Paolo Gambaro
Consulente Finanziario

Il CAVEAU
il deposito delle idee

N. 200
20 nov 2026

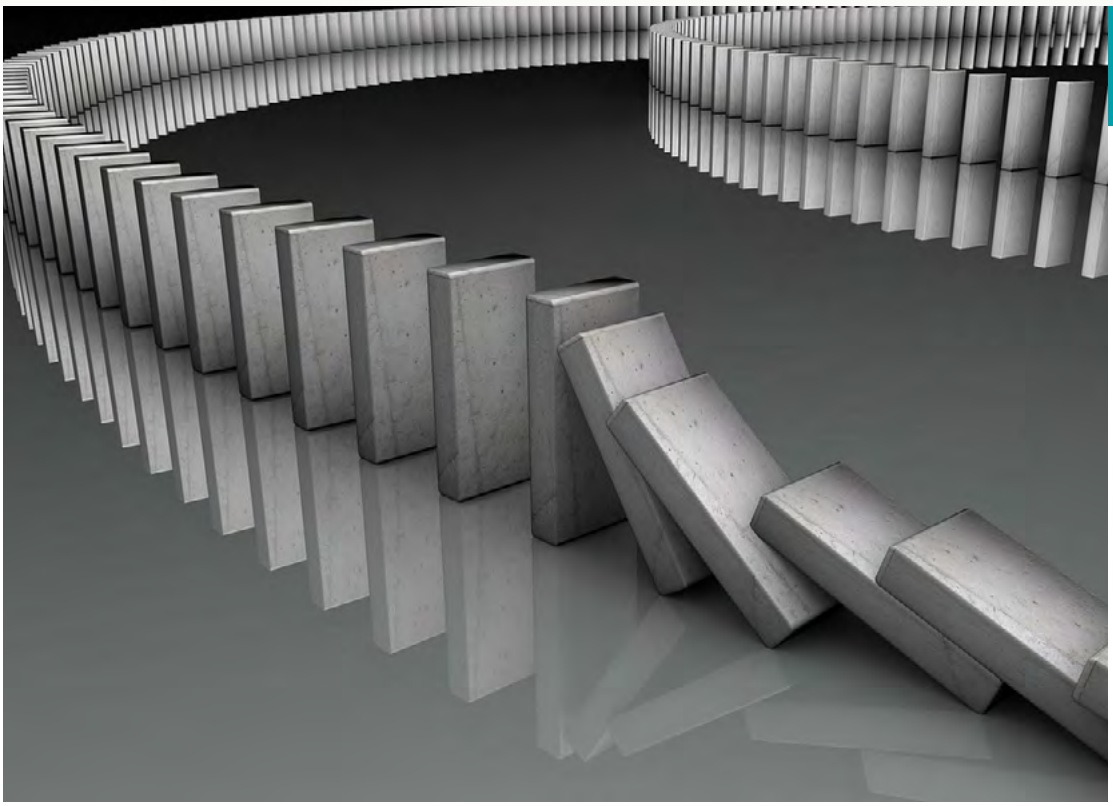


Photo: PublicDomainPictures - Pixabay

L'effetto domino del Cloud: quando i server si fermano, l'economia reale smette di respirare

Tra il pomeriggio di giovedì 12 e venerdì 13 novembre (secondo la cultura statunitense, una data nient'affatto propizia), un massiccio disservizio di Microsoft 365 — originato da un sovraccarico dei server di Exchange Online che ha travolto Outlook, Teams, SharePoint e Copilot — ha paralizzato milioni di aziende, ospedali, tribunali, compagnie aeree e uffici pubblici tra Nord America, Europa e Asia-Pacifico, con ricadute anche nei giorni successivi.

In Australia l'interruzione è stata ribattezzata il *"Microsoft long weekend"* dopo che intere organizzazioni hanno dovuto dichiarare persa la giornata lavorativa di venerdì, mentre nel Regno Unito ha mandato in tilt i sistemi amministrativi del servizio sanitario nazionale (NHS) e delle forze di polizia.

Fino a pochi anni fa, **un'interruzione dei servizi di posta elettronica o di archiviazione remota veniva derubricata a semplice fastidio operativo**. Oggi, nell'era dell'iper-connessione aziendale, un blackout del cloud non è più un intoppo tecnico circoscritto: è **un evento sistemico globale**. In

pochi minuti, un errore di configurazione o un collo di bottiglia nei protocolli di connessione può **bloccare aeroporti, congelare transazioni finanziarie e bruciare decine di miliardi di dollari di valore economico**.

Per comprendere la portata finanziaria di questi eventi, occorre guardare al costo orario dell'inattività, c.d. downtime. Se il benchmark storico elaborato da Gartner fissava il costo medio di un'interruzione IT intorno ai 5.600 dollari al minuto (circa 336.000 dollari l'ora), adesso **oltre il 90% delle medie e grandi imprese subisce perdite superiori ai 300.000 dollari per ogni ora di fermo, mentre per il 41% delle grandi aziende il danno oscilla tra 1 milione e 5 milioni di dollari l'ora**. Nei settori ad altissima intensità transazionale i numeri diventano vertiginosi: nel comparto bancario e finanziario un'interruzione critica può costare fino a 9,3 milioni di dollari l'ora, mentre nella sanità si superano i 7 milioni di dollari l'ora, tra blocchi diagnostici e rischi clinici. Inoltre, **sebbene la frequenza complessiva dei guasti gravi sia leggermente diminuita grazie a infrastrutture più moderne, il loro impatto economico unitario è esploso**.

A pesare sui bilanci non sono solo i ricavi sfumati dell'e-commerce o l'impossibilità di emettere fatture e incassare pagamenti, ma anche i costi invisibili: milioni di dipendenti pagati a vuoto, straordinari per i team IT e penali per le consegne mancate lungo la catena di approvvigionamento.

La storia recente offre altri casi emblematici che illustrano l'escalation del rischio sistemico legato al cloud:

- L'incidente CrowdStrike / Microsoft (19 luglio 2024): un aggiornamento difettoso di un software di sicurezza mandò in tilt 8,5 milioni di dispositivi Windows in tutto il mondo, sovrapponendosi a un disservizio di Azure. Le **perdite economiche globali furono stimate intorno ai 15 miliardi di dollari**. Il caso simbolo fu quello di Delta Air Lines: con quasi 7.000 voli cancellati, la compagnia aerea statunitense denunciò perdite per circa 500 milioni di dollari, innescando una dura battaglia legale per il risarcimento.

- L'"ottobre nero" del Cloud (20 e 29 ottobre 2025): Nell'autunno del 2025 il mercato sperimentò la fragilità simultanea dei due principali leader mondiali. Il 20 ottobre un'interruzione massiccia di AWS mise fuori uso piattaforme vitali per il lavoro quotidiano e i consumi, tra cui Slack, servizi bancari e portali di e-commerce. Appena nove giorni dopo, il 29 ottobre, un errore di configurazione su Azure Front Door provocò un blackout di circa otto ore su scala planetaria per Microsoft Azure, bloccando pagamenti con carta e sistemi aziendali. Gli analisti stimarono l'impatto economico complessivo tra 4,8 miliardi e 16 miliardi di dollari.

Di fronte a disservizi di questa portata, sorge spontanea una domanda: chi paga il conto? Contrattualmente, i colossi del cloud si tutelano attraverso gli SLA (Service Level Agreement), che garantiscono solitamente una disponibilità del servizio pari al 99,9% — una soglia che equivale a circa 43 minuti di fermo tollerati al mese. **Quando un blackout supera le 15 o 16 ore, come accaduto tra il 12 e il 13 novembre, scattano i mecca-**

nismi di rimborso, ma qui si nasconde una forte asimmetria finanziaria: le penali contrattuali dei giganti tech consistono quasi sempre in crediti di servizio (sconti sulle fatture future) e non in risarcimenti monetari per i danni da interruzione dell'attività, cosa che per molte aziende si trasforma in una sorta di **compensazione simbolica**. Inoltre, **molte polizze Cyber Insurance sottoscritte negli ultimi anni coprono i danni derivanti da attacchi informatici dolosi** (come i ransomware), ma escludono o limitano severamente i guasti tecnici non dolosi causati da fornitori terzi — proprio come quelli che hanno coinvolto Microsoft. Le aziende si scoprono così esposte proprio sul fronte più frequente, mentre i dipendenti costretti a ripiegare su e-mail personali o canali non protetti per continuare a lavorare aumentano ulteriormente il rischio di frodi e phishing.

Sui mercati azionari, la reazione segue invece dinamiche che riflettono la scala del problema, tanto che nel luglio 2024 CrowdStrike bruciò oltre l'11% della propria capitalizzazione in una sola seduta. Nel medio periodo, tuttavia, gli *hyperscaler* continuano a beneficiare di un potente paracadute finanziario: **l'elevatissimo costo di migrazione rende quasi impossibile per le grandi imprese abbandonare la piattaforma nel breve termine**, proteggendo i flussi di cassa ricorrenti.

Il nodo centrale della questione resta il fatto che **tre soli attori statunitensi** — AWS (circa il 30%), Microsoft Azure (tra il 20% e il 25%) e Google Cloud (intorno al 13%) — controllano circa due terzi dell'intera infrastruttura cloud mondiale.

Ora l'obiettivo delle aziende non è più la ricerca del massimo risparmio attraverso un unico fornitore, ma il finanziamento della **resilienza operativa**. **Investire in architetture multi-cloud**, mantenere sistemi ibridi ridondanti e testare piani di continuità indipendenti comporta costi di bilancio più elevati nel breve periodo, ma rappresenta ormai **l'unica polizza efficace per evitare che un errore a migliaia di chilometri di distanza possa azzerare i ricavi di un intero trimestre**.

Federica Coscia, Paolo Gambaro

Disclaimer | Paolo Gambaro Consulente Finanziario | Via P. Felice Piana, 12/14 | 28021 Borgomanero (NO) | Tel. +39 0322 211007
La presente pubblicazione è distribuita da Paolo Gambaro. Pur ponendo la massima cura nella predisposizione della presente pubblicazione e considerando affidabili i suoi contenuti, Paolo Gambaro non si assume tuttavia alcuna responsabilità in merito all'esattezza, completezza e attualità dei dati e delle informazioni nella stessa contenuti ovvero presenti sulle pubblicazioni utilizzate ai fini della sua predisposizione. Di conseguenza Paolo Gambaro declina ogni responsabilità per errori od omissioni. La presente pubblicazione viene a Voi fornita per meri fini di informazione ed illustrazione, non costituendo in nessun caso offerta al pubblico di prodotti finanziari ovvero promozione di servizi e/o attività di investimento.

La presente pubblicazione può essere riprodotta unicamente nella sua interezza ed esclusivamente citando il nome di Paolo Gambaro, restandone in ogni caso vietato ogni utilizzo commerciale. La presente pubblicazione è destinata all'utilizzo ed alla consultazione da parte della clientela professionale e commerciale di Paolo Gambaro cui viene indirizzata, e, in ogni caso, non si propone di sostituire il giudizio personale dei soggetti a cui si rivolge. Le opinioni espresse in questa rubrica costituiscono il parere personale del Consulente Finanziario Paolo Gambaro e vogliono essere uno spunto di lettura dei principali fatti di attualità, economia e finanza.
Per ricevere periodicamente la rubrica «Il CAVEAU», iscriviti sul sito www.paologambaro.it