vale una tonnellata di repressione, come dicono i nostri colleghi del Regno Unito.

Adalberto Biasiotti

---

www.puntosicuro.it