https://www.tecnosistemi.sv.it

Best practices per l'infrastruttura informatica

Frutto di oltre 30 anni di esperienza nel mondo dell'informatica, questo ebook raccoglie e sintetizza le best practice da implementare per avere una infrastruttura IT agile ed efficiente.
Nel corso della lettura andremo ad elencare le varie componenti presenti nella rete aziendali e ad analizzarne il modo migliore per utilizzarle, progettarle e sceglierle.

Linea internet

La linea internet è diventata il principale veicolo per lo scambio dei dati con il mondo esterno. Ne abbiamo la prova nella quasi scomparsadei fax, della corrispondenza cartacea e nell'invio e la ricezione in modo telematico dei documenti.

Visto la sua importanza possiamo fare alcune considerazioni.

Possibile ridondanza: In caso di infrastruttura strettamente dipendente da internet potrebbe essere necessario valutare l'installazione di una seconda linea, per evitare eventuali fermi dell'attività dovuti a qualche guasto o malfunzionamento sulla connessione principale.

Nel caso si decidesse di aggiungere una seconda linea internet sarebbe opportuno che la linea aggiuntiva fosse di una tipologia **diversa da quella principale**. Se abbiamo già una linea adsl o fibra, sarebbe opportuno affiancarne una di tipo wireless, per evitare che un guasto sul doppino o nella centrale possa coinvolgere entrambi le nostre connessioni anche se appartenenti a diversi operatori. Per dircela tutta, tanto rimane tra di noi, se una ruspa trancia un cavo del principale operatore telefonico il disservizio riguarda quasi tutti gli operatori e le connessioni, in quanto la quasi totalità dei provider si appoggia all'infrastruttura dell'operatore principale (avete capito chi è, vero ?).

Detto questo sarebbe opportuno avere gli strumenti per gestire in modo intelligente entrambe le nostre linee internet. Lo strumento migliore è il firewall UTM, del quale parleremo in seguito

Prestazioni: Un'altra considerazione è la valutazione delle caratteristiche tecniche della connettività. Oltre alla velocità di **download**, che è la velocità con la quale possiamo scaricare traffico dalla rete esterna, andrebbe valutata anche quella di upload, ovvero la banda che abbiamo a disposi-

zione per inviare materiale verso la rete internet (invio di email, file, etc). La velocità di **upload** diventa cruciale quando dobbiamo accedere dall'esterno a risorse interne dell'ufficio, per svolgere telelavoro, sfruttare il centralino voip per interni remoti o accedere a file e cartelle mentre siamo fuori sede.

Dimenticavo di dirvi che i parametri relativi alla velocità della connessione sono i valori massimi possibili e non quelli reali, effettivi e misurabili. Esiste un valore, definito BMG, che indica la **banda minima garantita**, cioè la velocità minima sia in download che in upload garantita da contratto, e che ogni operatore dovrebbe comunicarvi insieme alle altre specifiche. ***A voi lo hanno comunicato ?*** Scommetto di no.

Oltre alla velocità della linea andrebbe valutata la presenza o meno di un **IP fisso** assegnato alla navigazione; questo diventa importantenel caso dovessimo accedere dall'esterno a qualche risorsa presente all'interno della nostra rete locale. Facendo un esempio, se doveste accedere da remoto ad un server presente in azienda senza avere un IP fisso, sarebbe come se cercaste di consegnare un pacco ad un soggetto che cambia sempre indirizzo. ***E se non fosse possibile avere un IP fisso ?*** Beh, in questo caso si potrebbe usare un sistema di **Dynamic DNS**, da attestare sul router o sul firewall, ma questo è un argomento che andrebbe oltre alla funzione di questo ebook.

Come ultima considerazione consigliodi usare, quando possibile,un router di proprietà per avere libero accesso a tutte le configurazioni necessarie.

Cablaggio Lan

I cavi, oltre ad essere fonte di inciampo e di ingombro servono anche a fare transitare dati e informazioni all'interno della vostra rete locale. Ecco perché un cablaggio ordinato, oltre ad essere esteticamente piacevole, garantisce che non vi siano colli di bottiglia e che il flusso delle informazioni avvenga alla massima velocità possibile dall'hardware coinvolto.

Fatte questa premessa, per avere un cablaggio perfetto, tutti i cavi dovrebbero partire da un armadio rack e la parte stesa a pavimento, non dovrebbe essere calpestabili. Anche in assenza di rack, il cablaggio dovrebbe partire da uno switch(possibilmente a 1000 Mb/s) posto in posizione centrale da cui si diramano uno o più cavi per ogni periferica o postazione di lavoro, **evitando per quanto possibile l'aggiunta di altri switch aggiuntivi.**

Riguardo la parte**wireless**, ormai indispensabile in ogni ufficio, questa deve essere configurata per coprire in modo ottimale l'intera struttura, scegliendo il canale radio migliore,**evitando le impostazioni automatiche** e, nel caso fosse necessario più di un Access Point, configurando gli apparati in roaming, per consentire agli utenti di muoversi all'interno dei locali senza perdita di segnale.***Tutto qua ?*** No, però ci torneremo sopra parlando della sicurezza .-)

Sicurezza Informatica

Mantenere i datii**ntegri, riservati e disponibili** è, oltre ad un interesse personale, anche un obbligo di legge la cui mancata osservanza può portare a gravi e pesanti sanzioni.

Parlando di sicurezza informatica mi piace introdurre l'argomento prospettando il caso peggiore ***"immagina se i tuoi dati non esistessero più, cosa faresti ?"***Prima che la perdita di riservatezza, integrità o disponibilità diventino un problema, ti consiglio di prendere le precauzioni del caso.

Antivirus: l'antivirus deve essere **attivo e aggiornato**. Consiglio di installarlo, attivando solo le funzionalità essenziali ed evitando quelle aggiuntive (privacy, comportamento, personal firewall etcetc), questo per evitare che,in caso di rallentamenti o blocchi ingiustificati di applicazioni, l'utente abbia la tentazione di disattivarlo lasciandolo in tale stato. Consiglio anche di evitare le versioni free, spesso colme di pubblicità e difficilmente configurabili in modo granulare

Firewall UTM: l'uso di un firewall perimetrale è sempre una pratica saggia e raccomandata. Il firewall permette di **filtrare il traffico**, separando in modo fisico e logico la rete locale dalla rete internet. Oltre a discriminare il traffico permesso e vietato, sia in ingresso che in uscita, analizza e filtra il contenuto di ogni comunicazione, sfruttando i propri motori antivirus, antispam e antintrusione. In caso di telelavoro (smartworking) offre la possibilità di stabilire un canale criptato tra la macchina di casa e la rete dell'ufficio.Se abbiamo a disposizione più di una linea internet, il firewall ci consente di **gestire la connettività in modo intelligente**, lasciandoci decidere in base al tipo di traffico quale linea internet utilizzare,e cambiando automaticamente la connessione attiva in caso di guasto o mancata connettività (**failover**).

Facendo un esempio, potreste dedicare il traffico web alla linea1 e tutto il resto alla linea2, oppure assegnare la linea1 ad un gruppo di utenti e ad altri utenti la linea2. Fermo restando che, in caso di

guasto di una delle due linee, tutto il traffico verrà dirottato in modo trasparente sulla linea ancora funzionante, per poi tornare sulla linea originale al momento del ripristino del regolare funzionamento.

Password: le password, oltre ad essere un grattacapo, sono anche la prima barriera contro eventuali intrusioni o attacchi alla riservatezza dei dati. A questo proposito**le passworddevono essere complesse, cambiate spesso e non annotate su post-it appesi al monitor**. Bisognerebbe scegliere password diverse per ogni servizio e cambiarle immediatamentein caso di sospetto o sentore di compromissione. In caso sia presente un server windows, consiglio di configurare la policy di blocco account, che serve a bloccare l'utente in caso vengano inserite troppe password errate in un breve lasso di tempo. Come ultimo consiglio vi direi di bloccare lo schermo ogni volta che dovete lasciare incostudito il pc.

Beh, adesso puoi dirlo anche tu "ma a chi vuoi che interessino i miei dati ?" "Non puoi mai saperlo", ti rispondo io

Cryptare o proteggere con password le informazioni: mantenere riservate le informazioni oltre ad essereimportante è anche **più semplice di quanto voi possiate credere**.Con pochi click è possibile bloccare un documento con password o cryptarlo con una chiave. In entrambi i casi,inviando il documento al destinatario e **comunicandogli separatamente la chiave o la password**, potrete essere ragionevolmente sicuro che quel documento rimarràriservato.

A cosa potrebbe servire? beh, pensate ad un listino prezzi riservato ma anche a un elenco di indirizzi email, la copia di una busta paga, un contratto o qualsiasi altra cosa che potrebbe creare danno o imbarazzo nel caso venisse divulgata. **Un bella dimostrazione di serietà e professionalità ottenuta con un minimo sforzo.**

Ottima pratica è quella di creare, anche su una chiavetta USB, un disco virtuale protetto (per esempio utilizzando VeraCrypt) dove conservare tutti i file contenenti password e altre informazioni riservate.

Connessione WIFI: inutile dire che la connessione deve essere sempre protetta da password. Secondo la mia esperienza e secondo le best practice riconosciute, **andrebbero create una rete wifi privata ed una rete wifi pubblica.** La rete privata sarà destinata alle macchine aziendali che hanno bisogno di accedere alle risorse interne (notebook, tablet etc), mentre alla rete pubblica sarà concessa solo la navigazione internet. In questo modo potrete essere certi che, anche offrendo la connessione wifi a qualche ospite o visitatore, questi non potrà accedere ai dati presenti nella nostra rete locale.

Formazione: ricordate sempre che la maggior parte delle infezioni da virus e perdite di dati in generali avvengono per un **errore umano**. Detto questo potete capire che non esiste nessuna difesa che possa impedire all'utente poco attento di cliccare su un link malevolo o all'utente distratto di cancellare una archivio. In effetti una difesa esiste e si chiama formazione. Investire sulla formazione degli utenti, informandoli dei rischi, è **probabilmente la prima linea di difesa verso ogni tipo di minaccia.**

https://www.tecnosistemi.sv.it

Backup

Quando le cose sono andate male, ma veramente male, potete solo confidare nel backup… Il backup è come il paracadute di riserva, l'ultima speranza e la differenza tra la guarigione e l'estrema unzione.

Molti di voi fanno il backup dei dati ma non lo fanno nel modo corretto; Il rischio è quello di sprecare tempo e fatica effettuando salvataggi che si riveleranno inutili nel momento del bisogno.

Ecco le best practice per un backup ben riuscito

Discriminare innanzitutto tra i dati che cambiano di frequente e quelli che sono diventati statici. Per fare un esempio, ritengo inutile sprecare tempo e risorse per salvare ogni giorno i dati che non cambiano più: immaginate un archivio documentale storico o un vecchio programma gestionale che ormai usiamo solo per la consultazione. Per questi dati dovreste fare un backup una volta sola, magari in duplice copia, e archiviarne i salvataggi. Inutile salvare ogni giorno la stessa cosa, perdendo tempo e occupando spazio. Non siete d'accordo anche voi ?

Una volta fatta la selezione tra i dati che cambiano e quelli che non cambiano, scoprirete che è possibile fare backup efficienti in meno tempo e con più frequenza

Ma parliamo dei dati che cambiano, quelli che probabilmente impattano davvero sulla vostra attività di ogni giorno e riguardano testi, gestionali, email, archivi di indirizzi etc .**Questi andrebbero salvati almeno giornalmente o anche più frequentemente in caso di modifica massiva** degli stessi (immaginate un grosso consulente del lavoro, mentre sta elaborando decine di buste paga nei primi giorni del mese).

I backup vanno eseguiti possibilmente su un **NAS**(Network Attached Storage, o disco di rete), in una **condivisione protetta da password**dove solo il software di salvataggio è in grado di scrivere. Questo per evitare che un virus, infettando una macchina locale possa accedere ai vostri backup rendendoli inservibili.

Il software deve permettere l'invio di una notifica, magari per email, che segnali l'esito del backup e deve consentire la massima automatizzazione possibile per limitare l'intervento dell'operatore,

spesso pigro o distratto. Un altro consiglio è quello di conservare in altra sede una copia dei salvataggi, magari semplicemente copiandola su un disco usb e portandola a casa ogni weekend.

E il backup sul cloud ? La maggior parte dei software di backup ha già all'interno questa funzionalità e dipende solo da quali e quanti dati dovete salvare. Un ottimo compromesso potrebbe essere quello di salvare "anche" sul cloud alcuni dati e archivi importanti ma di piccole dimensioni. (archivi email, archivi gestionali etc)

Inutile dirvi che non è il caso di affidarsi a software gratuiti, spesso con funzionalità ridotte, o a chiavette USB come supporto di memorizzazione. ***Se doveste lanciarvi con il paracadute risparmierestesull'attrezzatura ?***

Telelavoro

Mai come adesso si sente parlare di telelavoro (diciamosmartworking, che suona più figo), e anche in questo caso ci sono delle best practice per **lavorare confortevolmente ed in totale sicurezza anche senza andare in ufficio.**

La macchina che utilizzate a casa dovrebbe avere prestazioni e caratteristiche adeguate allo svolgimento della nostra attività. E' possibile usare un tablet o uno smartphone per modificare un file dell'ufficio ma se il lavoro è più impegnativo dovreste pensare di utilizzare un personal computer anche tra le mura domestiche.

Per accedere alla rete dell'ufficio dovreste utilizzare una **VPN** (Virtual Private Network), ovvero creare un canale criptato tra la periferica domestica e la rete aziendale. Una volta stabilita questa connessione sarà possibile accedere in sicurezza alle risorse interne e scegliere il modo migliore per poterle utilizzare.

Non andrebbero mai effettuate connessioni che non siano all'interno di VPN per evitare che qualche malintenzionato possa sfruttare le vostre stesse porte di accesso e prendere possesso dei vostri dati. ***Non vi è mai capitato nullapur usando da sempre il desktop remoto per accedere al pc dell'ufficio ?****Bene, continuate a fare così, è solo questione di tempo prima che vi troviate le macchine criptate e una richiesta di riscatto in bella vista sul monitor.*

I vari **software di controllo remoto** come Anydesk, Iperius, Teamviewer, solo per citarne alcuni, sono nati per fare teleassistenza e non per accedere in modo continuoa un computer remoto non presidiato. Ogni volta che accedete alla vostra macchina usando questi software, i vostri dati tran-

sitano, **lasciandone traccia**, attraverso i server del gestore il quale agisce facendo da ponte tra il computer locale e il computer remoto. Immaginate cosa potrebbe succedere, tralasciandoi già citati problemi di privacy, se questa connessione sulla quale voi non avete nessun controllo potesse essere violata… Inoltre, immaginando che la maggior parte di voi stia utilizzando a torto la versione free, destinata ad usi non commerciali, in caso di furto o perdita di dati potreste essere sanzionati sia per la violazione della licenza d'uso del software che per la mancata adozione di adeguate misure di sicurezza per la minimizzazione del rischio.

Visto che la connessione viene effettuata tramite internet, **la banda disponibile deve essere sufficiente a garantire prestazioni accettabili**i. Potrebbe essere quindi necessario, durante le sessioni di telelavoro, disabilitare momentaneamente gli aggiornamenti automatici del sistema operativo ed evitare l'uso non necessario della nostra connessione (streaming, social etc).

Telefonia

Cambiano le tecnologie e le abitudini ma le persone continuano e continueranno a telefonare, cosa cambia realmente è solo il modo in cui la voce viene trasportata da un telefono ad un altro.

Tralasciando i dettagli sull'architettura voip che esulano dal fine di questo ebook, possiamo elencare alcune best practice per sfruttare al meglio queste nuove tecnologie.

La rete voce e la rete dati dovrebbero essere separate per evitare interferenze reciproche e problemi di audio; questa separazione può avvenire sfruttando lo stesso cablaggio ma utilizzando switch differenti.

In caso di interni remoti la banda in upload deve essere sufficiente a garantire una buona qualità della voce, ricordando sempre la regola aurea per la quale **se abbiamo problemi di audio disturbato è sempre dovuto alla connessione e se l'audio è monodirezionale il problema è sul NAT**. Ovviamente come connessione è inclusa anche la rete wireless domestica o aziendale dove si aggancia lo smartphone quando diventa un interno del centralino Voip.

La telefonia Voip, a differenza di quella tradizionale, non è legata a doppini, centrali e hardware dedicato e il numero di canali voce (chiamate contemporanee) assegnato ad ogni numerazione dipende dal tipo di contratto e dall'operatore.

Perché vi dico questo ?? Perché quando un provider vi propone di cambiare la vostra linea ISDN in numerazione Voip, spesso si dimentica di dirvi quanti canali vi saranno assegnati. Questo significa che, dopo avere

migrato la vostra borchia ISDN verso un linea voip vi potreste ritrovare con un solo canale telefonico anziché i due che avevate in precedenza. ***Io ve l'ho detto*** ☺

Gestione delle periferiche

Anche l'hardware vuole la sua parte, vero ? e come dargli torto ☺

I personal computer andrebbero per quanto possibile **tenuti aggiornati** e sostituiti circa ogni 4 anni; questo perché **i software cambiano e sono sempre più avidi di risorse**. Se non è possibile per vari motivi sostituire il computer,andrebbe valutato un aggiornamento per migliorarne le prestazioni, magari sostituendo il normale disco fisso con uno ssd di nuova generazione.

Per quanto riguarda il sistema operativo, dovrebbe essere sempre aggiornato all'ultima versione. E' vero che ci sono ancora in circolazione macchine con Windows XP ma è anche vero che ho visto utenti disperati, perché improvvisamente non potevano più fare Home Banking o cose simili, a causa di un aggiornamento non più disponibile per il loro sistema operativo.

Un'altra cosa consigliata,e troppo spesso trascurata, è quella di**cambiare sempre la password di default di router, firewall, nas e stampanti multifunzione**. Sì, avete letto bene, stampanti multifunzioni. Questo perché anche le stampanti sono delle vere e proprie periferiche intelligenti con a bordo portale web, ftp, ssh, etc, e come tali possono essere sfruttate per lanciare attacchi informatici all'interno della vostra rete locale. Senza trascurare il fatto che, qualche utente interno curioso e smanettone, potrebbe anche involontariamente cambiare qualche parametro provocando vari disagi e malfunzionamenti.

Dove salvare i dati

Questo ultima considerazione l'ho conservata per il finale, mettendola in fondo all'ebook sperando di non essere insultato solo per volere andare controcorrente.

Fatemi voi la domanda: "Cloud o non Cloud ?"

Secondo la mia opinione personale i dati, almeno quelli critici, andrebbero conservati **per quanto possibile in locale**. Una cosa sono le foto della comunione del nipotino, che possono anche essere parcheggiati sul google drive, e un conto sono i dati della mia contabilità che andrebbero conservati sul mio server aziendale. Questo perché, alla luce delle varie situazioni di emergenza, i cloud sono sempre più affollati e appetibili per i malintenzionati, e visto che la maggior parte dei server sono fuori dal territorio nazionale ho sempre timore che qualcuno decida di chiudere il servizio e tenersi i nostri dati.

Penso male ? Forse sì, però ci penso spesso.

E il gestionale sul cloud ? Beh, chi vi offre il gestionale vi dirà che così facendo non dovete preoccuparvi del server, del backup, degli aggiornamenti etc, senza dirvi però che, dal momento in cui i vostri dati gestionali sono sui loro server, **il rubinetto è definitivamente in mano loro**. Pensate cosa potrebbe succedere in caso di disaccordo relativo a pagamenti o aumenti unilaterali del canone. E se decideste di volere cambiare gestionale ?

Queste mie considerazioni le ho espresse in fondo all'articolo, in quanto sono e rimangono opinioni personali e vogliono essere solo uno spunto di riflessione basate sull'esperienza e nulla di più.

Spero che questo ebook possa esservi di aiuto. Ricordate che potete contattarci per consulenze e preventivi gratuiti.

Metteteci alla prova senza impegno e scoprirete come possiamo esservi utili

Buon lavoro a tutti ☺

Il Team di Tecnosistemi srl