

# Cryptolocker: e tu sei pronto?

Ormai gli esperti ne sono certi: **Ogni Azienda dovrebbe preoccuparsi del quando e non del se.**

Magari un po' meno catastrofica, ma anche la nostra esperienza ci porta a pensare che le possibilità di essere contagiati dal virus del secolo sia quanto mai concreta per tutti.

Certo la differenza la fanno le misure di prevenzione messe in atto e ancora più quelle di ripristino. Come ogni medico insegna, la prevenzione è almeno importante quanto la cura. Per non arrivare ogni volta a testare se i nostri sistemi di recovery e backup funzionino alla perfezione, è importante cercare di contrarre il virus il minor numero di volte possibile. E se non ci aiutano i nostri utenti/colleghi, che aprono qualsiasi cosa gli arrivi via mail (...) cerchiamo almeno di adottare strumenti che limitano lo spam. Già perché sebbene gli autori delle varianti di cryptolocker si siano ingegnati nel trovare sempre nuove forme di diffusione, la posta elettronica resta il veicolo migliore, quello con più resa, dove è più facile raggiungere l'utente distratto o sovrappensiero. **Perciò prima regola, un buon sistema antispam**, che filtri adeguatamente le mail e magari sia in grado di fare content inspection per cercare di limitare anche il contenuto maligno, magari sia provvisto di antivirus e magari di gray zone. Questo, unito ad un **buon antivirus** è il minimo che si possa fare per prevenire.

Fatto questo, bisogna preoccuparsi di cosa accade se, nonostante gli sforzi profusi, prendiamo il cryptolocker. Qui le cose si complicano un po'. Non solo perché questo è l'ultimo aspetto prima di sapere se sono andati persi dei dati o no, ma anche perché è un po' come quando si fa un incidente in macchina.

Dopo essersi accertati che nessuno dei coinvolti si sia fatto male, ci si inizia a preoccupare dei danni del mezzo. E quello che prima poteva essere un problema di secondo piano, diventa vitale.

Con i backup succede la stessa cosa. Quando succede qualcosa di grave, molto grave, come ad esempio la corruzione di tutti i documenti in rete, il Cliente ci chiama e la prima preoccupazione è la perdita dei dati. I tecnici verificano le procedure di backup e, se tutto è stato fatto a dovere, lo informano che tutti i backup sono consistenti, che non ci sarà perdita di dati. A quel punto, al posto di stappare una bottiglia di champagne, il problema diventa il tempo. Il fatto che su 400GB di dati non si perda nemmeno un bit, passa in secondo piano (non ci siamo fatti male) e l'unica cosa importante è tornare operativi in 10 minuti.

***L'efficacia del sistema di backup non si misura più sulla perdita di dati, ma sulla continuità di servizio, ovvero in quanto tempo gli utenti possono tornare operativi.***

Questa necessità porta noi consulenti a considerare efficace una soluzione di backup solo quando essa non solo protegge il dato, ma lo rende **disponibile in un tempo consono alle esigenze degli utenti**. Ci si sposta allora da soluzioni che hanno per decenni fatto egregiamente il loro dovere, a soluzioni più raffinate, che uniscono alla sicurezza del dato salvato, tempi di recupero molto più veloci. La cara vecchia cassetta (DAT, ULTRIUM, ecc.), seppur ancora ampiamente utilizzata, non rappresenta più l'unica soluzione, perché se da una parte offre la massima sicurezza di protezione del dato (una cassetta al giorno e sono sicuro che li i dati non li tocca nessuno), dall'altra non soddisfa le necessità di velocità nel ripristino. **Il virtuale ha dato una grossa mano**, sia perché è molto più semplice ed affidabile creare una copia completa del sistema (disaster recovery) così da consentire un ripristino dell'intera macchina e non solo dei dati, sia perché riduce molto i tempi di backup e ripristino rendendo possibile anche una periodicità delle copie più alta rispetto al classico quotidiano.

***Ma la vera rivoluzione è rappresentata dalle soluzioni di iperconvergenza.***

È grazie a questa tecnologia che si può davvero cambiare marcia. Basti pensare che è lo stesso concetto di backup ad essere sorpassato. Grazie a questi sistemi si effettuano delle istantanee dell'intero sistema, che grazie all'hardware e al software raggiungono performance ed efficienze mai viste, consentendo di avere **latenze di qualche minuto e ripristini in qualche minuto**.

Cosa significa tutto ciò? Semplice, che dal momento in cui si riscontra un problema di corruzione dei dati (sia esso per codifica vedi cryptolocker, o perdita, vedi danno hardware) si può recuperare in pochi minuti una copia integra e consistente di tutti i dati di pochi minuti prima.

***Per pochi minuti intendiamo 1, 2 o 3 minuti!***

Non stiamo dicendo che l'iperconvergenza sarà la soluzione di domani perché risolve i problemi dei tempi di ripristino, siamo convinti che sarà la soluzione di domani perché in generale affronta tutti i problemi legati alla business continuity come mai nessun'altra soluzione ha fatto fino ad ora.

## ML INFORMATICA SRL

UFFICI: Via Martiri di Nassirya, 18 - 23900 Lecco (LC)

Email: [info@mlinformaticasrl.it](mailto:info@mlinformaticasrl.it)

WEB: <http://wwwmlinformaticasrl.it>

Telefono: 0341499590 Fax: 0341259684

P.IVA e CF 02861890131 C.C.I.A.A. Lecco n° 300331



syneto



KASPER(SKY)

Synology