auroranetwork.it
internet solution provider

Piccola guida alle reti per le aziende

di Alessio Sperlinga – luglio/agosto 2011

http://www.auroranetwork.it

Sommario

Introduzione

Ho iniziato ad occuparmi di informatica nel 1987 e Il mio primo pc è stato un Amstrad 8086. In quel periodo nelle aziende cominciavano a diffondersi i personal computer e le reti fra computer cominciavano apparire ed erano così costose che solo le medie aziende potevano permettersele.

All'epoca l'informatica si usava per la contabilità e per la videoscrittura. C'erano già fogli elettronici e database, ma i costi del software erano ancora molto alti e la maggior parte del software era copiato.

Oggi le cose sono molto diverse, ad esempio sto scrivendo questo libretto con una tablet PC Samsung Galaxy con Android usando un programma gratuito di nome Evernote usando le dita su una tastiera .Questo computer permette di leggere la posta, di navigare su internet, di scattare foto e riprendere filmati, di registrare audio, di ascoltare musica e vedere film e fa da navigatore satellitare e da telefono.

Il problema è che l'informatica è diventata economica, semplice e portatile e nello stesso tempo inevitabile e complicata.
Tutti trovano comodo il cellulare e tutti litigano con telecomandi mostruosi. **Nelle aziende tutti si abituano ai servizi della rete locale, ma molti li ritengono troppo costosi e tutti si lamentano dei malfunzionamenti dei pc** e dei blocchi imprevisti dei servizi dai quali dipendono. Insomma è l'eterna lotta dell'uomo contro la macchina.

In mezzo ci sono le aziende come la nostra, che gestiscono le complessità delll'informatica , progettando le reti per raggiungere gli obiettivi operativi delle aziende e per renderle manutenibili evitando il più possibile fermi macchina, perdite di dati e problemi di sicurezza.

Con questo libretto vorrei tentare di dare qualche indicazione utile al lettore di qualsiasi età e grado di esperienza informatica per decidere serenamente cosa acquistare, quando e perché, insomma rendere misurabile il costo ed il vantaggio che l'informatica può dare, con un riferimento particolare alla piccola azienda che è sempre la più impreparata nelle scelte tecnologiche.

Le conoscenze per scegliere

La prima considerazione da fare **prima** di comprare qualcosa è che **la tecnologia cambia il nostro modo di fare qualcosa e quindi dobbiamo adottare solo la tecnologia che è utile per noi**.
Quindi quello che compriamo ci deve dare un vantaggio rispetto a quello che abbiamo.

Qual'è il vantaggio che ci possiamo aspettare da uno strumento tecnologico?
Un risparmio di tempo e/o un risparmio di spazio.
Ad esempio attraverso Google e Wikipedia risparmiamo tempo quando cerchiamo informazioni enciclopediche e attraverso i cellulari possiamo parlare con qualcuno senza spostarci. In un tablet PC o in una schedina di memoria possiamo mettere tantissimi libri risparmiando spazio e fatica di trasporto.

Quindi **«bello e nuovo» sono caratteristiche fondamentali per un vestito, ma sono irrilevanti per misurare l'utilità di una tecnologia**.
La tecnologia produce servizi e quindi va misurata nell'uso, il che è facile con le cose note e difficile con le nuove. Chi non ha mai usato un telefono non ne coglie il vantaggio finche' non lo prova.

Ad esempio se a casa usiamo il pc per navigare su internet, chiacchierare su Facebook, scrivere email e stampare foto, è più comodo un tablet PC di un pc, perché possiamo utilizzarlo seduti sul divano e non dobbiamo neanche comprare una linea Adsl perché basta una sim telefonica per navigare su internet, però la stampante anche se piccola deve poter funzionare senza fili (si dice wireless o Wi-Fi).

Insomma, i «guru» esistono perché la loro esperienza produce degli schemi di acquisto e scenari d'uso utili per noi.
Per esempio un ragazzo ha messo il suo curriculum su Google maps, inventando un nuovo modo di usare la possibilità di creare delle mappe

personalizzate e adesso lo fanno in molti e, soprattutto, lui ha trovato lavoro.

Insomma **l'abitudine è il peggior nemico dell'innovazione perché l'abitudine crea dipendenza e il nuovo spaventa**. Eppure tutti quelli che hanno cambiato provider sanno che è meglio avere un indirizzo email slegato dai provider per non doverlo cambiare ogni volta e non perdere l'accesso alle nostre vecchie email e perdere i contatti con chi ci scriverà ancora li.

Quando un'innovazione ci piace la trasformiamo in un'abitudine e ostacolerà l'innovazione successiva.

Quindi per riassumere in modo chiaro quanto sopra potremmo dire che prima di comprare qualcosa di tecnologico:
1) meglio chiedere un consiglio a chi ha più esperienza di noi o leggere qualche rivista.
2) rappresentarci in modo chiaro i vantaggi di una nuova tecnologia in termini di spazio, tempo e impatto sulle nostre abitudini.

Informatizzare una piccola azienda

A casa le cose sono relativamente semplici, tutti più o meno hanno due o tre televisori e telefoni, un pc o una tavoletta, stampante e console per giocare, router Wi-Fi ed accesso a internet, nelle aziende la situazione è meno caotica per quanto riguarda il numero di periferiche e più complicata per quanto riguarda i servizi , soprattutto, per quanto riguarda il software.

In sostanza **se un'azienda ha più di due personal computer comincia a diventare vantaggioso fare copie dei dati e della posta elettronica e condividere informazioni e servizi come l'accesso ad internet. Tutto questo è molto più semplice e soprattutto più sicuro se possiamo usare una macchina server.**
Server vuol dire servitore quindi una macchina che fornisce servizi ad altre macchine, ad esempio i Vostri pc detti client o terminali. Questo si fa attraverso una rete di fili oppure senza fili (Wi-Fi: ovvero una rete che usa onde radio) che permette a client e server di comunicare fra loro.

Una tipica rete informatica è composta da:
- uno o più server con un gruppo di continuità dedicato
- due o più personal computer
- un router
- un firewall
- un model adsl
- un sistema di salvataggio a cassette
- un armadio rack per contenere quanto sopra
- uno o più concentratori (switch) di rete con funzione di centralino per i collegamenti dei cavi e delle loro prese nei locali aziendali
- una o più stampanti con servizi multifunzione, fax, scanner e fotocopie poste in punti raggiungibili geograficamente da uffici contigui

e sempre più spesso
- uno o più unità di memoria chiamate nas o san per fare copie di salvataggio di macchine fisiche contenute anch'esse nell'armadio rack e

con un gruppo di continuità loro dedicato.

Tutto questo da solo non funzionerebbe senza il software, ovvero i programmi che rendono usabili i computer e ci danno servizi .
Tipicamente una rete ha dei software sul server che permette di condividere dei servizi:

- per l'accesso ad internet
- per la posta elettronica
- per i programmi di contabilità
- per ricevere e spedire fax sotto forma di file
- per proteggere il server da virus

Il sistema operativo del server permette di limitare l'accesso alle cartelle di memoria a particolari utenti e non ad altri, garantendo una riservatezza che un normale pc non permette.
Questo significa che per ogni utente deve esistere una Login, ovvero un nome ed una password.
L'utente amministratore può leggere e scrivere i dati di tutti gli utenti e leggere e compiere qualsiasi tipo di attività sul server.

I pc a loro volta devono essere dotati di software, ad esempio:
- antivirus e firewall
- programmi per scrivere e fare calcoli (office automation)
- programmi per ascoltare musica, vedere filmati e film su dvd
- programmi per scrivere (si dice masterizzare) cd e dvd
- programmi per vedere immagini e foto e per poterle modificare
- programmi per la posta elettronica e la navigazione su internet
- programmi per comprimere e decomprimere file (zippare e unzippare)
- programmi per leggere file acrobat, detti pdf, e programmi per convertire documenti in file pdf
- i programmi che consentono di usare periferiche come scanner e stampanti, detti driver

Un accenno alla sicurezza

Un problema aziendale **PERMANENTE** è quello legato alla sicurezza, sulla quale si sono versati fiumi d'inchiostro e alla fine è stato normato in Italia dal DL 196/2003 normativa sulla protezione dei dati personali che obbliga le aziende alla stesura di un documento programmatico sulla sicurezza (DPS).

Proveremo a descrivere in modo semplice cosa contiene la parola sicurezza per una rete aziendale, grazie al contributo di Francesco Trimarchi:

1) **Accessi** alla rete protetti da password e permessi di lettura e scrittura per singole persone (detti utenti) o gruppi di persone, tecnicamente si parla di identità e ruoli
2) **Protezione dei sistemi** da software malevoli e da intrusioni di estranei, questi programmi si chiamano worm o troian
3) **Protezione dei dati** e loro integrità, in altre parole una corretta procedura di copia dei dati, con ripetizioni quotidiane e periodiche e precauzioni come lo spostare le copie dei dati in un luogo fisicamente lontano dall'azienda

Tutto questo deve accadere senza che le reti si fermino, pena il blocco quasi totale dell'operatività dell'azienda. Questo richiede di mantenere sempre un certo livello di attenzione.

ACCESSI ALLA RETE
Tutti gli accessi alla rete devono essere resi sicuri con apposite regole e sistemi di protezione, i firewall sono le macchine specializzate in queste attività ed esistono anche sotto forma di programmi.
Tutti gli utenti autorizzati all'accesso devono essere muniti di apposite credenziali di autenticazione la cui password deve essere sufficientemente lunga e complessa e deve essere cambiata ad intervalli regolari.

Ogni utente deve essere responsabilizzato circa l'uso delle proprie credenziali e non le deve fornire a terzi se non in casi eccezionali e subito dopo è tenuto a cambiare la password nel più breve tempo possibile.

Gli accessi devono essere configurati perché un utente possa raggiungere soli i dati essenziali per lo svolgimento del suo lavoro e tutte le operazioni svolte sulla rete e tutte le operazioni devono essere opportunamente monitorate, cosa che di solito i programmi e i sistemi operativi fanno registrando ogni azione in uno o più file di diario detti file di log.
Tutti gli accessi dall'esterno, devono avvenire su canali protetti e criptati (VPN) in modo da garantire l'autenticità dell'operatore remoto. Questo significa che è possibile accedere alla rete aziendale anche da casa usando internet e dei programmi che devono essere presenti sia sul vostro pc sia sui server aziendali per rendere protetta la comunicazione.

PROTEZIONE DEI SISTEMI
Tutti i sistemi informativi aziendali devono essere protetti dai seguenti **pericoli**:

- **operazioni più o meno inconsapevoli da parte degli operatori**: tutti gli utenti devono essere configurati perché abbiano i privilegi minimi per poter svolgere le proprie mansioni
- **manomissioni da parte di eventi esterni** (malware e virus): tutti i sistemi devono essere protetti da programmi di sicurezza che monitorino tutti gli accessi e tutti i programmi in esecuzione in modo da bloccare sul nascere qualsiasi software dannoso; tutti i programmi dovrebbero essere periodicamente aggiornati ottenendo i file che compongono gli aggiornamenti di sicurezza dai produttori, questi file si chiamano fix, service pack, aggiornamenti
- **tutti gli accessi ad internet dovrebbero essere monitorati**, possibilmente con un firewall in grado di esaminare i dati in ingresso ed uscita, al fine di bloccare fuori dalla rete qualsiasi software malevolo.
- **problemi hardware**: purtroppo, ogni tanto, i sistemi informativi si rompono. Per minimizzarne l'impatto sulla produttività, tutte le

macchine strategiche devono essere protette da sbalzi di tensione mediante gruppi di continuità (detti UPS) e coperte da contratto di manutenzione con tempi d'intervento certi per la sostituzione delle parti presso la Vostra sede. Per i server, dove possibile, si prevede che le parti a rischio siano duplicate (si dice ridondate), ad esempio esistono metodi consolidati per duplicare l'alimentazione delle macchine e le memorie che contengono i dati, di cui sentirete parlare con varie sigle: raid, virtualizzazione, cloud.

PROTEZIONE DEI DATI

I dati sono il patrimonio dell'azienda: in caso di perdita, sottrazione o modifica fraudolenta le conseguenze sarebbero gravissime.
Uno degli aspetti più importanti della sicurezza prevede l'assicurarne la copia e l'integrità (vuol dire che siano completi e usabili) in modo da far fronte a qualsiasi evento catastrofico.
Tutte le azioni scritte sopra servono proprio per creare questa situazione.
La copia periodica di tutti i dati (si chiama backup) deve essere fatta su supporti esterni (dischi rimovibili, nas di rete, tape, repository internet, ecc.) da riporre in luoghi sicuri, possibilmente al di fuori dell'azienda.

Periodicamente è necessario provare a ricaricare (si dice ripristinare o fare il restore) i dati salvati in un ambiente di test e verificare che siano usabili.
Ove possibile, almeno una volta l'anno dovrebbe essere effettuato un test di verifica (si chiama disaster recovery) simulando che un server si sia rotto.

Gli aspetti economici

Le domande giuste secondo la nostra esperienza sono:

- Quanto costa l'informatica nella mia azienda ?
- Quant'è la vita media di una rete aziendale ?
- Come si misura il ritorno dell'investimento (R.O.I.) ?

Il modo più semplice di rispondere è che il costo di una rete è diviso in:

1) Rete fisica fatta di fili e di armadio rack e di concentratori (switch)
2) Il/i server con software,l firewall ed il router
3) I pc, i telefoni, smartphone e tavolette e le periferiche
4) Le persone per essere efficienti devono essere istruite e la formazione informatica incide per meno dell'1% sul costo del personale.
5) La 2) e la 3) hanno costi di manutenzione

La 1) è un costo di impianto e ha una vita media di 10 anni
La 2) è un costo da dividere su quattro, minimo tre, anni
La 3) è un costo da dividere su tre, massimo quattro, anni
La 4) è un costo di impianto e dura finché la persona lavora da Voi
La 5) è stimabile come costo di installazione iniziale e poi come costo annuo di manutenzione ordinaria in giornate di lavoro

Il ritorno dell'investimento dell'hardware si misura in termini di disponibilità di tutte le macchine al netto dei fermi e il ritorno dell'investimento del software si misura in produttività ovvero nella possibilità di eseguire una quantità di lavoro maggiore nella stessa quantità di tempo e con migliore qualità nel risultato.

Ecco uno schema di esempio sui costi per:

- Servizi di File Sharing con politiche di sicurezza su server
- Posta elettronica centralizzata
- Servizi di Office Automation
- Gestione Proattiva di Minacce di Sicurezza (Anti virus, malware, spam, ecc.) centralizzati.
- Gestione centralizzata Backup e DR (Disaster Recovery)

Costo di primo impianto (server, pc, firewall, s.o. e software applicativo): € 3.600,00 ad utente (investimento per 3 anni di circa 100 euro mese per utente)
Costo di manutenzione omnicomprensivo: circa € 360,00 annue/utente (circa 30 Euro mese per utente)

In generale, il costo complessivo di realizzazione e di manutenzione in efficienza di una rete informatica di una piccola-media aziende dai 10 ai 100 addetti, è di circa 130 euro mensili per posto di lavoro.