White Paper

# Perché è importante monitorare la rete

# QUANDO LA RETE È TUTTO - E QUALCOSA DI PIÙ

C'è stato un tempo nel quale i PC aziendali erano isolati gli uni dagli altri, il trasferimento di dati e programmi avveniva manualmente tramite floppy disk, i server non si sapeva nemmeno cosa fossero e il fax rappresentava il pinnacolo delle tecnologie di comunicazione.

A meno che la tua azienda non sia rimasta invischiata in una trappola spaziotemporale, il tuo lavoro poggia attualmente su basi ben diverse, persino irriconoscibili rispetto ad allora.

Prova a pensarci: oggi sei costantemente in contatto con chiunque in qualsiasi luogo e momento, dall'ufficio così come da casa o in viaggio.

**Il PC** che hai sulla tua scrivania è solo uno dei tanti strumenti informatici a tua disposizione, che si aggiunge a quell'arsenale di computer **portatili**, **tablet** e convertibili che nemmeno tu ricordi bene come abbia fatto ad accumularsi negli anni.

Vogliamo parlare poi degli immancabili **smartphone**? Quegli oggetti nati come telefoni e che oggi usiamo per tutto salvo quasi che per telefonare? **Sono tutte appendici digitali della tua capacità professionale**, strumenti con i quali produci, comunichi, ti informi, decidi, gestisci, acquisti e vendi. Strumenti che sono sempre a tua disposizione, alternativi ma complementari tra loro, **perfettamente funzionanti e costantemente collegati a un'infrastruttura** la cui esistenza e disponibilità hai imparato a dare per scontata: può essere un server chiuso in uno stanzino dell'ufficio piuttosto che un armadio di rack all'interno di un data center o un'entità astratta in ciò che chiamiamo "cloud".

Tutto unito all'interno di **quell'ambiente che rappresenta ormai il nostro modo attuale di lavorare: la rete**.

Reti locali, reti geografiche, reti wireless, reti cablate, Internet: impossibile oggi pensare di fare a meno di questo collante chiamato connettività. **La diamo per scontata** in ufficio e a casa, quando siamo in giro, quando viaggiamo in auto o in treno, tanto che una delle prime cose che chiediamo quando arriviamo in un hotel, un caffè, un locale qualsiasi o persino a casa di amici è... "la password del Wi-Fi".

Noi viviamo sempre connessi la nostra vita personale e quella lavorativa pur conservando la nostra individualità; ma **se pensiamo alle aziende**, specialmente quelle del terziario o dei servizi in genere, accade sempre più spesso che **dalla connettività dipenda la loro stessa esistenza**.

Un'attività viene ormai definita in termini di funzionalità che essa rende disponibili in rete e di velocità alla quale lo fa. **Un'azienda che per qualche motivo si disconnette è un'azienda che smette di esistere**, un business che si ferma perché tutti i suoi elementi funzionali si sganciano l'uno dall'altro oltre che con l'esterno. Insomma, se ci si aspetta che tutti noi si agisca nelle velocissime tempistiche di Internet, il cosiddetto "Internet time", il presupposto è che non si manchi di essere connessi e perfettamente operativi con tutti gli strumenti IT necessari.

Quanto la rete - intesa sia come "autostrada delle informazioni" che come dispositivi ad essa collegati - sia ormai parte indissolubile delle nostre esistenze lo si capisce semplicemente ripensando a tutto quello che facciamo nel corso della giornata, in ufficio come nel tempo libero.

Facciamoci caso: ormai c'è una corsa a interconnettere anche quello che è nato per funzionare in modo indipendente, i navigatori per auto ad esempio. **La rete agisce da moltiplicatore dell'efficacia e dell'utilità di qualsiasi oggetto** o applicazione, e quanto sia destinata a crescere ulteriormente di importanza nel futuro lo

si può desumere anche solo seguendo la diatriba internazionale in atto sul 5G: una tecnologia abilitante che promette di diventare il tessuto nervoso di un ambiente di miliardi di computer, dispositivi e oggetti, tanto da essere divenuta ormai un affare geostrategico alla pari delle materie prime da cui dipende l'economia del pianeta.

Ma **cosa succede quando la rete** o qualcuno dei suoi componenti **diventa indisponibile** per un qualsiasi motivo?

**Ne soffre la comunicazione**, innanzitutto. Poi **smettono di funzionare le applicazioni in cloud**, come Office 365 o Salesforce, togliendoci le funzionalità necessarie al nostro lavoro. **I database, i file server e le cartelle condivise smettono di essere accessibili**, impedendoci di attingere ai documenti e ai dati che ci occorrono. **Le applicazioni locali**, quelle che abbiamo installato sull'hard disk del computer, **non riescono più a "chiamare casa"** per verificare la validità delle licenze: qualcuna ci avvisa lasciandoci - bontà sua - qualche giorno di tempo per ricollegarci, altre invece si rifiutano di partire fin da subito. Le **piattaforme di collaborazione**, quelle che ci permettono di condividere il nostro lavoro con i colleghi offrendoci l'opportunità di dialogare in videoconferenza, **diventano semplici pezzi di software inerte**. **Non parliamo poi dei gestionali** su cui si basano le catene di approvvigionamento e produzione, la logistica e la contabilità.

**Prova a pensare alla tua attività in caso di blackout dell'IT. Se lo può permettere?**

Certamente no, e possiamo essere certi che a questa eventualità ti sia capitato di pensare, qualche volta. Magari la tua azienda possiede anche un piano di emergenza per gestire i casi peggiori di interruzione operativa.

## UN CONTINUO ACCUMULARSI DI GUAI

Il vero problema è che di norma questi cosiddetti *contingency plan* tendono ad affrontare le situazioni estreme, come il caso del crollo catastrofico dell'ambiente IT, secondo il noto approccio della chiusura della stalla a buoi ormai fuggiti.

Forse sull'onda dell'esperienza nel prepararsi a gestire le temute conseguenze del terribile bug dell'Anno 2000, queste procedure scaturiscono spesso come risposta ad eventi limite, sempre possibili ovviamente ma per fortuna non così diffusi nell'esperienza quotidiana.

Nella realtà invece **i veri problemi risultano assai più frequenti e subdoli**, un progressivo accumularsi sotto traccia di inconvenienti, di errori che si manifestano senza una causa apparente ma che non per questo sono meno importanti.

**Le conseguenze si avvertono**, magari a macchia di leopardo, **sotto forma di fastidi intermittenti** - a maggior ragione difficilmente identificabili - con un'abilità del tutto tecnologica di nascondere il vero colpevole dietro una cortina di fumo di falsi positivi e di variegate possibili ipotesi che distolgono tempo e risorse allontanando la soluzione.

Nel frattempo si può dire che l'azienda continui a funzionare, certo. Ma si tratta di un **funzionamento rallentato o a singhiozzo**, che costringe il personale a interrompere il proprio flusso di lavoro riducendo la produttività e impedendo ai tecnici IT, indipendentemente dal fatto che siano interni o esterni, di concentrarsi sugli interventi maggiormente strategici (quelli che possono avere un impatto diretto sulla

redditività e sulla crescita dell'azienda, come upgrade, ampliamenti e introduzione di nuove funzioni) poiché costantemente impegnati a inseguire i problemi sperimentati dagli utenti rattoppando qua e là dove necessario fino al momento in cui si arriva al temuto collasso.

Qualche esempio aiuta a capire di cosa stiamo parlando.

Iniziamo da un dispositivo al quale molte aziende assegnano erroneamente un ruolo secondario sul palcoscenico della produttività: la stampante. Quante volte capita che un lavoro di stampa non si avvii perché **la stampante** - che magari, essendo in rete, si trova pure in un locale differente - è spenta nonostante sull'interruttore campeggi un adesivo che invita perentoriamente a "non spegnere la stampante!". **Il dipendente deve quindi lasciare la scrivania interrompendo il proprio lavoro**; poi, magari, quando torna e riprova a lanciare nuovamente la stampa, questa si interrompe a metà perché l'inchiostro è esaurito. Altro stop per chiamare il tecnico, sempre nella speranza che la sostituzione della cartuccia possa essere effettuata immediatamente e che non occorra attenderne il riapprovvigionamento.

Ecco allora che **una procedura che avrebbe dovuto svolgersi in modo automatico e trasparente** senza bloccare il lavoro del dipendente si è rivelata causa di un fermo produttivo tanto più grave quanto più sensibile è l'attività della persona coinvolta.

**Un'importante videoconferenza** con un cliente si rivela un penoso tentativo di carpire il senso delle parole che riescono a filtrare qua e là da una trasmissione che procede a scatti; la **terribile qualità** video rende inutile ogni tentativo di condividere lo schermo per presentare graficamente le informazioni di cui si sta parlando.

Possiamo imputare la colpa al generico "server" del fornitore del servizio, solo per sentirci dire che il cliente ha appena terminato un'altra videochiamata con il medesimo operatore senza incorrere in alcun problema: un modo gentile per dire che l'anello debole risiede nella nostra infrastruttura... non certo un bel biglietto da visita per la nostra attività!

È sufficiente un momentaneo **calo di tensione** dovuto a un temporale estivo o dei lavori stradali di fronte all'ufficio **per far saltare i server** nonostante siano protetti da gruppi di continuità?

Certo, forse **nessuno si è accorto che le batterie degli UPS hanno ormai superato la tempo la loro vita utile**, tanto da conservare una carica insufficiente persino per garantire lo spegnimento ordinato dei computer. E questo magari ci costringe, una volta riavviate le macchine, a richiedere l'intervento di un tecnico per ripristinare qualche server applicativo o di database che non riesce più a riavviarsi correttamente dopo l'improvviso e brusco spegnimento.

Non parliamo poi delle **applicazioni residenti in cloud**, di quelle erogate in modalità "as-a-service" e dei desktop virtuali: ci sono giornate in cui il funzionamento appare più lento del solito o va a singhiozzo senza che vi sia una causa certa.

Internet? Il cloud server? Il firewall? Il router? La macchina locale? **Le variabili sono davvero tante**, e l'impegno necessario per analizzare ciascuna di esse è ancora di più. Il risultato è che spesso **si finisce con l'accettare la situazione passivamente** "perché non se ne viene a capo" e "tanto in qualche modo si riesce a lavorare lo stesso".

Un atteggiamento fatalistico che fa a pugni con la necessità di far andare avanti al meglio un'azienda per competere su un mercato che non fa sconti a nessuno.

Ma bisogna per forza sottostare a una situazione del genere?

Certamente no, come testimoniano le **numerose aziende che hanno saputo evitare questi problemi semplicemente ricercando e implementando le soluzioni necessarie**.

**La parola magica qui è "monitoraggio"**, ovvero quell'insieme di tecniche che permettono di **tenere sotto controllo l'intero ambiente di rete** - tanto l'infrastruttura quanto tutto quello che vi è connesso - **così da rilevare automaticamente l'insorgere degli inconvenienti** quando non addirittura prevenirli.

A pensarci bene si tratta di una soluzione logica: quando la tecnologia diventa troppo complessa ed estesa per poter essere seguita da un essere umano non bisogna far altro che assegnare alla tecnologia stessa il compito di controllarsi da sé.

Accade quindi quello che siamo abituati a sperimentare quotidianamente con le nostre automobili, che ci permettono di concentrarci sulla guida liberandoci dall'incombenza di tutte quelle continue verifiche necessarie per evitare di trovarci improvvisamente in panne.

Se le strade non sono costellate di vetture che tutt'a un tratto si sono trovate senza benzina, senza olio o col motore grippato perché il radiatore non riusciva più a raffreddare, lo dobbiamo alle spie e agli indicatori che popolano il cruscotto del guidatore. Una rapida occhiata e sappiamo come regolarci, quando è opportuna una sosta per il rifornimento e quando invece è tempo di un rabbocco del lubrificante o di un tagliando vero e proprio.

Per un'azienda si tratta di arrivare a disporre di qualcosa di molto simile: un **cruscotto di monitoraggio che raccoglie costantemente dati dall'ambiente di rete** avvertendo quando l'inchiostro delle stampanti è prossimo ad esaurirsi, quando il firewall non riesce a smaltire con efficienza il volume di traffico in entrata e in uscita, quando la connessione Internet con l'esterno sta diventando insufficiente per le necessità degli utenti, quando le batterie del gruppo di continuità o degli UPS mantengono una carica inferiore al livello utile e così via.

C'è una ulteriore conseguenza positiva nella scelta di introdurre la tecnologia di monitoraggio all'interno della propria rete, ed è la possibilità di **estendere il controllo ad ambiti ai quali magari non si pensava nemmeno**.

Riflettiamoci un attimo: se diamo al nostro ambiente IT la capacità di riportarci puntualmente il proprio stato di salute, perché limitarsi alle cartucce dell'inchiostro e alle batterie degli UPS?

Ecco allora che un buon tool di **monitoraggio sarà in grado di abbracciare qualunque risorsa** fino a fornirci lo stato dettagliato dello spazio disponibile sugli **hard disk dei vari PC e ai livelli di RAM mediamente impegnati su ogni computer**. Insomma, si dice giustamente che "l'informazione è potere". Il monitoraggio di rete ci offre tutto il potere che ci serve per far funzionare al meglio il nostro parco informatico, a qualsiasi livello.

E il bello è che questa sorta di cruscotto IT non permette solamente di prevenire le interruzioni operative o andare a colpo sicuro quando si rende comunque indispensabile l'intervento di un tecnico.

**Ai risparmi di tempo e denaro** che tutto questo già comporta **si affianca infatti la capacità di dirigere gli investimenti IT verso le aree che effettivamente ne hanno necessità** o che possono restituire vantaggi maggiori (il famigerato ROI o ritorno dall'investimento) attraverso decisioni che non vengono più prese "a

naso" sulla base delle sensazioni e delle esperienze forzatamente limitata di qualche utente per quanto esperto, bensì su numeri oggettivi che non mentono e non sbagliano.

Risultato: fine delle spese inutili e aumento dell'efficacia dei budget impegnati.

Se tutto questo non fosse sufficiente, esiste un altro aspetto ancora che è importante ricordare quando si parla di monitoraggio di rete, ed è la **sicurezza**.

Un ambiente monitorato è un ambiente di cui è possibile desumere un profilo di funzionamento standard sulla base delle normali attività di sistemi e utenti.

**Un qualsiasi evento che non rientri nel consueto comportamento della rete è in grado di far suonare un campanello di allarme** per avviare immediatamente le verifiche del caso minimizzando in tal modo gli effetti di qualsiasi intrusione o azione errata, illecita o non conforme.

Di fatto, **il monitoraggio** rappresenta quindi una barriera che **aiuta a evitare danni ben più significativi** rispetto al motivo (il malfunzionamento della rete) per cui è stato messo a punto.

## UNA STRUTTURA ALLA PORTATA DI TUTTI

Intorno al monitoraggio di rete si sono sviluppati negli anni **strumenti davvero sofisticati** che **rendono più efficace, razionale e pianificabile il lavoro dei tecnici IT**.

**Attraverso questi strumenti un consulente esterno può acquisire all'istante una panoramica dell'intero parco installato di un cliente**, il cosiddetto inventario, scendendo quindi a un grado di dettaglio tale da permettergli di verificare ed eventualmente modificare la configurazione di ogni singolo dispositivo presente nell'ambiente.

Questa capacità di intervento attivo è essenziale per completare l'equazione del monitoraggio di rete permettendo di risolvere tempestivamente qualsiasi problema, errore, inconveniente o rischio evidenziato dal cruscotto di controllo. Periodicamente possono essere **prodotti report che riepilogano gli interventi fatti e la situazione corrente**, gettando così le basi per **decidere se, dove e quanto allocare del budget IT per potenziare e far evolvere l'ambiente**.

Anche delegando il monitoraggio all'esterno ricorrendo al modello del servizio gestito, è facile verificare la convenienza economica di una tale scelta considerando **l'impatto economico provocato da anche un solo episodio all'anno di blocco dei sistemi**: è sufficiente infatti moltiplicare la perdita del fatturato e il costo orario del fermo produttivo e del personale per la durata media dell'evento, che la maggior parte degli studi effettuati nel settore indica essere compreso tra 7 e 24 ore.

Ebbene, **il monitoraggio di rete si ripaga nei primissimi minuti di un singolo blackout operativo**.

Al di là di questo, **occorre poi valutare tutti i benefit direttamente e indirettamente quantificabili che derivano da un ambiente di rete ben funzionante** e dalla scomparsa di tutti quei grandi e piccoli fastidi che altrimenti punteggiano la nostra giornata lavorativa come negli esempi che abbiamo visto prima.

L'obiettivo alla fine è **fare in modo che l'ambiente IT sia uno strumento sempre disponibile** in maniera trasparente come un qualsiasi servizio di utility, e non un'altra potenziale fonte di grattacapi e problemi capace di mettersi di traverso rispetto al nostro lavoro.