



L'inizio dell'anno è l'occasione ideale per un check-up
della struttura informatica: dove occorre rinnovare, aggiornare o, semplicemente, riorganizzare.

► Di Simone Zanardi

SMALL BUSINESS

(RI)PARTIRE COL PIEDE GIUSTO

Anno nuovo, propositi nuovi: se vale per la dieta, per il lavoro e per le faccende di casa, questo motto si adatta altrettanto bene all'informatica, soprattutto in ambito professionale dove gli uffici e le piccole aziende possono cogliere l'inizio dell'anno come occasione per un'analisi della struttura Itc e identificare a mente fredda quali siano gli ambiti in cui è opportuno intervenire per migliorare l'efficienza non solo di Pc e connessione Internet, ma di tutto l'ambiente lavorativo.

Vista la congiuntura economica, non solo italiana, è fondamentale innanzitutto conservare uno sguardo d'insieme sull'intera struttura, in modo da individuare gli aspetti più critici sui quali intervenire con nuovi acquisti, quali debbano essere semplicemente riorganizzati e quali ancora non richiedano interventi immediati. In questo modo si può indirizzare il budget a disposizione sulle problematiche più urgenti e sensibili ed evitare sprechi che nessuno si può permettere.

Non tutti i consigli che troverete nelle prossime pagine devono quindi essere perseguiti contemporaneamente: le esigenze delle singole realtà variano in base all'ambito di business, alle dimensioni della struttura informatica e al personale impiegato. È bene ad esempio non farsi trarre in inganno dalle sirene

del marketing che spesso parlano di tecnologie rivoluzionarie come panacea di tutti i mali: big data, Internet of things, virtualizzazione, sono tutti argomenti potenzialmente interessanti anche per la Pmi italiana, ma spesso è necessario ripartire dalle basi, mettendo a punto una buona connessione a banda larga, aggiornando le policy di sicurezza dell'azienda o percorrendo i primi passi nel cloud, tutte problematiche che a volte si danno per scontate ma sono ancora mal gestite nel Belpaese. Il nostro approccio in questo contesto si è focalizzato sull'ufficio e la piccola azienda italiana che, per intenderci, non è lo Smb statunitense: secondo una ricerca della Cgia di Mestre dello scorso agosto, su 4.425.950 aziende italiane,

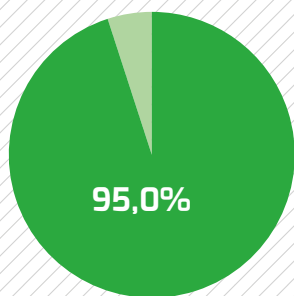
solo 105.431 (il 2,4%) è costituito da realtà con più di 15 dipendenti. Le dimensioni limitate non significano che

le piccole e medie aziende non possano trarre beneficio dalla tecnologia, anzi è spesso questa che consente di competere sul mercato con gruppi più grandi. Nelle schede che seguono ci siamo voluti concentrare sugli aspetti strutturali. Non si tratta quindi di una guida all'aggiornamento dei singoli personal computer, quanto di una panoramica degli aspetti più significativi che a nostro parere un responsabile It deve analizzare all'alba del 2015 in una piccola struttura informatica che vuole guardare al futuro.

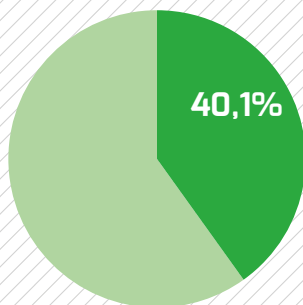
97,6%

La percentuale di aziende italiane con meno di 15 dipendenti

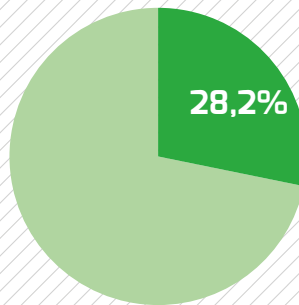
AZIENDE ITALIANE E TECNOLOGIA NEL 2014



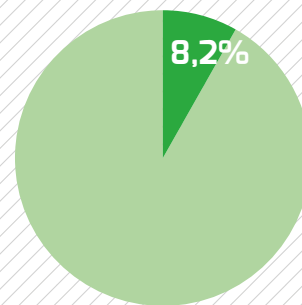
AZIENDE CON ACCESSO A BANDA LARGA



AZIENDE CHE INVESTONO NEL CLOUD COMPUTING



AZIENDE CON SISTEMI CRM DIGITALI



AZIENDE ATTIVE NEL CAMPO E-COMMERCE

CHECK-UP DELLA RETE

Pur con una complessità inferiore rispetto a quella delle grandi aziende, l'efficienza dell'apparato di un piccolo e medio ufficio dipende in modo intrinseco dall'infrastruttura di rete. Valutare una ristrutturazione o un aggiornamento in ambito It richiede quindi necessariamente alcune riflessioni sul network.

Tralasciando per qualche istante le considerazioni sulla connettività wireless, che rimandiamo alla prossima scheda, un primo esame deve riguardare il cablaggio dell'ufficio. Se il vostro ambiente di lavoro è ben predisposto, ad esempio con pavimenti flottanti e torrette di connessione, un eventuale aggiornamento del sistema di comunicazione interno è operazione relativamente semplice: il nostro consiglio è quello di sposare perlomeno la tecnologia Gigabit Ethernet, verificando innanzitutto che i cavi Utp che raggiungono le postazioni di lavoro siano come minimo di categoria 5e (la categoria identifica le caratteristiche trasmissive del cavo).

Nell'aggiornamento della rete ponete poi particolare attenzione all'aspetto topologico: se siete già al lavoro sulla posa dei cavi, badate che tutte le postazioni di lavoro siano raggiunte da una porta di rete (meglio sarebbero due porte per postazione).

L'inizio dell'anno è generalmente fuoriero di riorganizzazioni in termini di mansioni e di personale: dove possibile interpretate eventuali modifiche anche in ottica di struttura informatica, predisponendo la connettività cablata anche in locazioni che potrebbero tornare utili nel futuro prossimo. Se il vostro ambiente di lavoro non prevede già una struttura di



Gli Smart Switch rappresentano un compromesso tra switch gestiti e non, offrendo un livello di configurazione spesso ideale per le reti di piccole e medie dimensioni.

rete cablata, il nostro consiglio è quello di approntarla come mezzo di comunicazione preferenziale: proprio in una fase di mercato in cui proliferano i dispositivi wireless è infatti consigliabile che gli apparati fissi possano contare su di un collegamento via cavo, che non solo offre maggiore stabilità e prestazioni, ma evita di sovraccaricare la rete Wi-Fi che probabilmente dovrà gestire un numero già considerevole di terminali mobili.

In casi di ambienti di lavoro poco "cable-friendly", potete ricorrere a tecnologie alternative al cablaggio come il wireless o le Powerline (adattatori che consentono di collegare computer e altri terminali informatici attraverso la rete elettrica), o implementare delle canaline esterne, sempre che ciò sia consentito dall'architettura dei locali.

Dopo aver verificato la bontà della struttura cablata, è il momento di un check al centro-stella della rete, tipicamente situato nella sala server. L'elemento che aggrega e gestisce le connessioni provenienti dalle varie postazioni di lavoro è lo switch. Per valutare se sia opportuno aggiornare o meno questo

elemento sono necessarie diverse considerazioni. In primo luogo la velocità che deve essere gestita: se avete optato per un passaggio allo standard Gigabit Ethernet, il dispositivo dovrà chiaramente supportare questa banda.

Gli switch possono poi essere di tipo gestito o non gestito: questi ultimi sono apparati plug-and-play e non possono essere in alcun modo configurati, mentre gli switch gestiti offrono diverse opzioni tra cui l'aggregazione di banda, la possibilità di definire sotto-reti virtuali (Vlan), il filtraggio e la priorità delle porte, il controllo degli accessi. La maggior parte di queste funzioni sono sovradimensionate per la tipica piccola azienda italiana, ma alcune di esse (Vlan e aggregazione delle porte) possono tornare utili anche per applicazioni VoIP e Wi-Fi o per aumentare la banda di comunicazione verso il server centrale. Una volta scelto il tipo di switch, non siate troppo economi sulle porte: è bene prevedere un numero di connessioni libere per rispondere a esigenze di espansione future.



Un piccolo switch Gigabit a 5 porte può tornare utile per espandere la connettività presso un punto di rete già cablato.

Con la diffusione dello standard Gigabit Ethernet su rame, la connettività su fibra ottica è divenuta nella maggior parte dei casi sovradimensionata per le piccole aziende.

WIRELESS UPDATE



Sebbene in ambito aziendale l'utilizzo del computer desktop sia ancora consolidato, la spinta alla mobilità ha portato a una presenza più massiccia di dispositivi portatili anche in contesti professionali. Se nel caso dei Pc notebook la connettività wireless è spesso un'opzione alternativa al cavo, quando si parla di tablet e smartphone il collegamento alla rete locale deve avvenire necessariamente tramite una rete Wi-Fi. In quest'ottica è oggettivamente difficile immaginare un ufficio o un'azienda non ancora attrezzate con una Wlan (*Wireless Local Area Network*). Se siete tra i pochi rimasti a contare solo sul cavo, è bene non esitare oltre: non solo il Wi-Fi rende più versatile la vostra struttura di rete, ma trasforma l'azienda rendendola più efficiente e dinamica, sia nei rapporti di lavoro interni sia in quelli con clienti e fornitori. Anche se disponete già di una rete Wlan, il nuovo anno può essere l'occasione giusta per un aggiornamento degli apparati, in modo di rendere l'accesso wireless più sicuro, performante e scalabile.

La prima questione che dovete porvi è relativa alla copertura del segnale wireless ed è di conseguenza strettamente legata alla planimetria dell'ufficio o dell'azienda. Dare delle regole precise valide per ogni situazione è pressoché impossibile: i moderni dispositivi wireless sono in grado di operare con efficienza

anche in presenza di ostacoli come pareti portanti e strutture in metallo, ma rendono d'altro canto difficile prevedere la reale copertura senza un test sul campo. Con grande approssimazione potremmo dire che in un ambiente dall'area limitata (paragonabile a quella di un medio appartamento) potrebbe essere sufficiente un singolo access point, mentre per situazioni ad area maggiore o distribuite su due o più piani, la soluzione migliore è ricorrere a punti di accesso multipli. Il nostro suggerimento resta comunque quello di provare sul campo le varie zone di copertura, servendosi magari di un access point che già possedete.

Ricordate che l'impiego di un access point singolo ha dei limiti non solo in termini di portata del segnale, ma anche di utenti serviti: l'etere è una risorsa condivisa e in caso di accesso da parte di numerosi terminali le prestazioni possono degradare rapidamente, senza contare che gli access point entry-level potrebbero incontrare dei problemi computazionali nella gestione di numerosi collegamenti in contemporanea. Da questo punto di vista, un'azienda limitata a una decina di dipendenti e qualche ospite sporadico non rappresentano comunque un problema per un access point di medio livello.

In base a queste considerazioni, stabilite se la strada da seguire è quella del singolo access point o di un sistema wireless

Anche in caso di utilizzo di un access point singolo, è bene ricorrere a un modello dedicato professionale anziché a quelli integrati nei router di accesso forniti dagli Internet Service Provider.

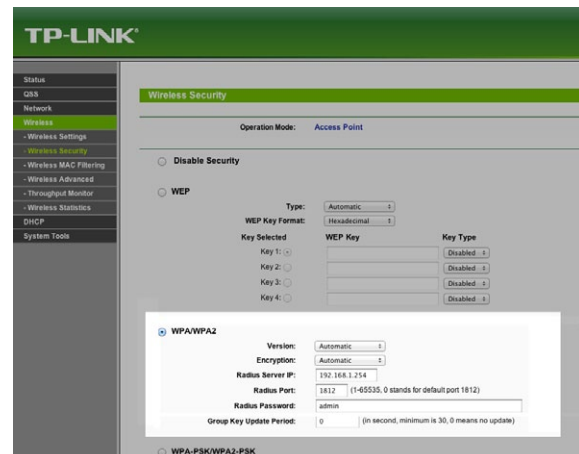
distribuito: quest'ultimo è di fatto costituito da un manager centrale collegato alla rete e da una serie di punti di accesso senza intelligenza periferica ma che vengono gestiti in modo unificato. In questo modo si possono distribuire con semplicità regole di accesso, parametri di sicurezza e aggiornamenti.

A prescindere dalla topologia scelta, due funzionalità wireless che possono tornare utili in ambito professionale sono certamente l'accesso guest e il supporto all'autenticazione degli utenti tramite server Radius. Il primo permette di definire una Wlan separata a cui fornire collegamento libero agli ospiti (clienti, fornitori o semplici visitatori). Questi possono accedere attraverso il Wi-Fi a Internet, ma non a risorse riservate come i server locali. L'autenticazione Radius consente invece di definire degli account separati per ogni utente della rete wireless, anche provvisorio. In questo modo se si rende necessario bloccare un account non è necessario intervenire su tutti gli altri con un cambio di password.

L'autenticazione tramite server Radius/802.1x consente di definire degli account specifici per l'accesso Wi-Fi da parte di ogni singolo utente.



I sistemi di gestione centralizzata della rete Wi-Fi consentono di configurare politiche di accesso condivise su access point multipli.





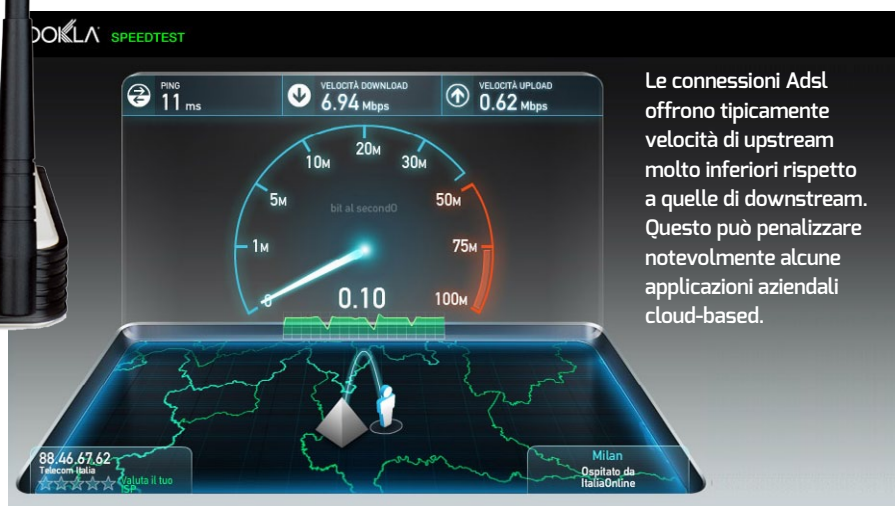
Molti router moderni dispongono di una porta Usb sulla quale è possibile agganciare una chiavetta 3G/4G per fornire alla Lan connettività Internet attraverso rete cellulare.



L'approccio alla tecnologia dell'informazione è sempre più cloud-centrico, anche in ambito aziendale: servizi di backup online, virtualizzazione delle macchine, hosting dei server di produzione e persino dei centralini telefonici VoIP sono solo alcuni degli esempi di come una rete informatica moderna non possa prescindere da una stretta e costante interazione con Internet. Per questo è fondamentale che l'accesso a banda larga a disposizione della Lan sia performante e affidabile. Se non siete soddisfatti del vostro attuale collegamento, il nuovo anno potrebbe essere l'occasione giusta per un cambio di provider.

Rispetto ai contratti tipicamente utilizzati in ambito residenziale, un accesso professionale deve in primo luogo poter contare su una banda minima garantita. Questa deve essere indicata per legge dal provider e rappresenta una sorta di salvaguardia quando la rete di accesso è particolarmente trafficata e quindi le performance di connessione degradano. Altro parametro a cui vi invitiamo a prestare particolare attenzione è la velocità in *upstream*, ovvero quella relativa alla trasmissione dei dati dalla vostra rete locale verso Internet. Nelle connessioni Adsl, le più diffuse in Italia, anche in ambito Pmi, questa è inferiore alla velocità di *downstream* ed è per questo meno pubblicizzata. Ricopre però un ruolo fondamentale nelle moderne applicazioni basate sulle comunicazioni online, che richiedono spesso massicci trasferimenti dati verso il cloud. Si pensi ad esempio

LA STRADA VERSO IL CLOUD



alla sincronizzazione di file su un account di gruppo Dropbox, o il backup di un disco su altri servizi di storage online. La velocità di upstream consigliata varia in base alle specifiche esigenze di ogni azienda, ma un ambiente moderno orientato al cloud con una decina di operatori non dovrebbe accontentarsi di meno di 1 megabit al secondo.

Analizzata la connessione a Internet dal punto di vista delle prestazioni, un altro elemento da tenere in considerazione è quello dell'affidabilità. In quest'ottica se la vostra azienda non può permettersi downtime, nemmeno sporadici, potreste considerare la sottoscrizione di un secondo contratto di connessione da utilizzare come backup in caso di guasti sulla linea principale. In questi casi è sempre opportuno che la connessione di ripiego non si basi sulla stessa tecnologia di quella principale: due linee Adsl, anche gestite da operatori differenti, potrebbero infatti essere vittime di un guasto fisico che blocchi entrambe. Per ovviare a interruzioni temporanee una buona soluzione è rappresentata dall'accesso Internet da rete cellulare: i network moderni 3G e 4G offrono velocità di tutto rispetto e molti router professionali possono interagire con le diffuse chiavette Usb degli operatori utilizzandole appunto

come interfaccia di *fail-over* alla linea Adsl o in fibra.

Se la connessione mobile non fa al caso vostro, ad esempio per problemi di copertura, un'alternativa più costosa ma anche più performante come linea di connessione secondaria è costituita da un Wisp (*Wireless Internet Service Provider*) che offra accesso tramite reti Hiperlan, WiMAX o satellitari. In questi casi le prestazioni, e i costi, possono essere paragonabili se non superiori a quelli di una linea a terra. Fortunatamente esistono router che permettono di utilizzare la doppia connessione a Internet non solo in modalità *fail-over* ma anche in *load balancing* ovvero sfruttano entrambe le linee per fornire la massima velocità disponibile a tutte le postazioni e applicazioni aziendali.

Oltre che un'alternativa, l'accesso Internet via satellite può essere un buon backup in caso di guasti sulla linea di terra.



SICUREZZA E ACCESSO REMOTO



Una buona suite di sicurezza installata su ogni personal computer della rete è indispensabile per proteggere dalle minacce provenienti dall'esterno e dall'interno dell'azienda.



All'alba del 2015 il problema della sicurezza della struttura informatica dovrebbe essere già stato affrontato da qualsiasi azienda o ufficio, a prescindere dalle dimensioni. Più volte su queste pagine ci siamo soffermati sugli aspetti legati alla protezione, ma nell'ottica di una revisione dell'intero reparto It come quella che ci siamo proposti è bene ricordare alcuni principi fondamentali.

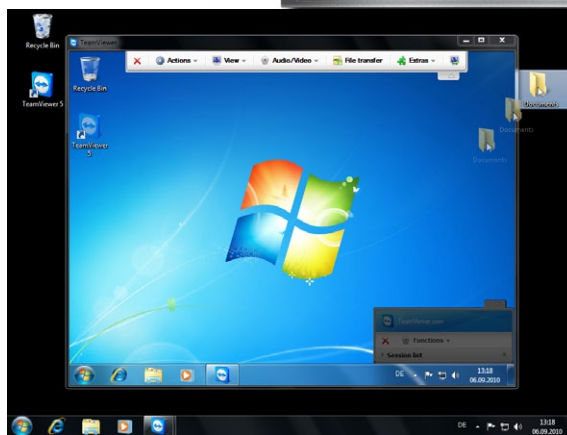
Innanzitutto, le minacce non provengono solo dall'esterno, ma anche dal personale che, anche involontariamente, può introdurre del codice maligno all'interno della rete locale. Da questo punto di vista è fondamentale che tutti i computer aziendali siano dotati di opportuni software antivirus e di sistemi operativi e applicazioni costantemente aggiornati. Sul mercato esistono numerose soluzioni atte allo scopo, anche in pacchetti completi comprensivi di assicurazione con rimborso in caso di mancati rilevamenti di minacce che infettano i computer su cui sono installati.

In ambito Pmi un problema di non poco conto può essere rappresentato dai dispositivi mobili, soprattutto quelli di proprietà dei dipendenti portati in azienda secondo il sempre più diffuso paradigma del Byod (*Bring Your Own Device*). Se non potete permettervi una soluzione completa di *Mobile Device Management*, il nostro consiglio è quello di inibire a questi dispositivi l'accesso

alle risorse aziendali più sensibili, imponendo inoltre al personale delle policy minime di sicurezza da adottare sui dispositivi utilizzati anche per lavoro (schermata di blocco con codice, wipe dell'apparato da remoto in caso di furto).

Una volta assicurata la compliance dei terminali alle policy aziendali, ci si può occupare della sicurezza periferica della rete. La parola d'ordine degli ultimi anni è Utm (*Universal Threat Management*) che identifica una serie di dispositivi in grado di garantire non solo protezione a livello firewall, ma anche ispezione dei contenuti tramite antivirus integrato, delle mail attraverso un modulo anti-spam, nonché il controllo dei siti potenzialmente dannosi sia per la sicurezza intrinseca sia per la produttività aziendale grazie ad opportuni sistemi di *Content Filtering* dinamico. Un dispositivo Utm ha un costo variabile che nel caso dei modelli Pmi può oscillare tra i 500 e i 1.000 euro, ma a questo va aggiunto l'abbonamento ai servizi dinamici appena citati che richiedono aggiornamento costante e interazioni con i database messi a disposizione dal security provider

Le appliance Universal Threat Management offrono protezione a 360 gradi contro i pericoli provenienti da Internet e integrano moduli per l'accesso sicuro da postazioni remote.



Il controllo remoto di un personal computer aziendale è spesso un'esigenza diffusa anche negli uffici di piccole dimensioni.

SERVER: SERVE ANCORA?

Un atteggiamento abbastanza comune nelle piccole aziende è quello di mantenere con una certa attenzione i personal computer e le stazioni di lavoro, trascurando spesso il server centrale che rappresenta invece una risorsa essenziale per la produttività della struttura informatica. Non è raro di conseguenza imbattersi in uffici e aziende che sfruttano come server un computer estremamente obsoleto, magari sovradimensionato ai tempi dell'acquisto originario ma oggi inadeguato alle esigenze, di affidabilità e prestazionali, del contesto.

Quando oggi si parla di server per piccole e medie aziende le opzioni a disposizione sono essenzialmente tre: aggiornare (qualora fosse necessario) l'hardware mantenendo invariato il software, passare a una nuova piattaforma software o eliminare del tutto il server per rivolgersi a una soluzione cloud-based.

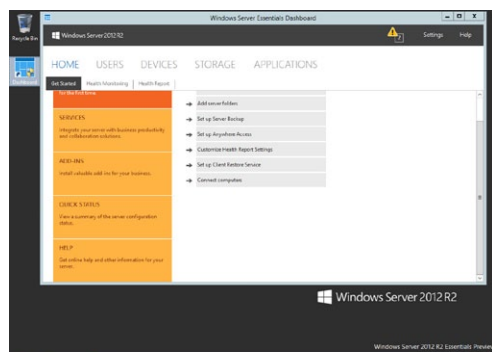
Per capire se il server aziendale debba essere sostituito o aggiornato è innanzitutto necessario stabilire quali applicazioni, e quindi quale sistema operativo, si devono utilizzare. Dopo l'abbandono ufficiale da parte di Microsoft di Windows Small Business Server, oggi le piccole

aziende che vogliono affidarsi a una soluzione proposta dalla casa di Redmond possono scegliere tra **Windows Server Essentials** e il nuovo approccio cloud di Office 365. Il primo è una versione limitata di Windows Server con licenza non scalabile e supporto a un massimo di 25 utenti (il prezzo indicativo è di 500 dollari). Da questo punto di vista è un prodotto più che adeguato agli uffici e alle piccole aziende italiane, ma va tenuto in considerazione che il pacchetto non include un server Exchange per la gestione di posta elettronica, calendari e rubriche. Un server Exchange può essere implementato su una seconda macchina (fisica o virtuale), ma la procedura non è sempre alla portata delle Pmi. L'hardware consigliato da Microsoft per un server Essentials prevede un processore a 3 GHz e 8 GB di Ram.

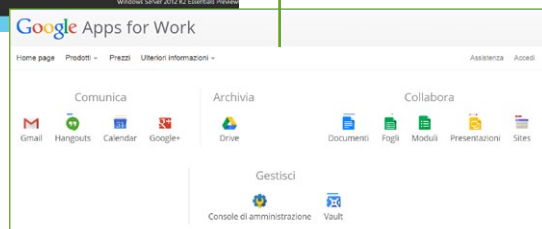
Restando in ambito Microsoft, l'alternativa a un server on-premise è la piattaforma cloud Office 365 Small Business. In questo caso il costo parte da 150 euro all'anno e la piattaforma può scalare sino a un massimo di 25 utenti. È compatibile con le soluzioni Exchange online che offrono le funzionalità di collaborazione estese. Sul fronte cloud l'opzione Micro-

soft non è l'unica percorribile: soluzioni altrettanto valide in tal senso sono rappresentate ad esempio da Google Apps for Work, Hyper Office o

Google Apps, una delle più diffuse suite cloud-based che include strumenti di comunicazione, collaborazione e produttività.



Windows Server Essentials: la soluzione Microsoft per organizzazioni sino a 25 utenti.



Zoho, tutte piattaforme che non solo offrono una serie di applicazioni equivalenti a Office, ma anche strumenti per la gestione della posta elettronica e della collaborazione.

Quale che sia il provider scelto, è bene valutare con attenzione il passaggio a una piattaforma cloud: questa elimina l'esigenza di un server fisico, vantaggio non da poco per una piccola e media azienda, ma richiede una costante interazione con il mondo online e quindi un accesso Internet affidabile e performante. Inoltre, se l'azienda deve utilizzare applicazioni espressamente pensate per l'installazione su computer, un server fisicamente presente in ufficio resta indispensabile.

Ultima, ma non meno importante è poi la strada Linux: tra le distribuzioni espressamente pensate per l'impiego su server Smb citiamo Igaware Small Business Server e Zentyal Smb Edition, mentre le piattaforme di collaborazioni paragonabili a Exchange sono ad esempio Sogo e Zarafa.

Se le esigenze di un server centralizzato si limitano all'utilizzo di storage condiviso e al backup delle stazioni di lavoro, si può infine considerare la strada Nas (*Network Attached Storage*), che con poco più di 500 euro permette di fornire all'azienda uno spazio disco con adeguate garanzie di affidabilità e prestazioni.



Un Nas è una soluzione ideale per la piccola azienda che necessita di un server come spazio per la condivisione di file e il backup.

ORGANIZZARE I BACKUP

Molti Nas supportano la copia di backup dei file su servizi cloud, come ulteriore misura di sicurezza per i dati aziendali.



Il backup dei dati aziendali è un aspetto della gestione IT tanto fondamentale quanto spesso colpevolmente trascurato. La ridondanza dei dati (oltre che dei dispositivi, come vedremo in seguito) è un fattore chiave per garantire continuità di servizio in caso di perdite o danni accidentali. Esistono numerose soluzioni per il backup dei PC e dei server di rete, che coinvolgono sia il software a bordo dei terminali sia i dispositivi e i servizi di network.

Per organizzare il backup dei personal computer è innanzitutto indispensabile selezionare un client di backup, o agente, che avvii periodicamente la copia di sicurezza dei file o dell'immagine di sistema. Windows 8 integra ben due sistemi di backup (Backup e ripristino di sistema, presente anche in Windows 7, e Cronologia dei file), ma sul mercato esistono numerose alternative gratuite e commerciali. Gli stessi produttori di Nas offrono generalmente un software

da installare sui personal computer della rete, con limiti di licenza variabili. Tra i numerosi pacchetti per il backup di personal computer meritano menzione Acronis True Image e R-Drive Image, che permettono di salvare immagini complete dei dischi di sistema, oltre a Easeus Todo Backup che supporta anche il backup incrementale e differenziale.

Una volta predisposto il terminale per l'esecuzione pianificata delle copie di sicurezza, il backup può essere effettuato verso diverse destinazioni, che possono coinvolgere vari dispositivi e servizi di rete. Una prima soluzione prevede la copia su un disco esterno collegato direttamente al terminale (ad esempio un hard disk USB). Questa opzione è in realtà difficilmente consigliabile in ambito business, dal momento che richiede un disco dedicato a ogni terminale o l'utilizzo a rotazione di uno o più unità, procedimento non solo scomodo ma anche poco efficiente e affidabile.

I Nas sono dispositivi ideali per la conservazione di copie di backup dei terminali; il supporto alle architetture Raid su più hard disk consente di conservare e accedere ai dati anche in caso di guasto sulle singole unità disco.



Un'alternativa certamente più adeguata agli ambiti aziendali è il backup su Nas (Network Attached Storage). In questo caso le copie di sicurezza dei file o dei sistemi sono conservate presso un server centrale, che dispone a sua volta di sistemi di protezione dei dati come architetture Raid per sopperire ad eventuali guasti sui singoli hard disk.

La terza via, sempre più diffusa anche in contesti professionali, è costituita dal backup sul cloud. Il vantaggio principale di questa soluzione è la delocalizzazione geografica: in caso di guasto catastrofico alla struttura informatica dell'azienda, il backup remoto è sempre disponibile per un ripristino immediato.

Le tre opzioni appena descritte possono essere combinate fra loro: un approccio diffuso ed efficiente consiste ad esempio nell'effettuare il backup principale dei terminali sul Nas aziendale, il quale opera poi a sua volta copie di sicurezza dei propri dati (e quindi anche dei singoli backup) su altri dispositivi Nas o direttamente sul cloud. La maggior parte dei Nas moderni supporta queste modalità secondo standard aperti e quindi interoperabili.

Oltre al backup in linea, è sempre opportuno effettuare per i dati più sensibili delle copie di sicurezza su media offline, che possono essere ad esempio dischi ottici (Dvd o Blu-Ray) o nastri. Lo scopo di queste copie è di quello di formare una sorta di archivio storico a cui ricorrere nel caso in cui tutta la struttura di backup in linea venga compromessa, ad esempio dalla propagazione di errori umani che cancellano o modificano file corretti.

TECNICHE DI BACKUP A CONFRONTO

BACKUP COMPLETO

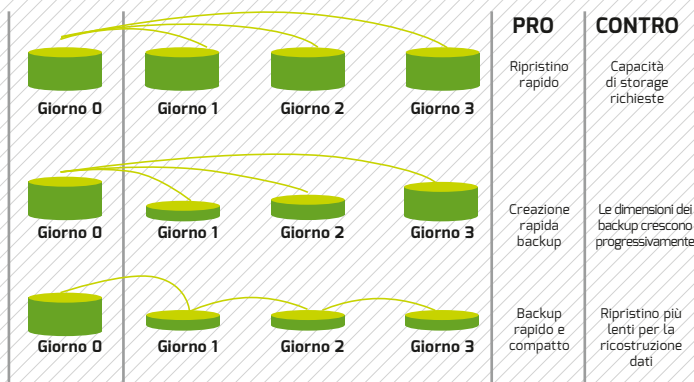
Ogni backup replica l'intera struttura dei dati.

BACKUP DIFFERENZIALE

Ogni backup conserva le differenze rispetto all'ultimo backup completo.

BACKUP INCREMENTALE

Ogni backup conserva le differenze rispetto all'ultimo backup (completo o incrementale).



PRO

Ripristino rapido

Creazione rapida backup

Backup rapido e compatto

CONTRO

Capacità di storage richieste

Le dimensioni dei backup crescono progressivamente

Ripristino più lento per la ricostruzione dati

UN ANNO SENZA INTERRUZIONI

Nelle pagine precedenti abbiamo già affrontato il problema della continuità di servizio che una rete informatica aziendale deve fornire a qualsiasi organizzazione per poter essere uno strumento e non un ostacolo alla produttività. Oltre che attraverso corrette procedure di backup e una buona pianificazione delle opzioni di collegamento a Internet, la continuità di servizio può essere garantita con una serie di accorgimenti spesso ignorati o sottovalutati dalle piccole e medie aziende, a partire dall'installazione di un buon gruppo di continuità, passando per gestione della ridondanza, sino ad arrivare alla disponibilità di pezzi di ricambio e attrezzi per un intervento immediato on-site in caso di imprevisti.

Un gruppo di continuità, o Ups (*Uninterruptible Power Supply*) mette al riparo uno o più dispositivi da cali o interruzioni di tensione sull'impianto elettrico che possono danneggiare i circuiti e portare alla rottura di parti hardware o alla perdita di dati. Oltre che dai black-out, i moderni Ups possono salvaguardare da picchi anomali di tensione, intensità o frequenza, altrettanto pericolosi per l'apparecchiatura. Non si limitano a proteggere

l'alimentazione, ma anche le connessioni di rete o telefoniche, anch'esse vulnerabili alle anomalie elettriche.

La scelta di un Ups dipende da numerosi fattori, ma in primo luogo è opportuno identificare quali e quanti siano gli apparati che devono essere salvaguardati: spesso le piccole aziende non proteggono con Ups tutta la struttura informatica, ma solo i dispositivi più sensibili e cruciali, come server di produzione e backup o workstation particolari. In base al carico che deve essere gestito dal gruppo di continuità, se ne identifica la capacità necessaria, ovvero la potenza massima sostenuta, espressa in Watt o Va (Volt-ampere) e l'autonomia, che dipende dal carico a cui l'Ups è sottoposto e dalle batterie in dotazione.

I gruppi di continuità si dividono poi in modelli off-line e on-line: i primi entrano in funzione solo dopo aver rilevato l'anomalia e generano quindi un piccolo "buco" (sino a una decina di millisecondi) in termini di alimentazione che può essere percepito dalle apparecchiature più sensibili. Gli Ups on-line utilizzano la cosiddetta doppia conversione e sono di fatto sempre attivi come fonte di alimentazione dei dispositivi a valle. Sono più costosi ma nettamente i più indicati per proteggere una struttura informatica sensibile. Gli Ups moderni possono interagire con gli apparati protetti, ad esempio tramite porta Usb, comunicando agli stessi lo stato dell'alimentazione

Nas e server possono essere dotati di doppio alimentatore per sopperire a guasti sulla singola unità.



Un gruppo di continuità mette al riparo gli apparati più sensibili da cali di tensione, blackout e anomalie sulla rete elettrica.

e sollecitando azioni automatiche. Un gruppo di continuità può così informare il server o il Nas della mancanza di corrente e "invitarlo" a una procedura di spegnimento morbido prima che l'autonomia dell'Ups stesso vada ad esaurirsi. Oltre che prevenire eventuali guasti, una struttura informatica può essere predisposta per farne fronte senza compromettere la continuità di servizio. La parola magica in quest'ottica è *ridondanza*: abbiamo già affrontato l'argomento in merito al collegamento Internet, ma un amministratore It può decidere di replicare qualsiasi dispositivo o struttura ritenga cruciale per la produttività: molti Nas e server, ad esempio, supportano le funzioni di high availability, ovvero l'installazione di due dispositivi sempre sincronizzati: il secondo apparato interviene a sostituire il primo in caso di malfunzionamenti. La ridondanza è un plus anche all'interno dello stesso apparecchio: così come le architetture Raid proteggono i dati dai guasti dei singoli hard disk, un doppio alimentatore permette ai server di operare in caso di rottura dell'unità principale.

Da ultimo: non scordate di munirvi di opportuni pezzi di ricambio per un intervento immediato in caso di guasto: tenete sempre a portata uno o più dischi per sostituire le unità danneggiate sui Nas, cavi di rete e alimentatori compatibili con i vostri server e workstation.



Non sottovalutate la disponibilità di pezzi di ricambio: in caso di guasto a un disco del server, ad esempio, la sostituzione immediata evita degradazione delle prestazioni e interruzioni di servizio.

