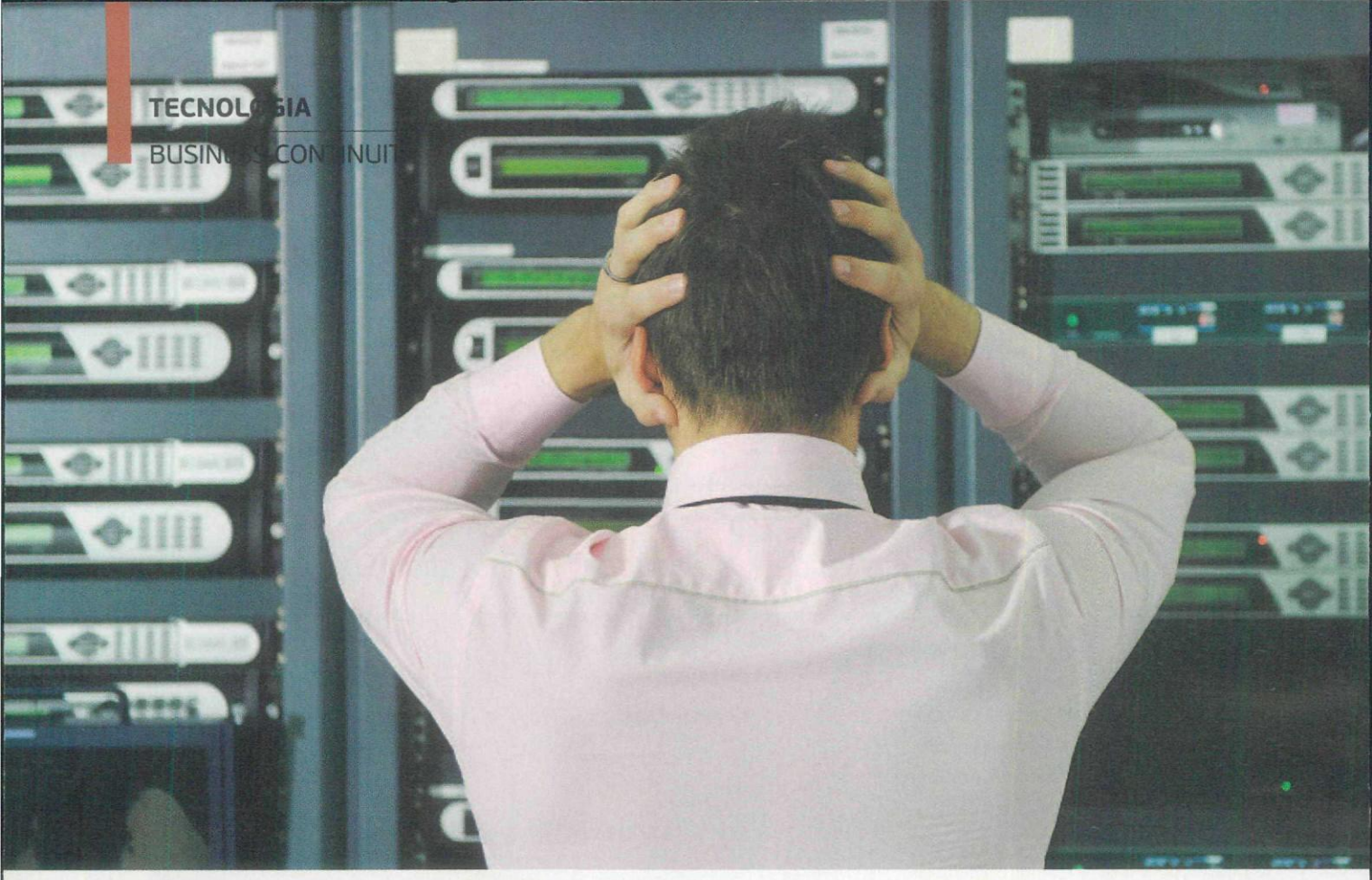

Dopo il disastro riparti in sei secondi

Le minacce della cybercriminalità diventano sempre più sofisticate, il backup non basta più: oggi bisogna garantire la continuità del business qualunque cosa accada

LUCA MASALI

La fantasia malvagia dei programmatori di virus non ha confini, e l'ultima trovata fa davvero spavento. Si chiama Cryptolocker, infetta i computer via email e quando si attiva cattura l'hard disk, crittografa i dati per renderli illeggibili e chiede un riscatto salato, 300 euro, promettendo al malcapitato di restituirgli i dati solo se paga (via bitcoin o voucher prepagati).

Naturalmente, avendo a che fare con una banda di criminali, non c'è nessuna garanzia che una volta pagata la tangente i dati vengano restituiti per davvero. Siamo insomma di fronte a una nuova categoria di crimine informatico che si chiama Rasomware, da "rasom" che in inglese è il riscatto. Per i delinquenti questa operazione è una vera miniera d'oro: seguendo i movimenti di conti bitcoin collegati a computer infettati da Cryptolocker, il blog tecnologico ZDNet ha scoperto un fiume di denaro verso i delinquenti, ben 41,928 bitcoin (oltre 25 milioni di euro) solo tra il 15 ottobre e il 18 dicembre 2013. A pagare sono in tanti, molti di più di quello che gli analisti si aspettavano: il 41% degli infettati, secondo una ricerca dell'Università del Kent.

Un successo che ha scatenato altre bande di criminali: nel 2014 in Australia sono stati scoperti virus molto simili, CryptoWall e TorrentLocker. Difendersi dall'attacco non è facile, e un backup serve a poco, visto che molto probabilmente anche la copia di sicurezza avrà il virus. Bisognerebbe andare indietro nel tempo, trovando un backup precedente all'infezione, e una volta fatto il restore dei dati togliere il trojan, operazione tutto sommato abbastanza semplice. Ma intanto si perde tutto il lavoro fatto nel lasso di tempo intercorso tra backup e infezione. La prevenzione è sempre meglio della cura, e bisogna evitare sempre di aprire gli allegati delle email, specialmente quelle che arrivano da istituzioni come banche, governo o Agenzia delle Entrate: questi Enti non

comunicano via email, e il virus impersona proprio le istituzioni più affidabili per diffondersi nella Rete.

Se proteggere un computer è un problema, figuriamoci proteggere la struttura IT di un grosso provider di servizi o di una grossa azienda, dove un eventuale disastro informatico, non solo virus, potrebbe mettere a rischio il business. Ne parliamo con **Andrea Veca**, AD di Achab, azienda che commercializza tra l'altro le soluzioni di Datto (gioco di parole tra Ditto, che sta per "Uguale" e Dato) ai provider si servizi che devono garantire ai loro clienti la business continuity, cioè assicurarli che qualunque cosa succeda il loro business non cadrà insieme ai server.

«Per le grandi aziende, il segreto è quello di copiare i dati e copiarli in altri posti, diversi dal server. Questo altro posto può essere o un dispositivo che sta a casa del cliente oppure il cloud, la nuvola; in pratica i dati sono replicati sui server remoti di chi offre il servizio di business continuity».

Detta così sembrerebbe solo un backup, cioè la copia di sicurezza dei dati.

«Diciamo che si parte dal backup, pratica indispensabile ma è solo metà del problema. L'altra metà è il restore, cioè il rimettere i dati al loro posto per poterli usare. Quando scoppia un disastro, i problemi sono due; quanto è vecchia l'ultima copia che ho (facendo un backup al giorno si rischia di avere dati vecchi di otto ore lavorative) e il secondo problema è quanto ci metto a rimettere al lavoro i miei utenti. In termini tecnici questi due aspetti si chiamano RPO (Recovery Point Objective) e RTO (Recovery Time Objective) e la somma tra questi due tempi, cioè l'ultima fotografia del sistema congelata nel backup e il tempo che occorre per rimetterli al loro posto dopo il crash è l'intervallo di tempo il cui il cliente non può lavorare e perde denaro».

IL SEGRETO PER DIFENDERSI
«Per le grandi aziende, il segreto è quello di copiare i dati in posti diversi dal server», dice Andrea Veca, ceo di Achab

In Italia ci sono stati 8mila casi di Cryptolocker

Quindi questo tempo va abbassato il più possibile... Quanto?

«La riduzione del tempo RPO+RTO a zero si realizza con architetture replicate: ho un server identico che replica al singolo bit il server di produzione, e questo è il massimo che si possa ottenere oggi. Ma ci sono costi che non tutti si possono permettere. E potrebbero anche essere sproporzionati rispetto al costo del fermo macchina. Noi proponiamo una specie di compromesso che abbatte notevolmente i tempo di ripristino rispetto a un backup e restore classico: idealmente, entro sei secondi dal crash l'azienda torna online».

E come funziona?

«Attraverso una soluzione ibrida, hardware software e cloud, facile da gestire. Il primo componente sta a casa del cliente ed è uno scatolotto che, attraverso il software dedicato, riceve dei backup dal server con una frequenza fino a cinque minuti: così nel caso peggiore ho il backup a cinque minuti prima del disastro. Una immagine, attenzione, non solo i dati: quindi anche tutto il software, le variabili d'ambiente eccetera. La stessa immagine del server che finisce sul dispositivo viene copiata anche sul cloud sui server Datto (in Europa per ragioni di normativa). Così io ho una immagine del server sia locale e una sulla nuvola. In caso di disastro posso montare l'immagine del server che ho sul dispositivo locale sul server di produzione, ma il bello è che il dispositivo può funzionare lui stesso come server, e lo stesso può fare il cloud: in questo modo il produttore parla di tempi di ritorno online attorno ai sei secondi dal disastro. Se non sono secondi, sono minuti, ma il discorso non cambia».

E se mi sono preso il malware Cryptolocker?

«Visto che il sistema fa una foto ogni 5 minuti, basta tornare al fotogramma immediatamente prima dell'infezione. Quest'anno in Italia abbiamo avuto 8 mila casi di Cryptolocker; non si risolve il problema ma lo si aggira, tornando a prima dell'incidente».