White Paper

Quanto costa un fermo dei sistemi IT?

QUANTO COSTA UN FERMO DELLA TUA AZIENDA?

Ti sei mai chiesto **che cos'è che veramente conta per la tua azienda**?

Probabilmente la risposta è una sola: **la continuità operativa**, ossia la possibilità di lavorare sempre e comunque anche se dovesse succedere un problema o un disastro.

In effetti l'imprenditore ha in mente una sola cosa: **che i ricavi siano superiori a costi**, quindi che il margine (ricavi - costi) sia quanto più grande possibile. E non c'è nulla di male in questo…è il lavoro dell'imprenditore! L'ottenimento di ricavi e quindi di margini è strettamente legato all'operatività dell'azienda, molto banalmente: se l'azienda è ferma non può fatturare, se non può fatturare non ottiene ricavi ma continua a sostenere dei costi.

Le continue migliorie tecnologiche e la vita lavorativa moderna hanno **alzato il livello delle aspettative dei lavoratori**; tutti si aspettano che la email sia sempre accessibile, che i server siamo sempre disponibili, che il gestionale sia in perfetta efficienza e che i dati siano disponibili da dovunque 24 ore su 24.

E se qualcosa si "inceppa" ecco che nascono i problemi.

Ma perché è così?

Tutte le aziende trattano informazioni e comunicano con terzi e, oggi, le informazioni sono dati, cioè file, e la comunicazione è fatta tramite strumenti tecnologici come email, chat e telefonate che ogni giorno passano sulla rete internet. Quindi, volenti o nolenti, **il lavoro di tutti è fortemente basato sull'IT**.

È allora necessario minimizzare i fermi aziendali dovuti all'IT: **serve avere un "piano B" che permetta di minimizzare i costi legati a un fermo aziendale**.

Se ci pensi bene anche molte attività apparentemente semplici, come per esempio quella dei tassisti, prevede sempre un piano B: c'è una ruota di scorta per sostituirla qualora si dovesse bucare, per continuare il proprio lavoro portando il cliente a destinazione.

Una delle sfide più difficili è capire **qual è la soluzione di protezione adatta alle proprie esigenze**.

Sono tre i parametri importanti da tenere in considerazione mentre si valuta una soluzione per proteggere la propria azienda:

- la probabilità dell'interruzione**, cioè qual è la probabilità che si verifichi un evento tale per cui venga interrotto il lavoro dell'azienda?**
- **il danno dell'interruzione, cioè quali sono i costi associati all'interruzione dell'attività?**
- **il costo della contromisura, cioè quanto costa mettere in pista un sistema di protezione?**

Partiamo dalla prima domanda: **qual è la probabilità di interruzione?**

Per rispondere a questa domanda dobbiamo capire **cosa può interrompere il funzionamento dell'IT di un'azienda**.

COSA PUÒ FERMARE L'IT DELLA TUA AZIENDA

Quali sono i disastri che possono portare a un rallentamento o addirittura un fermo dei sistemi IT?

Sicuramente ci sono dei disastri naturali come per esempio i terremoti, alluvioni, allagamenti trombe d'aria o incendi.

Tuttavia, nella maggior parte dei casi, il blocco dell'IT è dovuto a cause ben più banali e purtroppo anche molto frequenti.

- **Guasti hardware:** i dati sono sempre memorizzati sui dischi dei server o dei computer. Anche se talvolta sembra che i componenti possano durare all'infinito, in realtà hanno tutti un periodo di funzionamento dichiarato ufficialmente dalla casa produttrice. Questo vuol dire che ogni elemento hardware, quindi anche un disco di un computer, prima o poi è soggetto a rottura, e se si rompe un disco…come si accede ai dati che vi erano memorizzati sopra?
- **Problemi software:** sul lavoro si utilizzano quotidianamente diverse applicazioni. Cosa succede se una di queste all'improvviso si chiude sganciando un messaggio di errore e corrompendo il file su cui stavi lavorando, rendendolo inaccessibile? I software sono per definizione imperfetti, presentano bachi e problemi, ma non solo: questi si trovano ad agire all'interno di un altro ambiente, il sistema operativo, non esente da difetti. Ritrovarsi con un file danneggiato e dover recuperare ore, se non giorni, di lavoro e informazioni raccolte non è di certo un bello scenario, non trovi?
- **Cancellazione accidentale:** quante volte ti è capitato di cancellare un file pensando "tanto non mi servirà più", salvo accorgerti due giorni dopo che ne avresti ancora avuto bisogno? Oppure ancora, è mai successo a te o un collega di cancellare per errore un file, una cartella, una fattura o un ordine? Per quanta attenzione si possa porre durante il lavoro al PC, l'essere umano tende a distrarsi, talvolta ad agire sovrappensiero o con la mente poco lucida a causa del troppo lavoro, questo porta a errori a cui è difficile porre rimedio... a meno che tu non abbia un backup dei file!
- **Virus e ransomware**: i dati sono diventati il bene più prezioso per un'azienda, i cyber criminali lo sanno bene e mettono a punto virus in grado di cancellarli o di bloccarli completamente rendendoli indecifrabili. In questi casi si hanno due possibilità. La prima è pagare un oneroso riscatto ai criminali per riavere indietro i propri dati, senza però nessuna garanzia che questo avvenga davvero o che nel frattempo i dati non siano stati anche diffusi nel Dark Web. La seconda è perdere del tutto l'accesso a sistemi e file aziendali, con un danno economico difficilmente quantificabile che in passato ha messo in ginocchio anche aziende di grandi dimensioni**.**

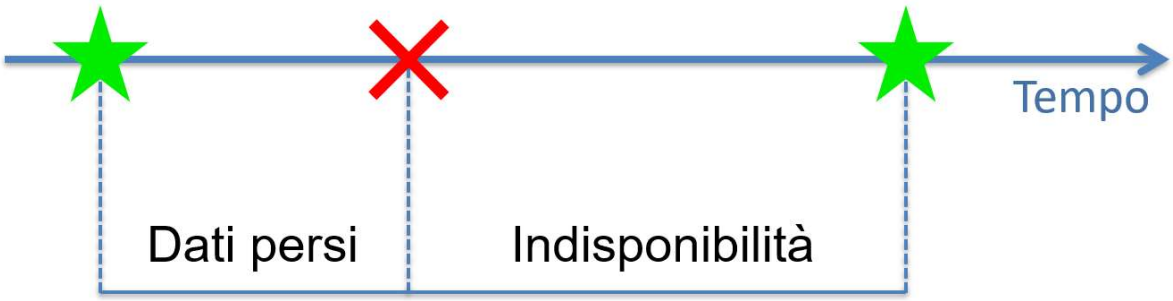
Se queste sono le cause di un possibile "disastro", qual è l'anatomia di un disastro? Quali variabili entrano in gioco e quali sono i costi associati?

Iniziamo con l'esplorare come è fatto un disastro.

ANATOMIA DI UN DISASTRO

Immaginiamo di avere un asse che rappresenta il tempo.

Immaginiamo ora **che al momento X avvenga un disastro** (o un incidente che rallenti o blocchi l'operatività della tua azienda).



Da qui **si possono individuare due momenti**: uno successivo al disastro e uno precedente al disastro.

L'istante successivo al disastro rappresenta il momento in cui si ricomincia a lavorare.

L'istante precedente al disastro rappresenta il momento dell'ultimo backup.

Questi due momenti individuano due intervalli di tempo ben precisi (e molto importanti): **l'intervallo di tempo che passa dal momento del disastro a quando si riprende a lavorare si chiama indisponibilità o RTO (Recovery Time Objective)** e indica la quantità di tempo durante il quale non sono disponibili i sistemi e quindi il tempo in cui tu non puoi lavorare.

L'intervallo di tempo che passa dal momento dell'ultimo backup al momento del disastro rappresenta l'RPO (Recovery Point Objective) e include i dati che sono stati prodotti fra il momento del backup dell'ultimo backup è il momento del disastro, dati di cui non potrai disporre anche quando riprenderai a lavorare. Supponiamo che tu faccia il salvataggio a mezzanotte. Se il disastro si verifica alle 10 di mattina, il valore dell'RPO in questo caso è il tempo che intercorre tra la mezzanotte e le 10 di mattina.

I DANNI DERIVANTI DAL FERMO AZIENDALE

Quindi: quanto tempo la tua azienda può stare senza lavorare?

Per rispondere occorre capire quali sono i costi legati al verificarsi di un disastro, perché sulla base di questo potrai scegliere un sistema di backup e disaster recovery adatto alle necessità della tua azienda.

Di seguito trovi un rapido elenco.

Improduttività

Questa voce indica i costi di struttura pagati a vuoto; basti pensare all'affitto o alle bollette o agli stipendi del personale: si tratta di costi che normalmente vengono sostenuti per far lavorare l'azienda ma che in questo caso vengono sostenuti senza che l'azienda possa "produrre", e quindi si tratta di un costo secco, non recuperabile.

Indisponibilità

Il fatto che uno o più sistemi non siano disponibili significa che il personale non può lavorare (per nulla o solo in parte); questo vuol dire che l'azienda non può portare avanti il proprio lavoro, non produce e quindi non "fattura": anche questo è un costo da tenere in considerazione.

Ripristino dei sistemi

Se i sistemi IT sono bloccati o fuori uso, sarà necessario l'intervento di qualcuno per rimettere l'IT in grado di funzionare; questo potrebbe essere un solo costo in termini di tempo se si dispone di un sistema di disaster recovery adeguato, ma laddove non ci si fosse preparati al peggio potrebbe essere necessario sostenere dei costi di acquisto, consegna e messa in opera di nuovo materiale informatico.

Perdita di integrità

Si è visto in precedenza che dal momento dell'ultimo backup al momento in cui avviene un disastro sostanzialmente si perdono dei dati. In qualche caso i dati sono persi per sempre (e questo potrebbe essere un danno incalcolabile), mentre in altri casi potrebbe essere necessario del lavoro extra o potrebbe essere necessario ingaggiare nuovo personale per un periodo di tempo limitato per "ricostruire" i dati persi.

Perdita di riservatezza

Questa voce rappresenta il costo legato al fatto che i dati della tua azienda possono finire in mano a qualcun altro. Purtroppo, oggi questo rappresenta un rischio non indifferente: i moderni ransomware, infatti, oltre a cifrare i dati e a chiedere un riscatto, chiedono un secondo riscatto minacciando di rendere pubblici i dati se non si paga un secondo riscatto.

Perdita di immagine e credibilità

Questo costo, difficilmente calcolabile, può essere altissimo: supponiamo che la tua azienda venga colpita da un ransomware e che perda i dati di tutti i clienti. Se i clienti vengono a sapere che avete perso tutti i loro dati, che figura ci fa l'azienda? Non credi che alcuni clienti (se non tutti) cambierebbero fornitore ritenendovi non professionali?

… in base all'attività della tua azienda, l'elenco potrebbe essere ancora più lungo.

A questo punto **andrebbe valutato il costo della contromisura da adottare** per poter lavorare anche in caso di disastro.

I sistemi di protezione, sicurezza, backup e disaster recovery **hanno costi molto variabili in base alle performance che sono in grado di fornire**.

Come regola base va tenuto presente che **più bassi sono RPO e RTO** (ossia per perdere meno dati possibile e ripartire il più velocemente possibile) **più è costosa la contromisura**. Quindi per ridurre al minimo la perdita di dati e il tempo necessario alla ripartenza potrebbe servire una soluzione mediamente più costosa.

Per capire quale sia la soluzione adatta a proteggere la tua azienda, **rivolgiti a chi eroga servizi IT, che probabilmente avrà già affrontato con successo questo tema con altre aziende come la tua e potrà consigliarti per il meglio**.