La sicurezza secondo noi non è un prodotto, ma un processo.

La sicurezza del tuo sistema informatico necessita di continui aggiornamenti e attenzioni, proprio nel momento in cui pensi di avere messo i tuoi dati al sicuro sei a rischio per cui .....

Non abbassare la guardia !!!!!!!

Indice

Lesson 1: Mitm "Man In he Middle".

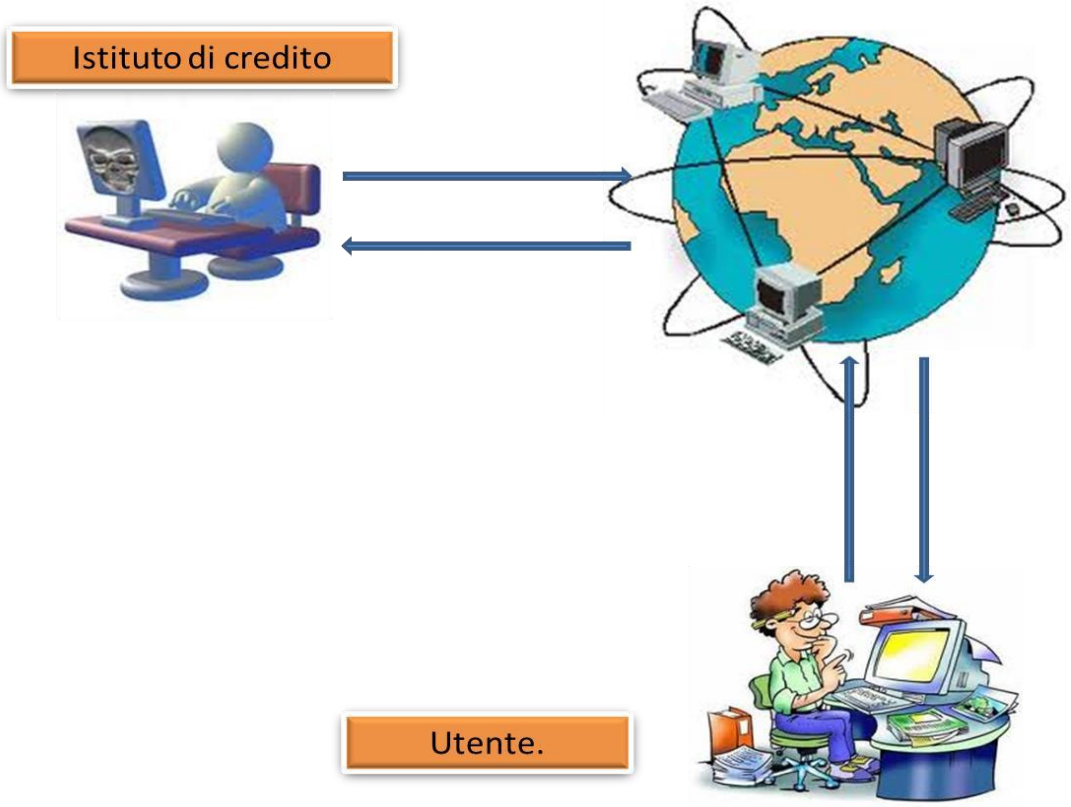
"Chi pensa di poter risolvere i problemi di sicurezza con la tecnologia, non ha capito i problemi e non ha capito la tecnologia".

EterNet
Vitalize your IT

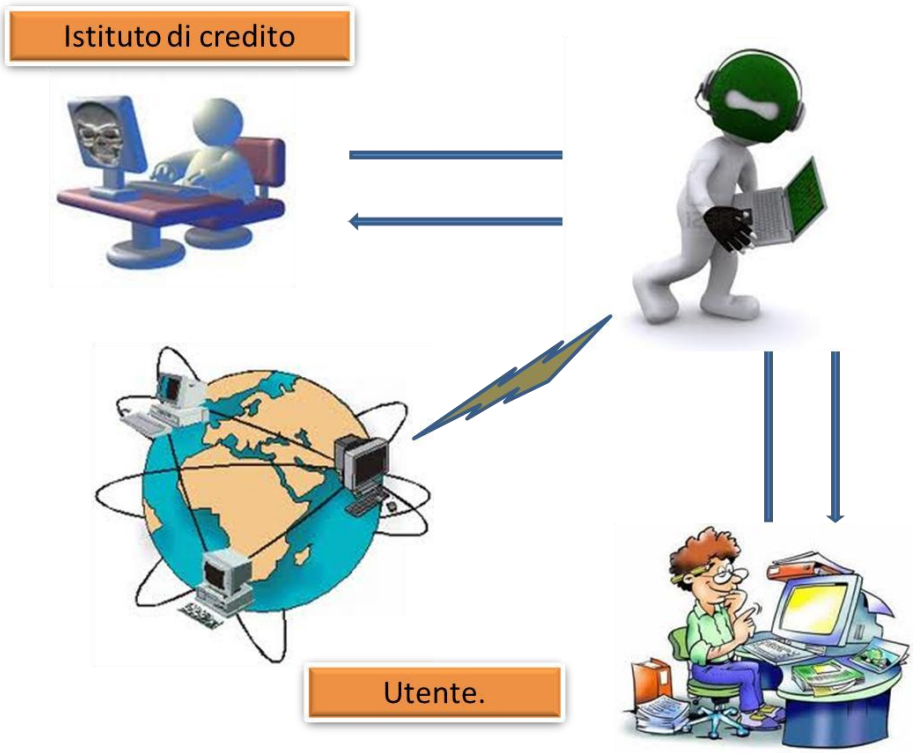
Iniziamo con il definire quando e perché si configura un attacco avente le caratteristiche del "Man In The Middle":

Questa tipologia di attacco **(uomo in mezzo)**, si configura solo quando l'attaccante mette in atto una serie di procedure tese a porlo di fatto nelle condizioni di leggere, inserire e modificare a suo uso e consumo i messaggi che intercorrono tra altri due utenti senza che nessuno di questi ultimi sia nella condizione di sapere che il collegamento tra di loro stabilito è stato compromesso da un terzo individuo, l'attaccante. In altre parole il malintenzionato, controllando a priori lo scambio di informazioni tra i due utenti, può volgere a proprio vantaggio la comunicazione sottraendo credenziali e dati personali agli ignari utenti. Durante un attacco si fatto l'hacker è in grado di sostituirsi in toto a un utente replicando la trasmissione dei messaggi, opportunamente modificati, verso uno solo od entrambi gli utenti.

Prima dell'attacco.



Dopo l'attacco.



I passi tipici di un attacco sono:

- Identificare il sistema da attaccare (per trovare il punto più vulnerabile e le modalità d'attacco).
- Ottenere un accesso utente (per penetrare nel sistema e tentare di ottenere accessi privilegiati).
- Ottenere un accesso privilegiato (per prendere il controllo completo del sistema tramite un attacco diretto a servizi o account con questi livelli).
- Coprire le proprie tracce (in modo che non sia possibile risalire all'attaccante e agli eventi esaminando i log del sistema).
- Installare backdoors (per rientrare nel sistema qualora venga individuato e/o eliminato il precedente metodo di penetrazione).
- Attaccare altri sistemi (una volta resosi anonimo e non individuabile).
- Prendere o alterare informazioni (presenti sulla macchina o sulla rete).
- Attuare altre attività non autorizzate (al fine di procurarsi un vantaggio o profitto).

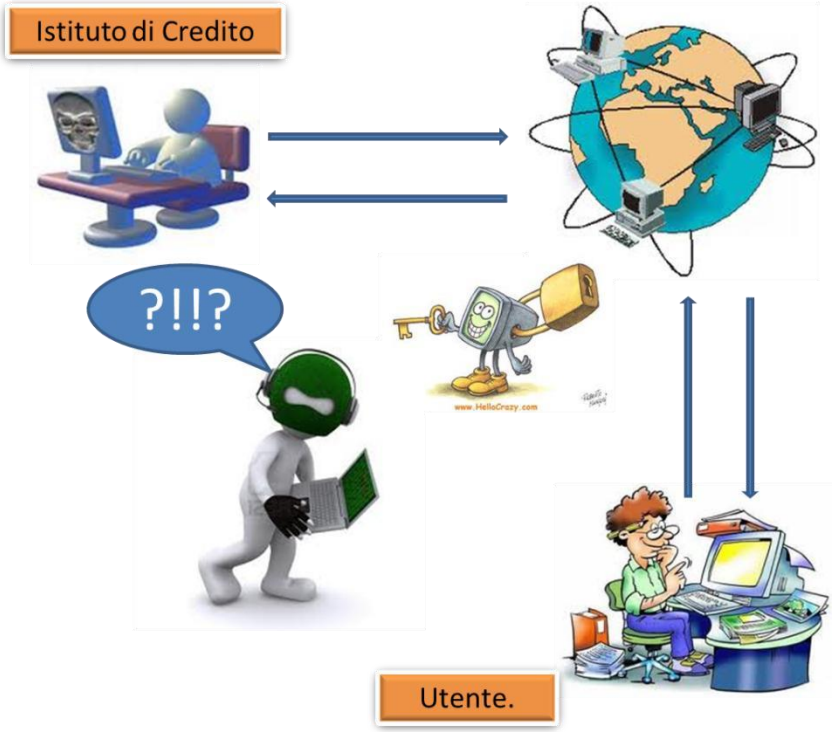
Supponiamo ora che tra i due utenti sopra riportati intercorresse una comunicazione criptata con scambio di Chiavi Pubblica e privata e vediamo come agisce il truffatore "Man In The Middle".

Esempio con scambio di chiavi pubblica e privata.

Supponiamo che il nostro utente intenda comunicare con il proprio Istituto di Credito tramite Home Banking per fare un pagamento e che il nostro malintenzionato, dopo essere riuscito ad ottenere in modalità truffaldina un accesso utente si sia posto nelle condizioni di spiare la comunicazione che avviene tra l'utente ed il suo Istituto di Credito. All'inizio della transazione l'utente deve chiedere all'Istituto di Credito la sua chiave pubblica. Quando L'Istituto di Credito invia la chiave il nostro malfattore, posto in mezzo, la intercetta ed inizia un attacco Man in the middle. Il malfattore invia semplicemente all'utente una chiave pubblica della quale possiede la corrispondente chiave privata. L'utente, credendo che questa sia la chiave pubblica dell'Istituto di Credito, cifrerà i suoi messaggi con la chiave del malintenzionato e invierà così i messaggi cifrati all'Istituto di Credito. A questo punto il malfattore è nelle condizioni di intercettare tutti i messaggi, di decifrarli, di tenerne copia, di alterarli e inviarli cifrati all'Istituto di Credito usando la chiave pubblica che l'utente gli aveva inviato in origine. In questo modo è possibile impartire all'Istituto di Credito ordini di bonifici verso conti correnti fantasma e contemporaneamente rassicurare l'utente con messaggi che gli facciano credere della buona riuscita dell'operazione impostata. E' possibile, in teoria, intraprendere un simile attacco nei confronti di qualsiasi messaggio inviato tramite tecnologia a chiave pubblica, e questo anche se gli utenti sono nella realtà dei computer o dei server che si scambiano pacchetti di dati trasportati da reti informatiche.

E' ovvio che, una volta svelata la modalità dell'agire truffaldino, è possibile instaurare una nuova procedura che di fatto impedisca l'azione criminosa; per cui, solo a scopo esemplificativo, di seguito un suggerimento per impedire quanto sopra spiegato.

Interlok.



Si tratta del protocollo conosciuto con il sinonimo "lucchetto intermedio", noto anche col nome di **interlock**. Funziona più o meno come segue:

L'utente invia il suo messaggio utilizzando per la cifratura la chiave ricevuta dall'Istituto di Credito ma solo per la metà della sua lunghezza. L'istituto di Credito a sua volta cifra il suo messaggio con la chiave ricevuta dall'utente e invia anch'egli solo una metà del messaggio. Soltanto quando l'utente riceve la metà del messaggio invia l'altra metà all'Istituto di Credito, il quale a sua volta invia la sua altra metà all'utente. **Il gioco è fatto!** Il trucco risiede nel fatto che, "**avere solo metà di un messaggio cifrato non consente la sua decifrazione**". Quindi, se il nostro malintenzionato intercetta entrambe le chiavi dell'utente e dell'Istituto di Credito non sarà comunque in grado di decifrare solo mezzo-messaggio (cifrato usando la sua chiave), e di re-cifrarlo e quindi inviarlo usando la chiave dell'Istituto di Credito. Dovrà gioco forza attendere la ricezione di entrambe le metà del messaggio, leggerle e spedirle, ma questo è possibile solo

componendo e quindi cifrando un nuovo messaggio. Così facendo potrà provare ad imbrogliare una sola delle due parti che alla transazione successiva si accorgerà dell'anomalia.

Un altro metodo per evitare un attacco MITM per i sistemi di cifratura a chiave pubblica è l'uso di **chiavi firmate**: se la chiave dell'Istituto di Credito fosse stata firmata da una terza parte, che si rende garante dell'autenticità, il nostro utente avrebbe potuto essere abbastanza tranquillo che la chiave firmata e ricevuta non avrebbe rappresentato un tentativo truffaldino.

E' infatti diffuso l'impiego di chiavi firmate (Autorità Certificante CA). Quanto citato è una delle strade primarie per rendere più sicuro il traffico WEB (HTTPS, SSL o protocolli Transport Layer Security).

Detto questo…… **"attenzione!!"**

Chiunque può rimanere vittima di un'intrusione o di un attacco!

Le ragioni di questa affermazione possono anche sfuggire a chi si considera "**low profile**" o non comprende bene l'importanza dei dati che custodisce sui propri sistemi.

Sono estremamente diffusi nelle comunità degli hacker tool che permettono di verificare con estrema facilità ed in breve tempo la presenza di determinate vulnerabilità partendo ad esempio da un elenco "**pseudocasuale**" di indirizzi IP (per esempio, tutti i domini.it, oppure tutte le macchine della subnet 151.4.*.*, etc.).

Spesso gli utenti ricorrono a soluzioni hardware e software per risolvere problemi di sicurezza specifici ma, proprio per la natura intrinseca delle problematiche, le soluzioni adottate diventano obsolete con il tempo in quanto continuamente superate dalla tecnologia.

Per questo non esiste e non esisterà mai una soluzione definitiva a questo problema.

La sicurezza di un sistema viene valutata a partire dalla resistenza del suo anello più debole, per ottenere un sistema che riesca a garantire al meglio gli obbiettivi di sicurezza richiesti, bisogna valutare nelle varie componenti del proprio sistema informativo i rischi che si vengono a generare, tenendo conto dei livelli di protezione che vengono garantiti.

Le informazioni che consideriamo banali o di scarsa importanza, possono risultare invece estremamente interessanti per altri, a tal punto che spesso si ignora quale sovrabbondanza di dati passi tramite le legittime informazioni considerate pubbliche:

- versione di S.O.

- Tipo e versione applicativi.
- Utenti e gruppi di lavoro.
- Configurazione zone DNS.
- Configurazione SMTP.
- Servizi di informazioni erroneamente accessibili come SNMP, NetBIOS, sunrpc, finger.
- Protocolli non sicuri come FTP, POP3, http.

Tutti i servizi superflui e le informazioni che sono liberamente accessibili diventano, nelle mani delle persone od organizzazioni sbagliate, un potenziale problema per la sicurezza dell'intero sistema in quanto rappresentano i dati o le porte d'accesso alla rete da attaccare.

L'atteggiamento di chi, pur essendo responsabile della sicurezza di sistemi informativi, confida nel fatto che proprio la non conoscenza o meglio ancora la diffusione di informazioni false lo possa aiutare a mantenere la sicurezza viene definito come "**Security through obscurity**". Questo atteggiamento è guardato con superiorità dai puristi della sicurezza che ritengono questo approccio del tutto inutile a garantire anche un ben che minimo baluardo contro gli attacchi informatici a cui una rete può essere sottoposta. Al di là del loro modo di pensare anche questo modo di agire può essere uno degli strumenti utili per ottenere lo scopo di sicurezza che ci si prefigge quanto meno nei confronti dei malintenzionati meno abili. Il rischio della brutta figura nei confronti di chi ti ha dato la responsabilità del sistema informativo è comunque molto alta.

Per questo motivo è comunque consigliabile impedire l'accesso a priori a tutte le informazioni superflue per mantenere la sicurezza dei sistemi.

Prendiamo ora come oggetto del nostro discorso una rete dati che sta alla base di un sistema informativo qualunque.

Questa è una rete che funziona.....ma.....!!!!!

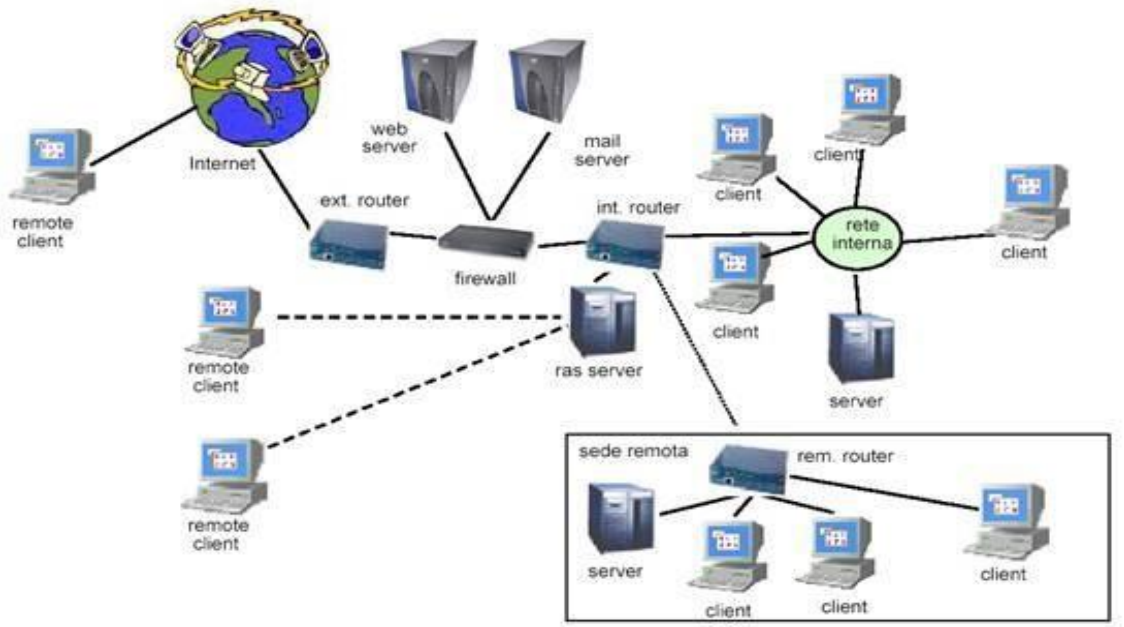


Figura 3 - Esempio architettura rete non "protetta" ....è sicura ?

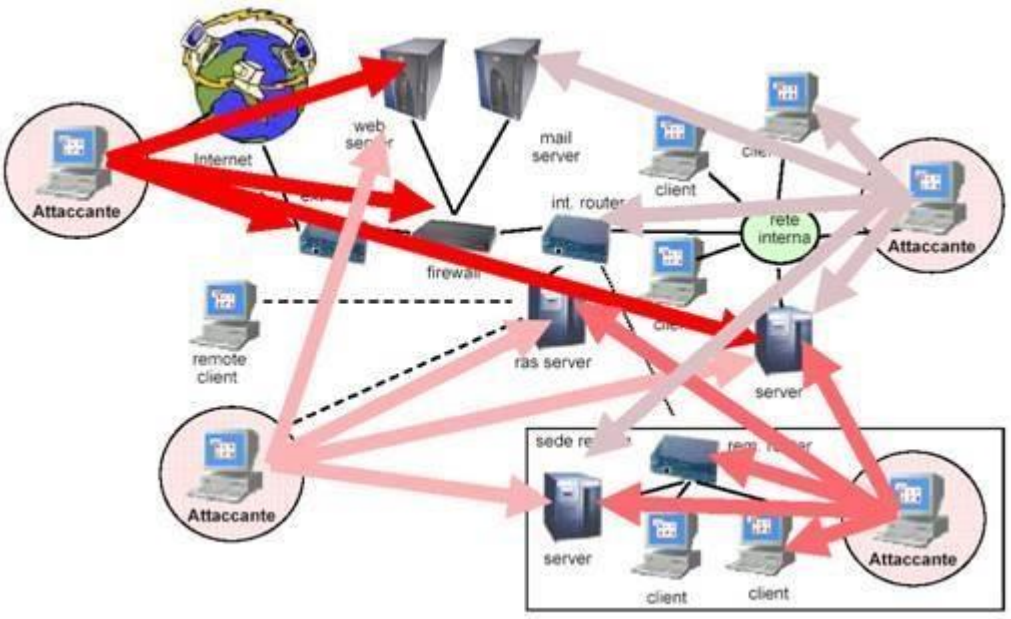


Figura 4 - Esempio attacchi all'architettura rete non "protetta"

Come si può notare dal disegno di rete sopra riportato, quella che Noi crediamo una rete sicura nella realtà ha una grande quantità di punti deboli attraverso i quali è possibile sferrare attacchi informatici.

Ricapitolando:

La tipologia di attacco che va sotto il nome di "man-in-the-middle" consiste nel dirottare il traffico generato durante la comunicazione tra due host verso un terzo host (attaccante) il quale fingerà di essere l'end-point legittimo della comunicazione. Il tipico attacco man in the middle è cosi strutturato:

- Gli attori sono la vittima, il cattivo ed il server dhcp.
- La vittima fa una richiesta di IP address.
- Al primo che risponde il cattivo assegna un indirizzo IP e un gateway che corrispondono ad una certa interfaccia.
- Vengono forniti insieme anche parametri utili a dirigere il traffico verso di noi.
- Da questo punto in poi tutte le comunicazioni della vittima passano dal cattivo.
- Il cattivo le legge e per non farsi accorgere di nulla le manda a chi le deve ricevere.
- Il cattivo riceve la risposta e legge anche quella.

Fare tutto ciò non richiede particolare destrezza ma basta ad esempio scaricare dal WEB uno dei tanti tools che consentono tali operazioni spesso addirittura automatizzate.

Quale può essere l'obiettivo dell'attaccante?

Rubare le credenziali oppure memorizzare tutto il traffico che un utente fa con un altro utente.

- Ma quali sono nel dettaglio le vulnerabilità di una rete informatica come quella sopra raffigurata?
- Come difendersi dagli attacchi?
- Esistono altre forme di pericolo per il mio patrimonio informatico?
- La legge chiede di proteggere i dati?
- Dove inizia e dove finisce la mia responsabilità? ➢ E poi …..ancora ???????????

Nei prossimi capitoli evidenzieremo a quali vulnerabilità si è esposti se i sistemi non sono configurati in modo opportuno, quali dati possono essere acceduti mediante questa tecnica e più nel dettaglio proveremo a dare una risposta alle domande sopra riportate.

Lesson 2: Protezione della posta elettronica e applicazioni core

La posta elettronica nelle Aziende

Il massiccio uso di Internet e della posta elettronica, in particolare, oltre a facilitare enormemente lo scambio di dati tra soggetti diversi, realizza di fatto una maggiore esposizione delle aziende verso l'esterno.

Questi strumenti elettronici ormai divenuti indispensabili per il flusso di documenti e di informazioni digitali, scambiate sia all'interno dell'impresa sia all'esterno con altre realtà, (aziende, enti, istituti di credito, ecc.) presentano però vantaggi e svantaggi. Mentre i vantaggi sono facilmente intuibili, vedi la riduzione dei tempi ed il conseguente abbattimento dei costi, gli svantaggi sono invece sostanzialmente legati al rischio di diventare vittima di attacchi informatici che insidiano la sicurezza dei dati e del business aziendale. In tale contesto, diventa indispensabile dotarsi di un piano di protezione, ovvero:

- adottare misure necessarie a bloccare i tentativi di intrusione da parte di soggetti, siano essi esterni o interni, non autorizzati nei propri sistemi;
- proteggere i dati in modo che le informazioni siano ben custodite e non corrano il rischio di andare perdute;
- evitare possibili danneggiamenti causati da una scarsa consapevolezza, sensibilità e formazione sul tema della sicurezza aziendale da parte del personale interno.

Nella lezione precedente abbiamo visto come la tipologia di attacco, che va sotto il nome di "man-in-the-middle", consente di dirottare il traffico generato durante la comunicazione tra due host verso un terzo host (attaccante), il quale fingerà di essere l'end-point legittimo della comunicazione. Questa attività presenta un elevato grado di pericolosità se applicata ad esempio alla posta elettronica o ad applicazioni core erogate in modo non conforme.

Per comprendere appieno come il servizio di posta elettronica possa divenire per un'azienda fonte di perdita o danneggiamento dei propri dati, è bene considerare che attraverso la mail passa ormai quasi il 100% delle informazioni aziendali. E' evidente quindi la centralità di tale servizio e di come sia importante proteggerlo. Per poter proteggere tale servizio è innanzitutto necessario capire come funziona.

Come viene erogato il servizio

Il primo passo per definire una strategia di protezione è la scelta di un servizio di posta elettronica, che può essere erogato in differenti modalità. Di seguito ne analizziamo le possibili alternative:

- a) scegliendo un provider esterno all'azienda che offra tale servizio;
- b) installando un proprio server presso una server farm di un provider;
- c) installando un proprio server nella propria server farm.

A) Affidando il servizio di posta elettronica completamente all'esterno, si decide di non applicare in autonomia nessuna policy di sicurezza, password escluse. Di conseguenza si sceglie di seguire il piano di sicurezza previsto dal provider per il servizio erogato. Oltre a questo, le modalità di recovery o di archiviazione della posta spesso non sono contemplate perché lo stesso provider non ha interesse ad implementarle.

B) Nel caso in cui si decida di installare un proprio server di posta elettronica in modalità Hosting, presso un provider, si avrà la possibilità di controllare l'intero iter di erogazione del servizio, comprese le policy di sicurezza. Per quanto riguarda l'archiviazione ed il recovery sarà necessario installare presso il provider o presso la propria organizzazione, dei server appositamente strutturati con un conseguente costo economico.

C) Installare il server di posta elettronica all'interno dell'azienda è sicuramente la soluzione migliore. Questa scelta comporta l'organizzazione di una struttura IT interna con persone dedicate. Nella propria server farm è possibile avviare i servizi sopra citati anche condividendo risorse già presenti e attive, rimane da affrontare solo il problema del "Disaster recovery", che qui accenniamo soltanto in quanto non oggetto della presente.

Ma vediamo ora come funziona la posta elettronica!

I protocolli di messaggeria (SMTP, POP3, IMAP4)

La posta elettronica è il servizio più usato su internet. Quindi la serie di protocolli TCP/IP utilizzati per l'erogazione del servizio offre una panoplia di protocolli che permettono di gestire facilmente l'instradamento (routing) della posta sulla rete. Il servizio di posta elettronica può essere realizzato tramite l'utilizzo di protocolli sicuri o non sicuri.

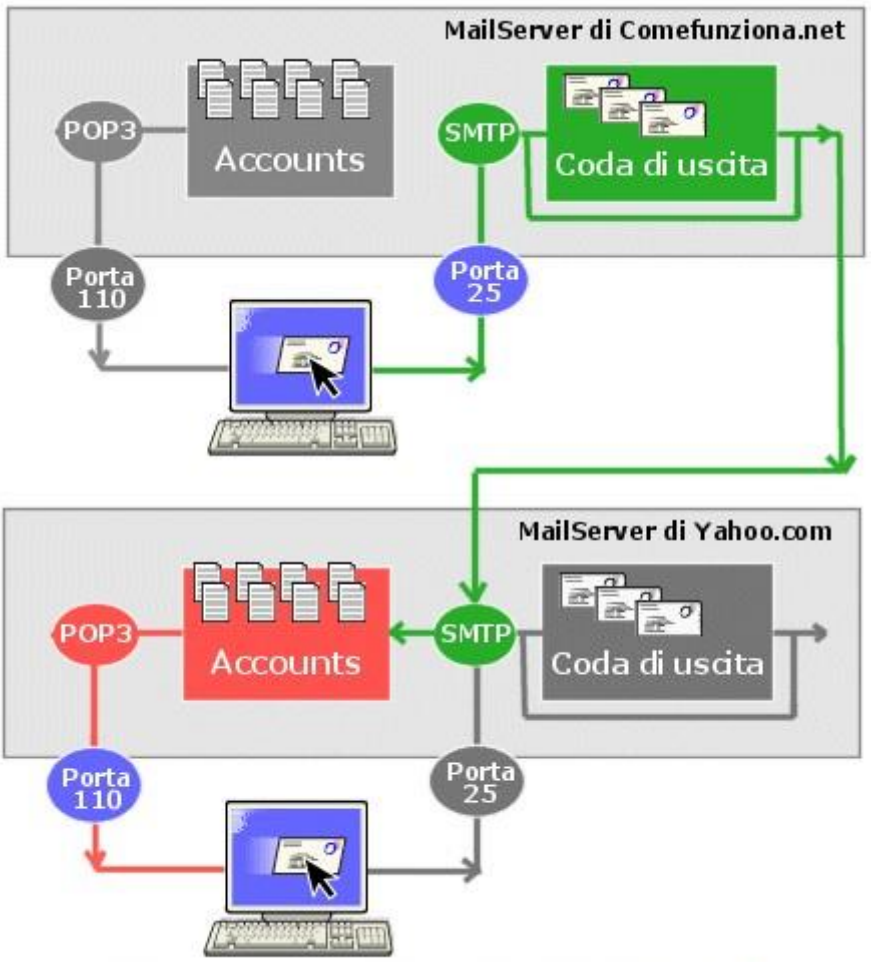
Protocolli insicuri:

- http,
- POP (porta TCP:110), ➢ IMAP (TCP:143), ➢ SMTP (TCP:25).

Protocolli sicuri:

- HTTP abbinato ad SSL,
- POP + SSL (porta TCP:995), ➢ IMAP + SSL (TCP:993), ➢ SMTP + SSL (TCP:465).

La prima considerazione da fare è quindi quella che diventa fondamentale per qualsiasi azienda, indipendentemente da come intenda erogare il servizio, e cioè analizzare quali protocolli sono o saranno utilizzati nel proprio servizio di posta elettronica.



Un disegno riasuntivo del viaggio compiuto dalla nostra eMail

Il protocollo SMTP

Il **protocollo SMTP** (*Simple Mail Transfer Protocol*, tradotto *Protocollo Semplice di* Trasferimento della Posta) è il protocollo standard che permette di trasferire la posta da un server ad un altro con una connessione point to point.

Si tratta di un protocollo funzionante in modalità connessa, incapsulato in una trama TCP/IP. La posta è consegnata direttamente al server di posta del destinatario. Il protocollo SMTP funziona grazie a dei comandi testuali inviati al server SMTP (per default sulla porta 25). Ognuno dei comandi inviati dal client è seguito da una risposta del server SMTP composta da un numero e da un messaggio descrittivo.

Ecco uno scenario di richiesta di invio di mail ad un server SMTP:

- All'apertura della sessione SMTP, il primo comando da inviare è "*HELO*" *(oppure EHLO)* seguito da uno spazio e dal nome del dominio del vostro terminale (come dire "buongiorno sono il tal terminale"), poi validare con invio;
- Il secondo comando è "*MAIL FROM:*" seguito dall'indirizzo e-mail del mittente. Se il comando è accettato il server rinvia il messaggio "*250 OK*";
- Il comando seguente è"*RCPT TO:*" seguito dall'indirizzo e-mail del destinatario. Se il comando è accettato il server rinvia il messaggio "*250 OK*";
- Il comando "*DATA*" è la terza tappa dell'invio. Esso annuncia l'inizio del corpo del messaggio. Se il comando è accettato il server rinvia un messaggio intermedio numerato "*354*" che indica che l'invio del corpo della mail può cominciare e considera l'insieme delle linee seguenti fino alla fine del messaggio individuata da una linea contenente unicamente un punto.

All'interno del corpo della mail ci sono poi altre informazioni contenute in campi appositi formattati in maniera diversa a seconda del client di posta utilizzato. Tali informazioni sono le seguenti:

- Date
- Subject
- Cc
- Bcc
- From

Se il comando è accettato il server rinvia il messaggio"*250 OK*".

E' possibile inviare una mail grazie ad un semplice telnet sulla porta 25 del server SMTP es: telnet smtp.pippo.net 25.

Il protocollo POP3

Il **protocollo POP** (*Post Office Protocol* tradotto con "*protocollo dell'ufficio postale*") permette, come indicato dal suo nome, di andare a recuperare la propria posta giacente su un server remoto (server POP). E' necessario a tutti quegli utenti che, non essendo connessi in permanenza ad internet, devono consultare le proprie mail off-line.

Esistono due versioni principali di questo protocollo, POP2 e POP3, alle quali sono attribuite rispettivamente le porte 109 e 110 e che funzionano attraverso dei comandi testuali radicalmente diversi.

Esattamente come nel caso del protocollo SMTP, il protocollo POP (POP2 e POP3) funziona grazie a dei comandi testuali inviati al server POP. Ciascuno dei comandi inviati dal client è composto da una parola-chiave, eventualmente accompagnata da uno o più argomenti ed è seguito da una risposta del server POP composta da un numero e da un messaggio descrittivo.

Comandi POP2

HELLO	Identificazione attraverso l'indirizzo IP del computer mittente.
FOLDER	Nome della casella da consultare.
READ	Numero del messaggio da leggere.
RETRIEVE	Numero del messaggio da recuperare.
SAVE	Numero del messaggio da salvare.
DELETE	Numero del messaggio da cancellare.
QUIT	Uscita del server POP2.

Comandi POP3

USER identificativo	Questo comando permette di autentificarsi. Esso deve essere seguito dal nome dell'utente; cioè da una stringa di caratteri che identificano l'utente sul server. Il comando USER deve precedere il comando *PASS.*
PASS password	Il comando *PASS* permette di indicare la password dell'utente il cui nome è specificato da un comando *User* precedente.
STAT	Informazione sui messaggi contenuti sul server.
RETR	Numero di messaggi da recuperare.
DELE	Numero di messaggi da cancellare.
LIST [msg]	Numero di messaggi da visualizzare.
NOOP	Permette di mantenere le connessioni aperte in caso di inattività.
TOP <messageID> <n>	Comando che visualizza *n* linee di messaggio, il cui numero è dato in argomento. In caso di risposta positiva da parte del server, questo rinvia le intestazioni del messaggio, poi una linea vuota e infine le *n* prime linee del messaggio.
UIDL [msg]	Richiesta al server di rinviare una linea contenente delle informazioni sul messaggio eventualmente dato in argomento. Questa linea contiene una stringa di caratteri, detta *listing d'identificatore unico*, che permette di identificare in modo univoco il messaggio sul server, indipendentemente dalla sessione. L'argomento opzionale è un numero corrispondente ad un messaggio esistente sul server POP, cioè un messaggio non cancellato.
QUIT	Il comando *QUIT* chiede l'uscita del server POP3. Esso implica la cancellazione di tutti i messaggi segnati come eliminati e rinvia lo stato di questa azione.

Risulta a questo punto evidente che il protocollo POP3 gestisce l'autentificazione tramite il nome utente e la password. Questa modalità di autenticazione **non è sicura** in quanto, come la mail, anche nome utente e password sono in chiaro (in modo non cifrato) e quindi facilmente intercettabili. Così come è possibile inviare una mail grazie a telnet, si può anche accedere alla propria posta grazie ad un semplice telnet sulla porta del server POP (110 per default):

Es:"telnet mail.pippo.net 110"

Immaginate a questo punto un malintenzionato venuto in possesso della vostra username e password… cosa può fare se il vostro sistema di posta utilizza i protocolli sopra descritti?

Il protocollo IMAP

Il protocollo **IMAP** (*Internet Message Access Protocol*) è un protocollo alternativo al protocollo POP3 ma che offre molte più possibilità:

- IMAP permette di gestire più accessi simultanei.
- IMAP permette di gestire più caselle postali.
- IMAP permette di smistare la posta secondo più criteri. ➢ IMAP **permette di criptare le password**.

Al di là delle caratteristiche del protocollo è subito evidente che il dato più eclatante è appunto quello di impedire il transito in chiaro delle password in modo da rendere inutile l'operazione di monitoraggio "Sniffer" da parte dei malintenzionati.

Le applicazioni Core

Quanto espresso per il servizio di posta elettronica è purtroppo valido anche per tutti gli accessi ad applicazioni e servizi pubblicati in modalità non sicura spesso necessari se non addirittura vitali per le aziende. A questo punto dare l'accesso a portali WEB, permettere lo scambio di informazioni via internet, consentire l'accesso remoto, utilizzare sistemi di messaggistica (facebook etc…), ci consente di stare tranquilli? Per le applicazioni diverse dalla posta elettronica che protocolli si usano? Che grado di sicurezza hanno?

Proviamo a fare un po' di chiarezza. Anche in questi casi i protocolli maggiormente utilizzati dalle aziende per accedere a determinate applicazioni sono da suddividere in sicuri e non sicuri.

Protocolli insicuri:

- http,
- FTP,

- Telnet,
- PPTP,
- VPN,
- ICQ,
- SNMP ver.1 e 2

Protocolli sicuri:

- HTTP abbinato ad SSL,
- FTPS o SFTP,
- SSH (non basato su SSL ma concettualmente similare),
- PPTP su SSTP VPN,
- Client di messaggistica istantanea configurati per l'uso di SSL,
- Skype (uso di PKI proprietario),
- Uso di SSL-VPN,
- L2TP (impiego di certificati digitali lato server e lato client),
- IPSEC (certificati digitali lato server e lato client oppure utilizzo di chiavi scambiate inizialmente),
- tunneling SSH VPN.
- SNMP ver.3

Il furto di credenziali

Utilizzando i protocolli non sicuri appena menzionati, sia per le applicazioni di posta elettronica che per quelle Core, è possibile con azioni di tipo "man in the middle" (descritte nella lezione 1) acquisire le credenziali dall'interno o dall'esterno della rete da cui l'utente si connette alla propria casella di posta elettronica o ai propri server applicativi.

Durante gli audit eseguiti anche in organizzazioni di rilievo, ci siamo trovati sovente di fronte a realtà molto diverse tra loro. Alcuni provider ad esempio Aruba, qui citato solo in quanto molte

aziende gli affidano il proprio servizio di posta elettronica, non offrono un servizio di **secure mail**. Tutto il traffico viene infatti fatto transitare in chiaro inclusa la posta elettronica esponendo i propri utenti al rischio sopra citato.

La stessa cosa accade per il traffico dei dati contenuto sui server posti in hosting all'interno della server farm (Web Server). A seguito di un'analisi fatta il traffico da e verso tali web server è in **http**. Lo stesso Facebook non supporta appieno tutti i protocolli di sicurezza e si corre il rischio di farsi intercettare le proprie credenziali. Anche in questo caso la citazione è fatta solo perché molto utilizzato all'interno delle aziende.

Molti portali aziendali consentono l'accesso ai propri utenti o ai clienti in modalità non protetta. Se i dati a cui si accede sono importanti o addirittura fondamentali (pubblicazioni di listini, acquisizione ordini, etc…), sarebbe buona norma proteggerli. In moltissimi casi però, non solo sono completamente privi di protezione ma addirittura le persone preposte alle strutture informatiche non sono a conoscenza delle falle e della legislazione in materia.

Rendere sicuri i dati genera un'immagine più sicura della propria azienda a tutti gli utenti fruitori dei servizi oltre a preservare i responsabili da pesanti azioni penali.

E' bene riflettere che permettere di entrare in possesso di username e password può purtroppo rappresentare per il malintenzionato la possibilità concreta di avere in un solo colpo l'accesso a tutti i servizi dell'azienda, in quanto è diffusissima la pratica di usare una sola password in modo da non dimenticarla. **Pessima abitudine……!!!!!!!!!!**

Un altro servizio diffusissimo in tutte le organizzazioni è quello rappresentato dal server FTP. Questo servizio viene implementato per consentire lo scambio di file tra organizzazioni diverse, tra utenti della stessa organizzazione e in generale tutte quelle volte in cui sia necessario spostare grosse quantità di dati, che con la posta elettronica non è consigliato inviare. L'accesso a tali server avviene spesso in modalità non protetta, correndo il rischio di facilitare l'acquisizione di dati e delle relative credenziali di autenticazione. Questo processo è alla base del furto o del danneggiamento delle informazioni contenute nei server.

Cos'è l'FTP e come funziona

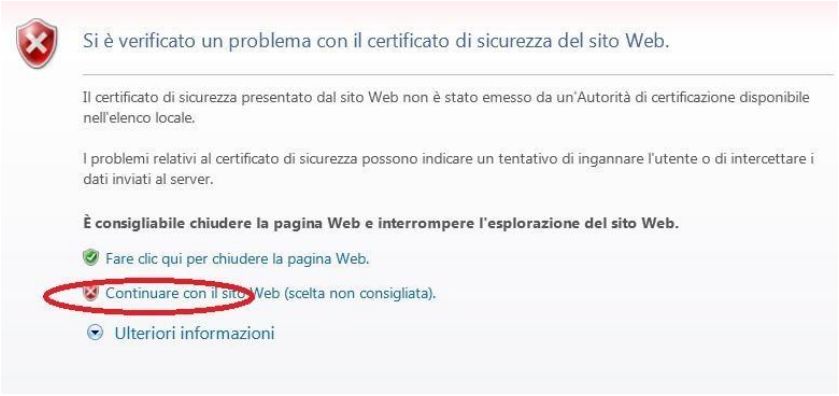
L'FTP (File Transfer Protocol) è un sistema di comunicazione datato, estremamente semplice da implementare e per questo molto usato da parte degli utenti. Questa combinazione lo rende preferibile ad altri sistemi più avanzati ma sicuramente più complessi. La struttura del protocollo consta di pochissimi comandi attraverso i quali è possibile impostare permessi, eliminare o spostare file, caricare o scaricare dati, mostrare il contenuto di cartelle e directory e via dicendo.

Trattandosi di un sistema ormai datato presenta alcuni problemi, il più grande dei quali è rimasto il sistema di trasferimento dei dati, tra il client ed il server. Il protocollo utilizza due distinti canali di comunicazione, il primo per lo scambio dei comandi che viene aperto alla connessione, ed il secondo invece viene utilizzato per lo scambio dei file che viene aperto e richiuso durante lo scambio dei dati. Avere due canali di comunicazione aperti contemporaneamente genera problemi di sicurezza e di trasmissione in quanto è possibile dare altre istruzioni mentre il trasferimento dati è in corso, con il rischio di perdita dei dati ed in alcuni casi la loro corruzione fino alla perdita totale. Per impedire questo problema è stato implementato **il supporto per le connessioni passive**. Queste connessioni vengono avviate dal client e non più dal server in modo da evitare anche i problemi legati a firewall, router o all'architettura della rete dell'utente finale.

A differenza però di quelle attive, le connessioni passive si portano in dote **notevoli problemi di sicurezza.** Una su tutte è quella dovuta al fatto che quando il server apre la connessione verso il client, non viene fatto più nessun controllo in quanto il software dà per scontato che dall'altra parte ci sia l'utente. Utilizzando invece l'altra connessione questa sicurezza non c'è più in quanto al posto del client ci potrebbe essere qualche software malevolo pronto a intercettare la comunicazione. Tra le altre debolezze c'è anche il fatto che la porta di connessione utilizzata in queste transizioni è casuale; per cui se si voleva utilizzare tale servizio è gioco forza aprire tutte le porte dei propri server per permettere il servizio stesso. **Una catena di punti deboli**. Buona norma è quella di non usare il protocollo FTP ma utilizzare l'**SFTP** che risulta integralmente cifrato e quindi sicuro.

Esistono poi soluzioni più o meno efficaci. Utilizzando ad esempio dei firewall in modalità Stateful Inspection è possibile risolvere molte delle problematiche legate alla sicurezza. Questi software, estremamente avanzati, leggono il contenuto di una sequenza di pacchetti e agiscono mettendo in campo azioni preordinate. Nel caso dell'FTP aprono la porta solo quando è necessario per eseguire la connessione passiva richiesta dal client e bloccano una connessione passiva qualora questa provenga da un IP diverso da quello della connessione principale.

Per l'utilizzo invece dei protocolli di comunicazione "**sicuri**", è necessario usare (lato server) i cosiddetti "certificati digitali firmati" riconosciuti da parte di Certification Autority. L'uso di certificati creati autonomamente oppure già scaduti è assolutamente sconsigliabile in quanto induce negli utenti la pratica pericolosa che è quella, purtroppo diffusa, di ignorare da parte dell'utente i messaggi d'allerta restituiti, ad esempio, dal browser.



La possibilità di usare SSL per la ricezione e l'invio della posta elettronica o per l'accesso a portali sicuri, dipende dalla configurazione del server utilizzato in quel momento (sempre consigliabile il suo utilizzo). Nel caso in cui si usi la posta elettronica o altre applicazioni WEB erogate da provider esterni, è possibile attivare entrambe le modalità di sicurezza. E' invece fortemente criticabile il fatto che venga impiegato in modo predefinito il protocollo http e non https. **Mai trasmettere informazioni in chiaro!!!!**

Per concludere ricordiamo che l'utilizzo di un protocollo di posta non sicuro consente ad un malintenzionato di:

- assumere l'identità di un'altra persona,
- di leggere le e-mail di un altro utente,
- di carpire i dati personali memorizzati sui server di posta,
- di inviare posta elettronica per conto dell'ignaro utente.

Solo un'idonea formazione può evidenziare questo pericolo, ma è un argomento sottovalutato in quanto assorbe tempo e risorse rendendo improduttive le persone durante tale periodo, ma……. è davvero tempo perso?

Lesson 3: Protezione apparati di rete

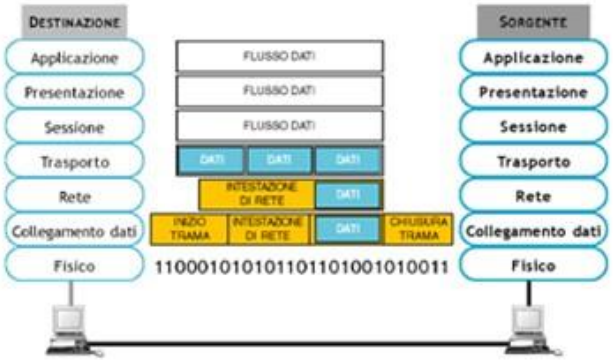
Gli Apparati di Rete

Con il termine apparati di rete attivi ci si riferisce comunemente ai dispositivi che gestiscono il traffico e la struttura del flusso dati nelle reti informatiche. Lo scopo principale di questa lezione è quello di verificare se gli apparati di rete sono stati installati e configurati in modo corretto tra di loro o verso il mondo esterno, risultando di fatto una struttura informatica sicura come spiegato nelle lezioni precedenti. Nell'ambito di un progetto di rete sono di fondamentale importanza le modalità con le quali la rete stesse viene concepita, realizzata e mantenuta efficiente. Nella costruzione della rete sono fondamentali le seguenti fasi:

- l'installazione,
- la configurazione,
- l'aggiornamento del firmware o del sistema operativo,
- l'amministrazione,
- un'accurata politica di sicurezza, ➢ il monitoraggio.

Quali sono gli apparati di rete

Gli apparati di rete più diffusi e normalmente impiegati all'interno delle reti vanno a posizionarsi all'interno della pila di protocolli ISO/OSI in funzione della funzionalità che svolgono nel processo di trasporto dei dati e precisamente:

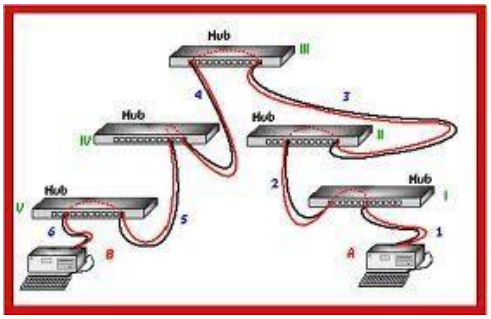


- Repeater
- Hub
- Bridge
- Switch
- Router

Repeater

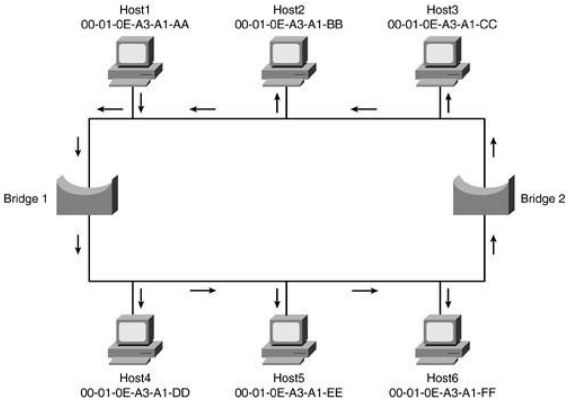
Sono dispositivi elettronici che rigenerano il segnale elettrico che si è attenuato per la perdita di potenza a causa della lunghezza del cavo. Dopo averlo rigenerato, lo ritrasmettono su di un nuovo segmento di rete. In questo modo garantiscono un livello di segnale ottimale su ognuno dei segmenti di rete che interconnettono. Possono essere connessi in modo seriale sino ad un massimo di 4 repeater. La distanza che possono coprire dipende dalla tipologia di cavo impiegato nella realizzazione della rete. Lavorano al livello più basso "fisico" della pila ISO/OSI, e non prevedono nessun meccanismo atto alla gestione dei dati, pertanto non delimitano né i domini di collisione né quelli di broadcast (ormai raramente utilizzati).

Hub



E' un ripetitore multi porta che mette in comunicazione più pc sulla stessa LAN. Anch'esso, come il repeater, non consente una connettività seriale oltre i 5 apparati. Realizza un nodo di rete all'interno del quale si concentrano gli host connessi alle sue porte (**rete a stella**). Nell'hub i dati entrano in una "**porta**" e vengono replicati e instradati verso tutte le altre, esclusione fatta per quella di provenienza. Viene usato come centrostella e consente di connettere le periferiche e di estendere le connessioni di rete. Questo apparato non contiene al proprio interno nessun meccanismo decisionale nei confronti dei dati. Per questo motivo tutti i dispositivi connessi all'hub ricevono, senza nessun filtro, tutto il traffico che attraversa l'apparato. Opera al livello più basso "fisico" della pila ISO/OSI. (Ormai raramente utilizzati).

Bridge



E' un apparato di rete più sofisticato dell'hub e viene utilizzato per connettere due segmenti di LAN diversi tra loro (per questo viene chiamato bridge "ponte"). Questi apparati esistono per supporto di tecnologie diverse (non solo ethernet). Realizza la connessione di 2 segmenti di rete, replicando e indirizzando intelligentemente i pacchetti dati secondo le indicazioni di una tabella di instradamento, implementata in maniera automatica ("autodescovery mode") al momento dell'accensione. Tale tabella viene poi aggiornata ogni qualvolta all'interno delle due reti connesse viene attivato un nuovo utente. Il Bridge può implementare logiche intelligenti in modo da intervenire sul passaggio dei dati da un segmento all'altro realizzando di fatto veri e propri blocchi di utenti da una LAN verso l'altra (Work Group locali). Nasce in origine dalla necessità di ridurre le lan in segmenti più piccoli, più facilmente gestibili e performanti. Implementa al suo interno protocolli intelligenti quali lo "Spanning Tree", che permette la connessione tra due reti in alta affidabilità (doppio path tra le stesse reti) evitando il loop del traffico. Il bridge opera a livello 2 "data link" della pila ISO/OSI. (Ormai raramente utilizzati).

Switch

Lo switch è un apparecchio di rete che mette in comunicazione diretta un host A con un altro host B senza che, come accade con un hub, tutti gli altri ascoltino. Viene definito anche come "bridge multi porta", in grado cioè di connettere più segmenti di rete realizzando di fatto una gestione più efficiente dei dati con conseguente incremento delle performance di rete (velocità e bandwidth o ampiezza di banda). Non realizza nessuna conversione diretta sui dati. Per la determinazione della destinazione dei dati utilizza delle "forwarding table". Al contrario dell'hub, può supportare funzionalità avanzate come le VLAN (Virtual LAN). Questi apparati a seconda del SW implementato sopra possono operare a vari livelli del modello ISO/OSI. Principalmente lavorano a livello 2, occupandosi appunto del Forwarding dei dati intervenendo al più sulle priorità dei pacchetti "802.3X". Gli Switch più evoluti invece implementano anche funzionalità di livello 3 e 4 normalmente appannaggio di altri apparati. Gli switch di Layer 2 utilizzano una tabella nella quale sono riportati i numeri che corrispondono alle porte dello switch accanto ai quali vengono associati i "mac address" degli apparati a loro connessi. Per gli switch di Layer 3 rimandiamo invece alla descrizione del Router (Comunemente utilizzati nella realizzazione delle reti dati).

Host MAC Address	Port
00 00 80 45 FE 21	5
00 00 80 45 DA 47	3
00 40 00 80 45 FE	2
00 40 80 10 AA 21	1
00 00 80 00 FF AB	5

Router

Sono utilizzati principalmente per estendere e interconnettere Reti locali geograficamente distanti tra loro. Sono di solito posizionati alla periferia della rete in quanto ne rappresentano di solito la porta d'ingresso o di uscita. Sono apparati più lenti rispetto ai Bridge e agli Switch. Infatti, dovendo prendere decisioni critiche su come instradare i pacchetti ricevuti verso le altre reti sulla base di tabelle di instradamento, hanno la necessità di leggere ed elaborare una quantità superiore di dati per cui il loro tempo di latenza è più alto. Realizzando la funzionalità di connessione tra reti diverse, i routers, al contrario dei bridge che connettono solo una rete ad un'altra, possono interconnettere centinaia di reti diverse decidendone anche i percorsi in funzione di parametri quali: il traffico, la qualità della connessione, la variata situazione della rete, un preciso piano di indirizzamento, etc, etc. Per questo motivo i router racchiudono al loro interno un po' tutte le funzionalità degli altri apparati di rete come concentratori, ripetitori, convertitori di dati, gestori di traffico. Un router può a seconda dell'esigenza disporre di interfacce sia di tipo LAN che WAN e può così estendere segmenti di reti locali, anche tecnologicamente diverse tra loro, su aree più estese (WAN). All'interno di una LAN, il router può anche essere usato per scopi di segmentazione in modo da proteggere per esempio l'area server dall'utenza oppure in un contesto WAN come dispositivo di interconnessione e interfacciamento tra tecnologie diverse. I routers utilizzano tabelle di routing sia costruite staticamente (vedi ad esempio dall'amministratore di rete) oppure dinamicamente tramite gli automatismi forniti da appositi protocolli "routing protocols". Il router lavora a livello 3 "rete" della pila ISO/OSI. Sostanzialmente analizza i pacchetti di livello 3 cioè di indirizzi IP. L'operazione di routing, a differenza dell'operazione di switching, decide in base alle informazioni di livello 3 "IP Address" quale strada far prendere a un pacchetto dati.

Non affrontiamo in questa fase le funzionalità di un firewall che saranno oggetto di una futura trattazione, ma lo consideriamo parte integrante della sicurezza perimetrale della nostra rete.

Topologia di rete

Le reti odierne sono costituite principalmente da switch di Layer 2/3/4. Solitamente quelli con funzionalità di routing sono posti al centro stella e connettono gli apparati di layer 2 ubicati in periferia. A fronte di tali connessioni, la topologia di rete migliore da realizzare risulta essere di tipo stellare. Esistono svariate tipologie di apparati alcuni dei quali sono "intelligenti" perché dotati di un SW di management. Questa peculiarità li rende i più indicati in quanto consentono di monitorare la rete e le sue performances.

Il protocollo standard utilizzato per realizzare i sistemi di Network Management è l' **SNMP** ed è utilizzato di fatto per la gestione dell'intera infrastruttura di rete.

SNMP

"Simple Network Managment Protocol" (SNMP) permette il monitoraggio (statistiche sullo stato dei sistemi) e il controllo (modifica delle impostazioni) di dispositivi di rete quali Server, Router, Switch, Hub ecc. Grazie a questo protocollo è possibile conoscere il throughput (carico dati sulle interfacce di rete) e le intere prestazioni di un sistema di trasmissione dati.

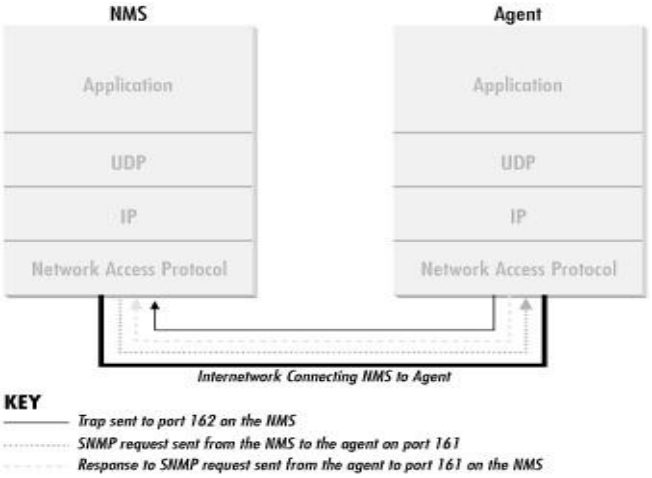
SNMP è passato attraverso alcune revisioni fino all'attuale versione 3:

- **SNMPv1**: descritto nelle **RFC 1155-1157** rappresenta la prima versione, utilizza l'invio dei nomi di community (utilizzati come password) in **chiaro**;
- **SNMPv2**: descritto nelle **RFC 1441-1452** è la seconda versione a cui sono state aggiunte nuove funzionalità tra cui la crittografia tramite **MD5**;
- **SNMPv3**: descritto nelle **RFC 2571-2575** è lo standard finale ed opera con protocolli sicuri cifrati ma è al momento raramente utilizzato.

Sostanzialmente un framework SNMP è composto da una o più Stazioni di Gestione (Management Station) e dagli agenti SNMP (SNMP Agent) installati sui devices di rete. Le Management Station interrogano gli agents i quali inviano le informazioni richieste. Solitamente gli agent SNMP di un apparato di rete sono implementati nel firmware dello stesso, mentre per quanto riguarda i server, vengono implementati tramite dei SW, operanti sui server come servizi. Le variabili gestite dagli agents, che rappresentano le caratteristiche e gli stati in cui si trovano gli oggetti monitorati, sono raccolti, in ogni singolo device, in un database chiamato MIB (Management Information Base) secondo la struttura definita nella SMI (Structure Management Information) che descrive l'oggetto stesso.

Gli apparati di rete possono essere anche settati in modalità tale da non doverli interrogare, ma da poter inviare in autonomia determinati messaggi di allarme alle Management Station al raggiungimento di una soglia precedentemente impostata. E' infatti possibile configurare gli agents impostando le così dette trap. Grazie all'impostazione delle trap è possibile ad esempio sapere quando un'interfaccia di rete smette di funzionare. Infatti al verificarsi del guasto precedentemente configurato, l'agent SNMP, che esegue il monitoraggio dell'apparato invia alla

Management Station un allert che identifica il problema specifico. SNMP utilizza come protocollo di trasmissione lo stack TCP/IP e nel particolare il "UDP" in modo da ottenere migliori performance e minore overhead della rete. Ricordiamo che UDP al contrario del TCP non effettua controlli e non iserisce bit ridondati all'interno del Frame, questo aumenta l'efficienza e la velocità di trasmissione. In particolare viene utilizzata la porta UDP 161 per le interrogazioni e le risposte, e la porta UDP 162 come destinazione dei messaggi trap SNMP generati dagli agents.



SNMP COMMUNITY

L'insieme degli apparati di rete gestiti da SNMP appartengono ad una **comunità** "community". La comunità rappresenta un **identificativo** che permette di garantire la sicurezza delle interrogazioni SNMP. Un agent SNMP risponde **solo** alle richieste di informazioni effettuate da una Management Station appartenente alla **stessa** comunità. I nomi di comunità sono formati da 32 caratteri e sono di tipo case sensitive.

Esistono tre tipi di comunità:

- **monitor**: permette di lavorare in sola lettura, quindi di effettuare solamente interrogazioni agli agents (il cui nome di comunità deve corrisponde a quello della management station che ne ha fatto la richiesta);
- **control:** permette tramite gli agents SNMP di effettuare delle operazioni in lettura/scrittura sul dispositivo, quindi di variarne le impostazioni sempre previo controllo di sicurezza;
- **trap:** permette ad un agent di inviare un messaggio trap SNMP alla management station secondo la propria configurazione.

La sicurezza

Purtroppo è uso abbastanza comune dare poca importanza agli apparati di rete. Una volta installati, vengono lasciati in funzione con i parametri di default. Se si vuole perseguire la sicurezza non è sufficiente impostare la password di accesso al device, occorre anche modificare la community di appartenenza.

I nomi di community di default predefiniti sono public per le comunità di sola lettura e write o private per quelle in lettura/scrittura. Se questi vengono lasciati così anche dopo l'installazione, è assurdo poi lamentarsi se qualche male intenzionato ha approfittato di questa leggerezza per carpire informazioni relative ai dati trasportati dai nostri apparati. E' bene modificare queste impostazioni di default con password e nomi scelti con cura.

Lo stesso firmware obsoleto, perché mai aggiornato, può rappresentare una minaccia. Occorre quindi costantemente verificare la documentazioni inerente i nuovi rilasci di release per appurare se contengono unicamente aspetti innovativi o risolvono invece problemi che possono mettere a rischio la stabilità della nostra rete.

Quanto detto, non è comunque sufficiente a garantirci la sicurezza. Se riprendiamo la metodologia di attacco descritta nel primo capitolo "Man in the Middle", ci rendiamo conto che, se applicata nei confronti degli apparati di rete, ci consente di acquisire informazioni fondamentali. Come per le altre applicazioni aziendali, anche in questi casi i protocolli maggiormente utilizzati per accedere ai sistemi di rete sono da suddividere in sicuri e non sicuri.

Protocolli insicuri:

- http,
- Telnet,
- SNMP ver.1 e 2

Protocolli sicuri:

- HTTP abbinato ad SSL,
- SSH (non basato su SSL ma concettualmente similare), ➢ SNMP ver.3

Mettere in sicurezza gli apparati di rete

Sicurezza fisica:

E' consigliabile installare gli apparati in un locale controllato e possibilmente chiuso a chiave, al riparo da scariche elettrostatiche o altre interferenze radio o elettromagnetiche. Il locale dovrebbe essere attrezzato con sistemi antincendio, controllo della temperatura e umidità e alimentazione ridondata con gli apparati, in caso di centro stella, connessi a due distinti UPS.

Sicurezza degli accessi:

Anche gli apparati di rete così come gli applicativi, i Data Base e i dati in genere, sono oggetto di controllo da parte della normativa sulla sicurezza che chiede agli amministratori di rete delle aziende di effettuare un rigoroso controllo degli accessi effettuati ai sistemi. Occorre quindi definire e controllare chi può accedere agli apparati, a quale livello di funzionalità e quale sia la funzione degli utenti che vi accedono. E' necessario disabilitare le interfacce, i protocolli e i servizi non usati.

In particolare, occorre prevedere:

- **di restringere** le modalità d'accesso (su quali porte, da quali utenti o IP, con quali protocolli);

- **di registrare** (log) chi ha avuto accesso, quando l'ha avuto e che cosa ha fatto;
- **di autenticare** chi accede (singoli, gruppi, servizi offerti);
- **di limitare** il numero di tentativi di login e imporre una pausa tra tentativi successivi;
- **di autorizzare** le azioni (singole funzioni o "views") che ogni utente può svolgere;
- **di visualizzare** una nota legale (scritta con un consulente) che appaia prima delle sessioni interattive;
- **di proteggere** i dati archiviati localmente, o in transito sulle linee dati, da copia e alterazione.

L'accesso agli apparati per scopi amministrativi può avvenire in locale, con cavo console (preferibile), e, se da remoto, attraverso l'impiego di protocolli preferibilmente quelli che cifrano il traffico. Per esemplificare in caso di connessione remota è meglio usare **SSH** Secure SHell invece di un comando **Telnet** sulla **CLI** (comand line interface). E ancora: è preferibile il protocollo **HTTPS** invece di **HTTP** sulla **GUI**(guide user interface). E infine, in caso di Network management, è preferibile **SNMP v3** invece di **SNMP v1-2**. Un'altra accortezza da applicare è quella di definire l'Host o la rete da cui si accetta l'accesso remoto, le interfacce su cui esso è accettato e i protocolli ammissibili prima di attivare la connessione remota.

VLAN (Virtual LAN)

Prima di effettuare operazioni di monitoring è sempre bene realizzare una **Vlan di Layer 3** appositamente dedicata al management, che consente una maggior sicurezza alle informazioni in arrivo dagli apparati di rete.
Le VLAN sono reti logiche e vengono implementate quando è necessario suddividere il traffico o le reti. Per questo motivo, se ne dedichiamo una al management, realizzeremo di fatto una divisione tra i dati in transito sulla rete, gli allerts, i comandi in arrivo e quelli verso gli apparati di rete (maggior sicurezza).

Benefici e Vantaggi

L'implementazione delle VLAN porta scalabilità, un miglioramento delle performance di rete e di conseguenza una migliore disponibilità del servizio (availability).

Ecco i vantaggi :

- **Migliore utilizzo della banda:** le VLAN risolvono il problema della scalabilità in reti grandi e molto complesse, suddividendo la rete in domini di broadcast minori;
- **Sicurezza:** le VLAN implementano un livello minimo di sicurezza permettendo la separazione di frame particolarmente sensibili, inserendoli in VLAN differenti;
- **Isolamento degli errori in un dominio di broadcast:** forse la ragione più importante per implementare le VLAN. Infatti il suo impiego riduce notevolmente l'impatto dei malfunzionamenti sulla rete, limitando le problematiche di un unico dominio di broadcast.

Conclusioni

La corretta configurazione degli apparati di rete e l'implementazione di una VLAN di management, rappresentano le due operazioni principali da effettuare per perseguire la sicurezza direttamente correlata agli apparati di rete. L'impiego delle VLAN, dividendo i domini di broadcast e le tipologie di traffico, oltre ad aumentare l'efficienza del monitoring è in grado di evitare pratiche di hacking purtroppo molto diffuse a livello 2 della rete.

Tutte le reti sono realizzate tramite l'impiego degli apparati sopra descritti per cui è inevitabile che, **se si vogliono proteggere i dati, bisogna prima di tutto proteggere gli apparati.**

Se i dati rappresentano il denaro e gli apparati la cassaforte è bene che la combinazione di quest'ultima non sia nè conosciuta nè di facile reperibilità, ma soprattutto…… è inutile nascondere la combinazione nella cassaforte se quest'ultima può essere…… **facilmente rubata !!!!!**

Lesson 4: Protezione reti wireless

La rete wireless

L'introduzione di tecnologie wireless all'interno delle reti LAN rappresenta ormai da qualche anno una consuetudine tale che risulta difficile trovare una rete dati priva di un'estensione senza fili. Questa tecnologia, nonostante i tanti detrattori, è in costante crescita. Le "reti senza fili" infatti rappresentano un sistema economico e flessibile adatto ad ogni realtà comprese le piccole e medie imprese. Per realizzare una rete wireless non sono necessari lavori di muratura o di posa dei cavi per il fissaggio delle infrastrutture. Gli apparati che le costituiscono sono di facile reperibilità e di basso costo se confrontati con gli apparati che compongono una rete Wired. Una rete wireless infine si adatta alla crescita e al dinamismo di qualsiasi azienda. In pratica la realizzazione di una tale struttura all'interno della propria azienda consente di mettere in campo le sole risorse per la realizzazione del servizio di trasmissione dati necessario in quel momento.

Come per gli apparati di rete LAN risultano di fondamentale importanza alcune operazioni di seguito riportate:

- Installazione,
- Configurazione,
- Aggiornamento del firmware o del sistema operativo,
- Amministrazione, ➢ Monitoraggio, ➢ Sicurezza.

Quali sono i sistemi che compongono una rete Wireless

La crescente proliferazione di dispositivi portatili con connettività wireless e i recenti sviluppi delle stesse tecnologie, hanno aperto un nuovo scenario agli utenti che oltre a fruire dei tradizionali servizi Internet, quali il web o e-mail, hanno la possibilità di beneficiare anche di servizi collaborativi avanzati. I nuovi servizi consentono agli utenti di comunicare all'interno delle proprie organizzazioni ovunque si trovino, in qualunque momento e condizione (fermi o in movimento).
Per realizzare una rete wireless così strutturata si utilizza una grande tipologia di apparati di cui i più conosciuti sono:

- router wireless,
- modem wireless,
- access point,
- network card,
- chiavette USB, ➢ adattatori wireless.

Gli standard

Le wireless LAN sono state standardizzate nel giugno 1997 dal Comitato IEEE.
Lo standard include requisiti dettagliati per la trasmissione fisica dei pacchetti di dati attraverso le onde radio. Nel 1999, IEEE pubblica le due versioni dello standard **802.11**: **802.11a e 802.11b**. Nel 2003 viene ratificato lo standard **802.11g** e nel 2009 viene rilasciata la versione dello standard **802.11n.**

NB: Per la propagazione via radio dei segnali, **sono state liberalizzate** le frequenze intorno ai 2.4 Ghz e non occorre quindi richiedere licenze specifiche per l'installazione di punti di accesso Wi-Fi (anche quelli domestici).

La famiglia 802.11 consta di tre protocolli dedicati alla trasmissione delle informazioni (a, b, g), la sicurezza è stata inclusa in uno standard a parte, **802.11i**. Gli altri standard della famiglia (c, d, e, f, h, …) riguardano estensioni dei servizi base e miglioramenti di servizi già disponibili. Il primo protocollo largamente diffuso è stato il b; in seguito si sono diffusi il protocollo a e soprattutto il protocollo g.

I protocolli **802.11b e 802.11g** utilizzano lo spettro di frequenze (banda ISM) intorno ai 2,4 GHz. Si tratta di una banda di frequenze regolarmente assegnata dal piano di ripartizione nazionale (e internazionale) ad altro servizio, e lasciato di libero impiego solo per le applicazioni che prevedono potenze EIRP (Massima Potenza Equivalente Irradiata da antenna Isotropica) di non più di 20 dBm da utilizzare all'interno di una proprietà privata (è vietato l'attraversamento del suolo pubblico). Trovandosi però ad operare in bande di frequenze ove già lavorano altri apparecchi, i dispositivi b e g possono essere influenzati negativamente durante la loro trasmissione. Possono infatti risentire, anche in modo pesante, della vicinanza con telefoni cordless, ripetitori audio/video per distribuire programmi televisivi satellitari o altri apparecchi all'interno di un appartamento o ufficio che utilizzano quella banda di frequenze.

Il protocollo **802.11a** utilizza la banda ISM dei 5,4 GHz. Tuttavia non risponde alla normativa europea ETSI EN 301 893[1] che prevede DFS (Dynamic Frequency Selection), TPC (Transmit Power Control) e radar meteorologici; tale normativa di armonizzazione europea è valida in Italia su indicazione del Ministero delle Comunicazioni con il decreto ministeriale del 10 gennaio 2005. Per ovviare al problema in Europa è stato introdotto nel 2004 il protocollo **802.11h**, che risponde ai requisiti richiesti. Un apparato WIFI per trasmettere su suolo pubblico in Italia a 5.4 GHz deve obbligatoriamente utilizzare questo standard.

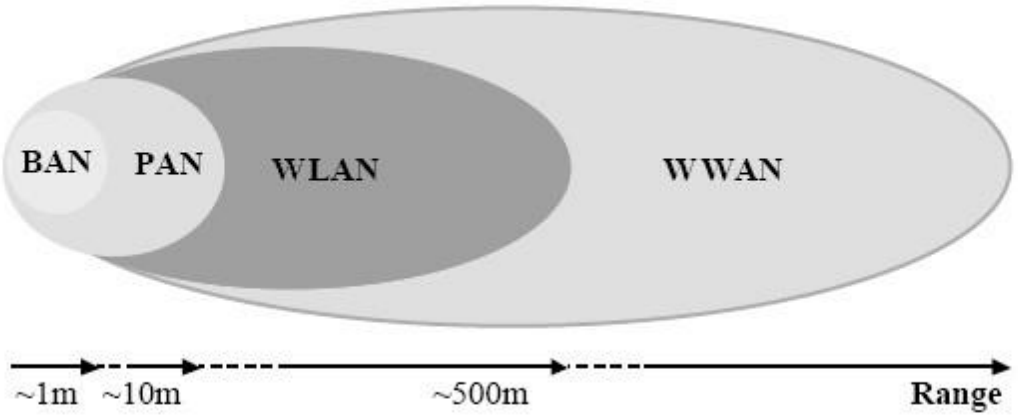
Implementazione dei protocolli WIFI

Il susseguirsi delle continue evoluzioni dei protocolli WIFI, frutto delle continue richieste del mercato, ha creato un po' di confusione, per cui, con la tabella riportata nella pagina seguente proviamo a fare chiarezza riassumendo brevemente le caratteristiche principali che identificano i vari standard.

Standard	Frequenza	Velocità di trasferimento (Mbit/s)
802.11 legacy	FHSS, 2,4 GHz, IR	1, 2
802.11a	5,2, 5,4, 5,8 GHz	6, 9, 12, 18, 24, 36, 48, 54
802.11b	2,4 GHz	1, 2, 5.5, 11
802.11g	2,4 GHz	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
802.11n	2,4 GHz, 5,4 GHz	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, 125

Topologia di rete wireless

Possiamo indicativamente classificare le reti wireless in base all'area coperta dal segnale trasmesso dai dispositivi, in diverse categorie: **BAN, PAN, WLAN e WWAN**.



Body Area Network

Le BAN sono reti il cui raggio di trasmissione copre all'incirca le dimensioni di un corpo umano, tipicamente 1-2 metri, e consentono di connettere dispositivi indossabili quali auricolari, palmari, lettori MP3, telefoni cellulari etc.
Tra le caratteristiche principali delle reti WIFI BAN troviamo la capacità di connettere dispositivi eterogenei accompagnata a quella di auto-configurarsi, rendendo di fatto trasparenti all'utente operazioni come la rimozione o l'aggiunta di un nuovo dispositivo.
La connessione wireless è considerata la soluzione naturale per una BAN in quanto l'utilizzo di fili risulterebbe estremamente scomodo.

Personal Area Network

Il raggio di comunicazione delle PAN è tipicamente superiore ai 10 metri. Le PAN consentono a dispositivi vicini di condividere dinamicamente le informazioni. E' possibile perciò connettere dispositivi portatili con altri oppure con stazioni fisse, ad esempio per accedere ad Internet. Tecnologie ad infrarossi e radio rendono nelle PAN notevolmente più pratiche le operazioni quotidiane di sincronizzazione fra portatile, desktop e palmare, ma anche il download delle immagini dalla macchina fotografica digitale, l'upload di musiche nel riproduttore di MP3, ecc. Tra gli standard più usati per realizzare le BAN e le PAN ricordiamo il protocollo IrDA e il protocollo Bluetooth.

Wireless Local Area Network

Le WLAN hanno un raggio di comunicazione di 100, 500 metri tipico dell'area mediamente occupata da un singolo palazzo. Nelle WLAN troviamo gli stessi requisiti delle tradizionali wired LAN, come la connessione fra le stazioni che ne fanno parte e la capacità di inviare messaggi broadcast. Le WLAN si trovano però a dover affrontare alcuni problemi specifici di questo ambiente, come la sicurezza dovuta al mezzo trasmissivo (trasmissioni via etere), il consumo energetico, la mobilità dei nodi e la limitata larghezza di banda.
Esistono due differenti approcci all'implementazione di una wireless LAN, uno basato sull'infrastruttura e uno su reti strutturate ad hoc.

L'architettura basata su un'infrastruttura prevede l'esistenza di un controller centralizzato chiamato "Access Point" solitamente connesso con la rete fissa, che realizza l'accesso tra i sistemi aziendali e i dispositivi mobili.

Una rete ad hoc è invece una rete "peer-to-peer" formata da nodi mobili posti all'interno dei reciproci raggi di trasmissione. Detti nodi si configurano sino a formare una rete temporanea gestita da un controller dinamicamente eletto tra tutti i nodi partecipanti alla comunicazione.

Wireless Wide Area Network

Le **WWAN** (Wireless Wide Area Network) sono le reti wireless che dispongono del range più ampio oggi disponibile, e vengono, nella maggior parte dei casi, installate nell'infrastruttura della fonia cellulare. Le **WWAN** offrono anche la possibilità di trasmettere dati.

Le **WWAN** sono estese su vaste aree geografiche e hanno un raggio di trasmissione dell'ordine dei km, tipicamente compreso tra 1,5 e 8 Km. Sono state concepite per rispondere all'esigenza di collegare utenti che si trovano a grandi distanze tra loro. Sfruttando questa loro caratteristica, tale tipologia di rete viene usata anche per collegare diverse LAN situate in località distanti tra loro.
Le soluzioni **WWAN**, che si basano su un'infrastruttura a rete cellulare, o su trasmissione satellitare, rappresentano il futuro della comunicazione dei dati.
Le "Wireless Wide Area Network" forniscono accesso alle informazioni anytime & anywhere in presenza di copertura di rete cellulare.

Le reti wireless di tipo **WLan,** molto diffuse ormai nelle aziende, rappresenteranno l'oggetto della presente lezione.

Quando si utilizza una rete wireless è di fondamentale importanza sapere che:

- gli apparati wireless vengono venduti con tutte le misure di sicurezza disattivate, per cui chiunque si può collegare e fare danni: **è necessario l'intervento dell'utente per attivare le protezioni**;
- la sicurezza delle reti wireless è molto più debole di quanto nella realtà viene dichiarato dai produttori;
- le prestazioni reali sono di gran lunga inferiori a quelle pubblicizzate.

Partendo da queste considerazioni e dalla conoscenza dei limiti imposti dalla tecnologia, è possibile realizzare reti dati correttamente funzionanti. Vediamo allora come mettere a Vostra disposizione la nostra esperienza maturata in anni di analisi e di realizzazioni di reti Wireless.

Implementazione rete wireless

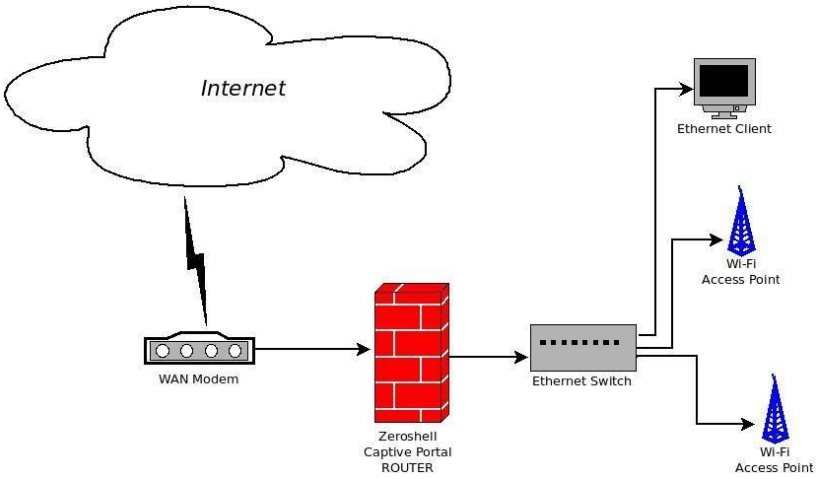
In funzione dell'estensione dell'area da coprire possono essere utilizzate due diverse architetture wireless:

- stand-alone;
- con controller.

Quando scegliere una modalità invece di un'altra? Se la necessità è quella di offrire un accesso in un'area aziendale ben definita o comunque connettere un numero limitato di access point, la soluzione **stand-alone** è quella più indicata. Nel caso invece di implementazioni più complesse, con un numero elevato di aree aziendali da coprire e di access point, l'adozione di una rete **con controller** è mandatory.
Vediamo le principali differenze tra i due sistemi:

Autenticazione

Entrambi i sistemi supportano autenticazione mediante **MAC** o server radius **802.1x**, in alcuni casi le controller hanno già implementati sistemi di autenticazione o di "captive portal" oggi sostituiti dalla modalità "Hot Spot Router" per utenti guest.



Encryption

Gli **access point stand-alone** criptano la comunicazione che intercorre tra loro e i device, archiviano le chiavi di criptografia in un proprio data base interno evitando la loro trasmissione in rete e quindi la loro lettura da parte di terze parti non autorizzate. Le reti **con controller** consentono invece la criptazione dell'intera architettura che intercorre tra access point, device e controller, partendo da un unico punto centralizzato con minore possibilità di errore.

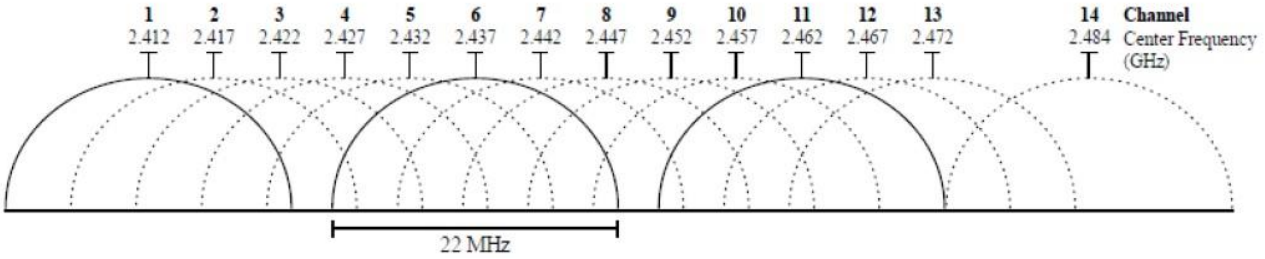
SSID/VLAN

Nel caso degli **access point stand-alone** la configurazione dei SSID e di eventuali VLAN avviene su ciascun dispositivo e in dipendenza della configurazione ereditata dalla rete locale cablata. Nella rete **con controller** invece si può avere funzionalità di Layer 3 e implementare quindi servizi indipendenti dalla rete a cui la rete wireless è connessa.

Radio Management/ Channel Management

La modalità **con controller** consente la gestione dei canali radio in modo da evitare le interferenze dovute a trasmissioni adiacenti alla rete su frequenze identiche (sovrapposizione di canali).

Il funzionamento di un sistema wireless infatti permette di utilizzare 13 canali (regolamentazione per lo stato italiano), di cui però solo 3 alla volta per non interferire tra di loro. Infatti, come si può notare dallo schema successivo, molti canali vanno in sovrapposizione di altri generando disturbi che abbassano le performance dell'infrastruttura e, in alcuni casi, bloccandone il corretto funzionamento.



Ogni canale ha un ampiezza di 22MHz, per cui vista l'ampiezza totale di banda dedicata ai sistemi WIFI, ogni canale va a sovrapporsi a quelli contigui. Ne risulta che, i canali realmente utilizzabili sono sempre a gruppi di 3 (1,6,11 o 2,7,12 o 3,8,13). Siccome ci sono dispositivi che non supportano i canali 12 e 13, per ovviare a qualsiasi problema, è stato deciso che i canali veramente utilizzabili sono solamente 3 (1,6,11).

Alla luce di quanto detto sopra, per evitare segnali interferenti, generati dagli access point impiegati per la copertura, sarà necessario riconfigurare su tutti i moduli radio il canale da utilizzare e fissarlo, in modo da evitare ogni interferenza con i segnali generati dagli access point adiacenti. Nello schema a lato è rappresentata la miglior configurazione delle frequenze dei canali su cui è bene fissare gli access point.

La configurazione suggerita consente infatti di non avere canali interferenti sovrapposti, garantendo il miglior SNR **Signal-to-noise ratio** e aumentando nel contempo le performance della rete WIFI.

Group configuration

Una rete wireless con controller, mediante gestione centralizzata, consente di realizzare configurazioni di gruppo agevolando di fatto le operazioni di manutenzione quali la distribuzione delle configurazioni o gli aggiornamenti del firmware.

Bandwidth/ Load balancing

Una rete wireless con controller consente di limitare la larghezza di banda massima che gli utenti possono utilizzare oltre a bilanciare il traffico in zone ad alta densità di connessione facendo transitare i dati tra più access point.

Redundancy

Il sistema basato su controller rappresenta un single "point of failure" che in caso di fault bloccherebbe tutti gli access point ad esso connesso. Per questo motivo è consigliato adottare una doppia controller in modo da garantire la continuità del servizio.

Network Access Control

Sempre tramite le controller è consentita l'implementazione di policy d'utente o di gruppo per l'accesso alla rete o alle singole applicazioni.

Security

Alcuni access point integrano sistemi di IDS (intrusion detection system) che sono limitati alla propria funzionalità in rete, mentre una controller implementa criteri di sicurezza su tutta l'architettura wireless. Può essere dedicato un canale radio per il rilevamento delle intrusioni wireless e monitorata la rete wireless per il controllo di minacce, attacchi di spoofing, attacchi Denial of Service, di reti ad-hoc, ecc.

Quality of Service

Sia i sistemi stand-alone che quelli basati su controller sono in grado di assegnare delle priorità al traffico, in base alle applicazioni e ai protocolli, ma solo la controller è in grado di garantire il roaming tra i vari access point per poter offrire servizi multimediali efficienti quali voce, video etc.

Mesh Networking

Entrambe le tecnologie consentono la creazione di topologie magliate, sia tramite l'utilizzo del cavo che dell'etere. In questo ultimo caso però si riduce la disponibilità della banda che risente in modo diretto del numero di hop che il pacchetto dati deve passare. La controller, al contrario della stand-alone, è in grado di modificare in automatico la magliatura, in base a precise esigenze definite da parametri quali la priorità, il protocollo, il tipo di traffico, la congestione di rete, ecc.

Live monitoring of Wireless network and location based services

La controller consente un monitoraggio in tempo reale della rete wireless e di eventuali servizi basati sulla localizzazione. E' possibile integrare le planimetrie dei locali con l'architettura wireless implementata per individuare i singoli device e l'area entro la quale stanno operando con lo scarto di qualche metro.

SNMP Comunity

Come evidenziato nella precedente lezione, anche per i device wireless è fondamentale la configurazione corretta dell'SNMP. L'insieme degli apparati di rete gestiti da SNMP appartiene a una **comunità** (*community*). La comunità rappresenta un **identificativo** che permette di garantire la sicurezza delle interrogazioni SNMP. Un agent SNMP risponde **solo** alle richieste di informazioni effettuate da una Management Station appartenente alla **stessa** comunità. I nomi di comunità sono formati da 32 caratteri e sono di tipo "case sensitive".

Esistono tre tipi di comunità:

- **monitor**: permette di lavorare in sola lettura, quindi di effettuare solamente interrogazioni agli agent (il nome di comunità deve corrisponde a quello della management station che ne ha fatto la richiesta);

- **control**: permette tramite gli agent SNMP di effettuare delle operazioni in lettura/scrittura sul dispositivo, quindi di variarne le impostazioni sempre previo controllo di sicurezza;
- **trap**: permette a un agent di inviare un messaggio trap SNMP alla management station secondo la propria configurazione.

La sicurezza

Come premesso all'inizio, una volta installati i device wireless, spesso vengono lasciati in funzione con i parametri di default. Pessima abitudine.

Non è sufficiente impostare una password di accesso al device, occorre anche modificare la community di appartenenza. Ottimo suggerimento.

Spesso i nomi di community di default predefiniti sono "public" per le comunità di sola lettura e "write" o "private" per quelle in lettura/scrittura. Ovviamente è bene modificare queste impostazioni di default per motivi di sicurezza. Assolutamente da fare.

E' necessario schermare le onde radio che attraversano aree di non pertinenza propria mediante l'utilizzo di apposite antenne direzionali o con accorgimenti quali carta stagnola o simili.

Il firmware obsoleto può rappresentare una minaccia, occorre costantemente verificare le documentazioni inerenti i nuovi rilasci di release, controllare se contengono unicamente aspetti innovativi o risolvono problemi che possono mettere a rischio la stabilità della nostra rete. Spesso per i più esperti.

NB: quanto sopra non è comunque sufficiente a garantirci la sicurezza.

Se riprendiamo la metodologia di attacco descritta nel primo capitolo "Man in the Middle", ci rendiamo conto che, se applicata agli apparati di rete wireless, consente di acquisire fondamentali informazioni, esattamente come per gli apparati di rete wired.

Come per le altre applicazioni aziendali, anche in questi casi i protocolli maggiormente utilizzati per accedere ai sistemi di rete sono da suddividere in sicuri e non sicuri.

Protocolli insicuri:

- http,
- Telnet,
- SNMP ver.1 e 2, ➢ WEP.

Protocolli sicuri:

- HTTP abbinato ad SSL,
- SSH (non basato su SSL ma concettualmente similare), ➢ SNMP ver.3, ➢ WPA e WPA2.

Mettere in sicurezza gli apparati di rete

Sicurezza degli accessi:

Anche gli apparati di rete wireless sono soggetti al controllo accesso da parte degli amministratori di sistema che la normativa richiede alle aziende. A questo proposito occorre definire e controllare:

- chi può accedere agli apparati;
- a quale livello e funzioni;
- disabilitare le interfacce non usate;
- disabilitare i protocolli;
- disabilitare i servizi non necessari.

In particolare, occorre prevedere:

- di restringere le modalità di accesso (da quali utenti o IP, con quali protocolli);
- di registrare (log) chi ha avuto accesso, quando l'ha avuto e che cosa ha fatto;
- di autenticare l'utente che accede (singoli, gruppi, servizi offerti);
- di limitare il numero di tentativi di login imponendo una pausa tra i tentativi successivi;
- di autorizzare le azioni (singole funzioni o "views") che ogni utente può svolgere;
- di proteggere i dati archiviati localmente o in transito sulle linee dati da copia e alterazione.

L'accesso amministrativo può avvenire in locale, tramite cavo console (preferibile) o da remoto con vari protocolli tra i quali è bene preferire quelli che cifrano il traffico a quelli in chiaro, come indicato nei punti precedenti.

Ad es. è meglio usare:

- SSH Secure SHell invece di Telnet sulla CLI; ➢ HTTPS invece di http sulla GUI; ➢ SNMP v3 invece di SNMP v1-2.

Inoltre è consigliabile anche:

- definire l'Host o la rete da cui si accetta l'accesso remoto; ➢ definire le interfacce su cui esso è accettato; ➢ definire i protocolli ammissibili.

Occorre poi impostare protocolli di criptazione dei dati sicuri, appositamente studiati per reti wireless. Poiché i segnali radio vengono inviati via etere, è possibile che vengano rilevati anche da dispositivi o utenti non autorizzati ad accedere alla rete WIFI, compromettendo quindi la sicurezza della rete e delle informazioni veicolate al suo interno. Per tale motivo, all'interno degli standard di trasmissione wireless, sono stati implementati protocolli e misure rivolte all'aumento della sicurezza delle reti.

Chiave di Autenticazione Pubblica (WEP)

Questo tipo di autenticazione (Wired Equivalent Privacy) presente nello standard IEEE 802.11, è stato progettato per fornire una sicurezza comparabile a quella delle reti LAN via cavo, e richiede che l'access point invii ad ogni stazione una chiave pubblica (a 64 o 128 bit) che viene trasmessa su un canale indipendente.

Chiave di crittografia WPA

Il **WPA** (WIFI Protected Access) è progettato, a differenza del **WEP**, per utilizzare l'autenticazione delle postazioni e la distribuzione di differenti chiavi per ogni utente. Tale operazione è effettuabile attraverso una Pre-Shared Key (PSK), che presenta una sola password d'accesso per qualsiasi utente ne richieda l'accesso. Una delle modifiche che introducono maggiore robustezza rispetto alla chiave WEP è l'utilizzo del metodo di criptaggio dei dati basato sul **TKIP** (Temporal Key Integrity Protocol) che, cambiando periodicamente la chiave (ora fino a 256 bit) in uso tra gli apparati Wi-Fi in modo dinamico e criptato, consente di ottenere una maggiore efficacia contro i tentativi di accesso non autorizzato alla rete wireless.

Controllo Access-List ristretta

Sull'access point è possibile abilitare soltanto alcune determinate postazioni utente mediante uno specifico elenco dei **Mac-Address** relativi alle schede di rete wireless. In tal modo, soltanto le schede WIFI, con i Mac-Address specificati nella lista, saranno abilitati ad accedere alla rete wireless.

Nome della rete WIFI (SSID) nascosto

Sull'apparato che trasmette il segnale wireless (access point), è possibile configurare il nome della rete wireless in modalità nascosta. Tale modalità, consente di evitare che i dispositivi rilevino in modo automatico la rete wireless. Gli utenti autorizzati potranno connettersi alla rete solo specificando, con la configurazione in modo manuale, il nome dell'access point (SSID).
VLAN (Virtual LAN)

La creazione di una Vlan di Layer 3 di management consente di mettere in sicurezza gli apparati di rete wireless. Le VLAN sono reti logiche e vengono implementate quando è necessario suddividere il traffico o le reti (vedi lezione precedente sugli apparati di rete).

Applicazione utile

Oltre alle debolezze riscontrate nelle configurazioni dei sistemi di rete wireless, abbiamo sovente riscontrato un problema legato alla gestione dei nostri device nei confronti delle connessioni di rete disponibili. Durante gli audit in aziende, dove è stata implementata una rete wireless per consentire mobilità in ufficio, abbiamo riscontrato lentezze di trasmissione molto significative nonostante gli utenti fossero connessi alla rete cablata. Facendo dei test di velocità di trasmissione, non si riusciva ad andare oltre il 20% delle potenzialità della rete dati e questo

perché l'utente, che si era sconnesso dalla LAN per recarsi in sala riunioni, agganciava la rete wireless per questioni di mobilità. Una volta però tornato alla propria postazione e riconnesso alla LAN, restava di fatto ancora connesso alla rete wireless senza accorgersene.

Tutto ciò accade perché il client non è in grado di discriminare o di assegnare delle priorità alle network cards. Essendo molti gli utenti mobili, o meglio diventandolo con questa modalità operativa, si viene ad accumulare un numero decisamente elevato di utenti connessi in WIFI con conseguente degrado delle performance di rete.

Chi ha scaricato questa lezione può anche scaricare un tool trial che una volta installato sul proprio client consente di disabilitare in modalità automatica la rete wireless una volta connessi alla rete LAN.

Conclusioni

Il wireless, oltre che di fondamentale importanza per i servizi aziendali, sta diventando una delle più grandi rivoluzioni del mondo dell'elettronica. Oltre agli impieghi visti durante la lezione, la rete wireless può collegare un computer ad internet e ad apparecchi come:

- stampanti;
- telefoni;
- tablet;
- videocamere e telecamere;
- console videogiochi;
- Hard Disk portatili;
- DVD player;
- impianti hi-fi;
- TV di nuova generazione; ➢ sistemi per l'automobile; ➢ domotica.

Questo vuol dire che è possibile ascoltare in ogni stanza della casa i file MP3 contenuti nel computer fisso e, per chi parcheggia nei pressi della propria casa, scaricare direttamente nello stereo i file audio che intende ascoltare durante il viaggio.

I segnali video, come quelli provenienti da un ricevitore satellitare, possono essere visti su qualsiasi tv di casa, così come le stazioni radio, che trasmettono su Internet, possono essere ascoltate su qualsiasi impianto hi-fi. Allo stesso modo, la centralina del riscaldamento e tutti gli elettrodomestici di casa possono essere telecontrollati da una apparecchiatura adatta allo scopo.

Insomma, l'unico limite all'applicazione della tecnologia WIFI sembra davvero essere la fantasia, motivo in più per applicare idonee politiche di sicurezza per evitare spiacevoli inconvenienti e una volta tanto…….. **fate attenzione**:

non sempre una rete wireless aperta è solo un'opportunità per navigare gratis, potrebbe rivelarsi invece un mezzo per acquisire le vostre informazioni.

Lesson 5: Open Port – Protocolli layer 2 – Condivisione Rete

Security Audit: l'analisi di rete

L'esponenziale crescita dell'ICT (Information Communication Technologies) e il pervasivo aumento di reti per l'interconnessione dei sistemi informativi, impongono un'ostinata attenzione agli aspetti legati alla sicurezza informatica.

Non crea certo meraviglia il numero di personal computer compromessi, che ha subito in questi ultimi anni un aumento esponenziale, così come le reti di prestigiose organizzazioni violate oppure addirittura fermate perché oggettivamente non più sicure. Indietro ormai non si torna. I computer rappresentano la nostra modalità di trasmissione dei dati. A loro abbiamo affidato il nostro business e ancora peggio il nostro **KNOW HOW**. Come fare allora per proteggersi?

Scopo della lezione è proprio quello di analizzare in prima persona le vulnerabilità a cui i nostri computer sono esposti, provare a identificarle e insieme cercare qualche strumento per difenderci magari in modo preventivo. L'argomento principale sarà quindi il **vulnerability scanning**.

E' meglio chiarire subito che per "vulnerability scanning" intendiamo esclusivamente "l'analisi lecita" della nostra rete o comunemente definito **forensic analysis**.

Non è nostra intenzione offrire i mezzi e le conoscenze per sferrare attacchi informatici illeciti. A tal proposito ricordiamo che:

"l'accesso abusivo a sistemi informatici è un reato punito dal codice penale".

Gli strumenti messi a disposizione dalla comunità del software libero per analizzare e quindi **contrastare** le possibili vulnerabilità di un sistema sono molteplici.

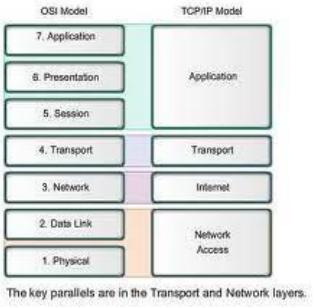
L'esposizione dei nostri sistemi ai rischi di attacchi **è una nostra responsabilità**, ignorare il problema non ci solleva dalle conseguenze che ne derivano. Le normative vigenti richiedono tra l'altro di tutelare l'utilizzatore dei sistemi e di garantirne la privacy. Molto spesso si tende a sottovalutare la cosa ma è fondamentale ricordarsi che quanto evidenziato…….

"spetta per legge al proprietario/gestore del sistema informativo".

Prima di procedere con l'argomento della lezione è bene chiarire che la quasi totalità delle reti dati utilizza come linguaggio lo **Stack TCP/IP**, per cui comprendere a pieno le sue modalità funzionali significa anche capire le possibili criticità. E' fondamentale conoscere la lingua per capirne i contenuti. Nel particolare ci soffermeremo sui due principali protocolli, il **TCP** e l'**UDP**.

Descrizione

Il **TCP** (Trasmission Control Protocol) può essere parificato al livello di trasporto (OSI level 4) del modello di riferimento OSI, e di solito è usato in combinazione con il protocollo di livello di rete (OSI level 3) **IP** (Internet Protocol). La corrispondenza con il modello OSI non è perfetta, in quanto il **TCP** e l'**IP** nascono prima del suddetto modello. La combinazione dei due livelli è comunemente indicata come TCP/IP.



Spesso è erroneamente considerato un unico protocollo. Da qui, la difficoltà di una classificazione univoca per un protocollo che comprende, a pieno titolo, due livelli completi dello Stack OSI.

Confronto con UDP

Le principali differenze tra **TCP** e **UDP** (*User Datagram Protocol*), quest'ultimo principale protocollo di trasporto della suite di protocolli Internet, sono:

- il TCP è un protocollo orientato alla connessione, pertanto per stabilire, mantenere e chiudere una connessione, è necessario inviare pacchetti di servizio i quali aumentano "l'overhead" di comunicazione. Al contrario, l'UDP è senza connessione e invia solo i datagrammi richiesti dal livello applicativo.
- L'UDP non offre nessuna garanzia sull'affidabilità della comunicazione ovvero sull'effettivo arrivo dei datagrammi e sul loro ordine in sequenza ed in arrivo. Al contrario il TCP, tramite i meccanismi di "acknowledgement" e di ritrasmissione su timeout, riesce a garantire la consegna dei dati, anche al costo di un maggiore overhead (raffrontabile visivamente confrontando la dimensione delle intestazioni dei due protocolli).
- L'oggetto della comunicazione di TCP è il flusso di byte, mentre quello di UDP è il singolo datagramma.

Pacchetto TCP

Vediamo velocemente insieme come è fatto un pacchetto TCP.

TCP Header

Bit offset	Bits 0–3	4–7	8–15	16–31
0	Source port			Destination port
32	Sequence number			
64	Acknowledgment number			
96	Data offset	Reserved	CWR ECE URG ACK PSH RST SYN FIN	Window Size
128	Checksum			Urgent pointer
160	Options (optional)			
160/192+	Data			

Gli argomenti che tratteremo ora sono i seguenti:

- **Port Scanning**: rilevazione porte TCP/UDP aperte (pericoli in agguato).
- **Sniffer**: rilevazione di protocolli che generano broadcast o multicast a livello 2.
- **Shared di rete**: permessi e accessi a cartelle condivise.

Port Scanning

In informatica il Port Scanning è una tecnica utilizzata per raccogliere informazioni su un computer connesso ad una rete stabilendo quali e quante porte sono in ascolto sulla macchina esaminata. Letteralmente significa "scansione delle porte" e consiste nell'inviare richieste di connessione al computer bersaglio (soprattutto pacchetti TCP, UDP e ICMP creati ad arte). Elaborando le risposte è possibile stabilire, anche con precisione, quali servizi di rete sono attivi su quel computer. Una porta si dice "in ascolto" (listening) o "aperta" quando vi è un servizio o programma che la usa. Di per sé il port scanning non è pericoloso per i sistemi informatici, e viene comunemente usato dagli amministratori di sistema per effettuare controlli e manutenzione.

Il suo impiego rivela però informazioni dettagliate che potrebbero essere facilmente usate da un eventuale attaccante per preparare una tecnica mirata a minare la sicurezza del sistema. Per questo viene posta molta attenzione dagli amministratori a come e quando vengono effettuati port scan verso i computer della loro rete. Un buon amministratore di sistema sa che un firewall ben configurato permette alle macchine di svolgere tutti i loro compiti, ma rende difficile, se non impossibile, la scansione delle porte. E' possibile comunque procedere implementando ad esempio, meccanismi di accesso selettivo basati sul **port knocking**.

TCP Port

Le porte sono numeri (TCP e UDP riservano 16 bit per un totale di 2^16=65536 porte possibili) utilizzati per identificare una particolare connessione di trasporto tra quelle al momento attive su un calcolatore.
I pacchetti appartenenti ad una connessione sono identificati dalla seguente quadrupla: **[<indirizzo IP sorgente>, <indirizzo IP destinazione>, <porta sorgente>, <porta destinazione>]**.
I pacchetti nella direzione opposta avranno ovviamente sorgente e destinazione scambiati. Mentre la porta di destinazione è l'identificativo univoco del processo applicativo, la porta di sorgente è assegnata casualmente in maniera tale da identificare univocamente la connessione da parte del mittente col destinatario all'interno di una rete locale.
Il livello di trasporto (tipicamente realizzato dal sistema operativo) associa a ciascuna porta utilizzata un punto di contatto (ad esempio, una socket), utilizzata da uno o più processi applicativi per trasmettere e/o ricevere dati.
Per poter inviare con successo un pacchetto con una certa porta destinazione, ci deve essere un processo che è "in ascolto" su quella porta, ovvero che ha chiesto al sistema operativo di ricevere connessioni su quella porta.
La porta sorgente utilizzata in una connessione viene scelta dal calcolatore che inizia la connessione tra una di quelle al momento non impegnate.
In Internet, c'è una convenzione per cui ad alcuni numeri di porta sono associati determinati protocolli di livello applicativo. Ad esempio: se voglio contattare il server HTTP eventualmente in esecuzione su un certo calcolatore, so che devo tentare di stabilire una connessione verso la porta 80. I numeri di porta sono classificabili in tre gruppi:

- Le porte conosciute, assegnate dall'Internet Assigned Numbers Authority (IANA), sono quelle inferiori a 1024, e sono generalmente utilizzate a livello di sistema operativo o di processi di sistema.

  In genere rimangono in ascolto su queste porte applicazioni con funzioni di server. Alcuni esempi possono essere le applicazioni che utilizzano protocolli FTP (21), SSH (22), TELNET (23), SMTP (25) e HTTP (80). Sono dette porte ben note.
- Le porte registrate invece sono spesso utilizzate come riferimento fra applicazioni, come una specie di accordo.
- Le porte dinamiche sono tutte le altre. Sono liberamente utilizzabili da tutte le applicazioni utente, salvo l'occupazione contemporanea da parte di qualche altro processo.

Le porte più comuni

Supervisionare le porte "in ascolto" cioè aperte è di estrema importanza sul fronte della sicurezza dei dati per evitare attacchi informatici che nel caso più grave possono portare al controllo completo del computer da parte dell'intruso. Le porte normalmente più vulnerabili sono quelle legate a servizi e applicazioni di cui abbiamo già parlato nelle lezioni precedenti:

- Servizi di Login: Telnet (23/TCP), SSH (22/TCP), NetBIOS (139/TCP), ecc.
- Posta: SMTP (25/TCP), POP (109/TCP e 110/TCP), IMAP (143/TCP), ecc.
- Web: HTTP (80/TCP) e SSL (443/TCP, tranne quelle verso i server web esterni. Si dovrebbero bloccare anche le porte HTTP comuni (8000/TCP, 8080/TCP, 8888/TCP e così via)
- Piccoli servizi: porte prima delle 20/TCP e 20/UDP, NTP(TCP/UDP:123)

Ecco un elenco delle principali porte:

Porta	Descrizione
1/tcp	TCP Multiplexor
2/tcp	compressnet Management Utility
3/tcp	compressnet Compression Process
7/tcp	Echo Protocol
7/udp	Echo Protocol
8/udp	Bif Protocol
9/tcp	Discard Protocol
9/udp	Discard Protocol
13/tcp	Daytime Protocol
17/tcp	Quote of the Day
19/tcp	Chargen Protocol
19/udp	
20/tcp	
21/tcp	
22/tcp	

23/tcp	Chargen Protocol
25/tcp	FTP - Il file transfer protocol - data
53/tcp	FTP - Il file transfer protocol - control
53/udp	SSH - Secure login, file transfer (scp, sftp) e port forwarding
67/udp	Telnet insecure text communications
68/udp	SMTP - Simple Mail Transfer Protocol (E-mail)
69/udp	DNS - Domain Name Server
70/tcp	DNS - Domain Name Server
	BOOTP Bootstrap Protocol (Server) e DHCP Dynamic Host Configuration Protocol (Server)
	BOOTP Bootstrap Protocol (Client) e DHCP Dynamic Host Configuration Protocol (Client)
	TFTP Trivial File Transfer Protocol
	Gopher

79/tcp	finger Finger
80/tcp	HTTP HyperText Transfer Protocol (WWW)
88/tcp	Kerberos Authenticating agent
104/tcp	Dicom - Digital Imaging and Communications in Medicine
110/tcp	POP3 Post Office Protocol (E-mail)
113/tcp	ident vecchio sistema di identificazione dei server
119/tcp	NNTP usato dai newsgroups usenet
123/udp	NTP usato per la sincronizzazione degli orologi client-server
137/udp	NetBIOS Name Service
138/udp	NetBIOS Datagram Service
139/tcp	NetBIOS Session Service
143/tcp	IMAP4 Internet Message Access Protocol (E-mail)
161/udp	SNMP Simple Network Management Protocol (Agent)
162/udp	SNMP Simple Network Management Protocol (Manager)
389/tcp	LDAP
411/tcp	Direct Connect Usato per gli hub della suddetta rete
443/tcp	HTTPS usato per il trasferimento sicuro di pagine web
445/tcp	Microsoft-DS (Active Directory, share di Windows, Sasser-worm)
445/udp	Microsoft-DS SMB file sharing
465/tcp	SMTP - Simple Mail Transfer Protocol (E-mail) su SSL
500/udp	IKE chiave di scambio Internet. associazione di sicurezza nella suite di protocolli IPSec
514/udp	SysLog usato per il system logging
563/tcp	NNTP Network News Transfer Protocol (newsgroup Usenet) su SSL
591/tcp	FileMaker 6.0 Web Sharing (HTTP Alternate, si veda la porta 80)
631/udp	IPP / CUPS Common Unix printing system
636/tcp	LDAP su SSL
636/udp	LDAP su SSL
666/tcp	Doom giocato in rete via TCP
993/tcp	IMAP4 Internet Message Access Protocol (E-mail) su SSL
995/tcp	POP3 Post Office Protocol (E-mail) su SSL

Classificazione delle porte

I sistemi di port scanning classificano le porte secondo queste 6 categorie (nmap):

- **Open** (aperta)
- **Closed** (chiuse)
- **Filtered** (filtrata)
- **Unfiltered** (non filtrata)
- **Open|filtered** (aperta|filtrata)
- **Closed|filtered** (chiusa|filtrata)

Questi stati non sono proprietà intrinseche delle porte stesse, ma descrivono come i port scanning le vedono. Ad esempio, uno scan Nmap proveniente dalla stessa rete nella quale risiede l'obbiettivo può mostrare la porta 135/tcp come aperta, mentre una scansione nello stesso momento con gli stessi parametri ma proveniente da internet può mostrare quella stessa porta come filtered.

Open: un'applicazione accetta attivamente su questa porta connessioni TCP o UDP. La ricerca di questo tipo di porte è spesso l'obbiettivo primario del port scanning. Chi si dedica alla sicurezza sa che ogni porta aperta può diventare una strada per un possibile attacco. Gli attaccanti e i tester di sicurezza (penetration testers), conosciuti anche come "pen-testers" hanno come obbiettivo quello di trovare e trarre vantaggio dalle porte aperte, mentre d'altro canto gli amministratori di rete e i sistemisti provano a chiuderle o a proteggerle con firewall cercando di limitare il meno possibile gli utenti autorizzati al loro uso. Le porte aperte sono anche interessanti per tutta una serie di scansioni non indirizzate unicamente alla sicurezza ma perché mostrano i servizi disponibili sulla rete.

Closed: una porta chiusa è comunque accessibile (riceve e risponde ai pacchetti di probe) ma non vi è alcuna applicazione in ascolto su di essa. Si rendono utili perché possono mostrare l'attività di un host su un particolare indirizzo IP (host discovery o ping scanning), oppure per evidenziare le tipologie di sistemi operativi installati (operating system discovery). Poiché una porta chiusa rimane raggiungibile, per verificare se queste vengono aperte è sempre consigliato effettuare scansioni a posteriori. Chi amministra una macchina o una rete può bloccare tali porte con un firewall che, in questo caso, le farebbe apparire "filtrate", come mostrato in seguito.

Filtered: in questo caso non si può determinare con esattezza se la porta sia aperta o meno, perché un filtro attivo sui pacchetti in transito impedisce ai probe di raggiungere la porta. Questo filtro può esser dovuto a un firewall dedicato, alle regole di un router, o a un firewall software installato sulla macchina stessa. Per loro natura queste porte forniscono poche informazioni e rendono frustrante il lavoro dell'attaccante. Questa tipologia di porta a volte può rispondere con un messaggio ICMP del tipo 3, codice 13 ("destination unreachable: communication administratively prohibited", ovvero "destinazione non raggiungibile: comunicazione impedita da regole di gestione"). In genere è molto più comune il filtraggio di tutti i pacchetti che semplicemente ignorano i tentativi di connessione senza rispondere. Questa modalità di "non risposta" obbliga a riprovare molte volte, semplicemente per essere sicuri che il pacchetto non sia stato perduto a causa di una congestione di rete o di problemi simili piuttosto che dal firewall o dal filtro stesso. Questo riduce drammaticamente la velocità della scansione.

Unfiltered: lo stato "unfiltered" indica che una porta è accessibile, ma che non siamo in grado di determinarne lo stato di aperta o chiusa. Solo la scansione di tipo ACK, usata per trovare e classificare le regole di un firewall, può correttamente indicare una porta in questo stato. Una ricerca di porte in questo stato ("non filtrate") mediante altri tipi di scansione come il "Window scan" (scan per finestre di connessione), il "SYN scan" o il "FIN scan" aiuta a determinare se la porta sia aperta o chiusa.

Open|filtered: la porta rilevata in questo stato non consente di determinare se sia aperta o filtrata. Questo accade quando una porta aperta non risponde in alcun modo. La mancanza di informazioni potrebbe anche significare che un filtro di pacchetti ha lasciato cadere ("drop") il probe o qualsiasi risposta sia stata generata in seguito. Le ricerche che classificano porte in questo stato sono le scansioni IP, UDP, FIN, Null, e Xmas.

Closed|filtered: questo stato è usato quando non si è in grado di determinare se una porta sia chiusa o filtrata. Esso viene usato solo per l'IPID "Idle scan".

Sniffing

Tutto ciò che è trasferito e lasciato circolare in una rete è suddiviso e "incapsulato" in unità ben definite chiamate "pacchetti". Ogni pacchetto viene etichettato con un indirizzo IP e/o un indirizzo MAC che specifica la sua destinazione, e ad esso sono associati altri parametri (header) che serviranno ad instradare e riassemblare i pacchetti, operazione compiuta dalla macchina del destinatario. Poiché tutto il traffico di una rete deve essere ridotto in pacchetti lo **sniffer** non deve far altro che raccogliere tale traffico e analizzarlo sia nella sua forma frammentata sia nella sua forma riassemblata, alla ricerca delle informazioni a cui si mira. Le funzioni tipiche degli **sniffer** possono sinteticamente essere riassunte in:

- filtraggio e conversione dei dati e dei pacchetti in una forma leggibile dall'utente;
- analisi dei difetti di rete, ad es. perché il computer A non riesce a dialogare con B;
- analisi di qualità e della quantità dei dati trasportati dalla rete (performance analisys);
- ricerca automatizzata di password e nomi di utenti (in chiaro o cifrati) per successiva analisi;
- creazione di log: lunghi elenchi contenenti traccia del traffico sulla rete; ➢ scoperta di intrusioni in rete attraverso l'analisi dei log del traffico.

Livelli di rischio

Gli **sniffer** rappresentano un rischio elevato per una rete o per il PC dell'utente medio. La semplice esistenza di uno **sniffer** in rete rappresenta una falla e una minaccia alla sicurezza e alla riservatezza delle comunicazioni all'interno della rete stessa. Quando la LAN che si utilizza è sottoposta al controllo di uno **sniffer** ci sono di solito due possibilità:

1. un intruso, dall'esterno, è riuscito ad entrare all'interno della rete e ad installare lo sniffer;
2. oppure un utente o il gestore della rete stessa sta combinando qualcosa che potrebbe andare ben oltre la manutenzione e il monitoraggio delle connessioni.

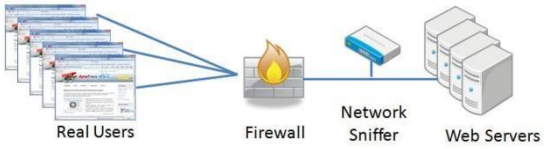
In ogni caso la privacy, o peggio, la sicurezza stessa delle comunicazioni, è compromessa.

TCP/IP agevola gli sniffer

TCP/IP non offre nessun meccanismo di verifica o protezione dei dati. I dati viaggiano in chiaro e non è fornito nessun modo per garantire l'autenticità degli interlocutori, sebbene ciò possa essere fatto dalle applicazioni. Ciascuna macchina su cui viaggiano i dati potrebbe visualizzarli o anche modificarli. Se un'applicazione gestisce a basso livello la connessione può addirittura falsificare la propria identità (man in the middle) in quanto TCP/IP si ***fida*** semplicemente dell'indirizzo specificato dal mittente. Anche a livello applicativo non vengono adottati automaticamente strumenti per garantire l'autenticità e la privacy dei dati.

Utilità dello sniffer

Ovviamente uno degli scopi della lezione non è quello di impiegare lo **sniffer** per acquisire informazioni perché abbiamo parlato di questa possibilità nelle lezioni precedenti. L'obiettivo è invece quello di utilizzare lo strumento per identificare gli eventuali problemi della nostra rete. Uno **sniffer** deve essere solitamente connesso ad un dominio di collisione, ad un hub o, se si utilizza uno switch, ad una porta configurata in monitor sugli apparati di rete di layer 2.
In questo modo viene filtrato tutto il traffico in transito da una specifica porta.
L'utilizzo invece da noi consigliato è quello di attivarlo connessi alla propria rete aziendale in modo da verificare quali pacchetti raggiungono la nostra interfaccia di rete in quanto broadcastati sulla stessa e che potrebbero rappresentare un problema. Alcune applicazioni o una rete mal costruita, possono generare un traffico anomalo a livello 2, quindi può capitare di ricevere pacchetti che per loro natura generano traffico e rallentano le prestazioni della nostra rete.



Analisi

L'analisi dei pacchetti ricevuti è fondamentale per individuare ed isolare il problema. Quanto espresso nel precedente capitolo inerente alle porte TCP/UDP aperte è in stretta correlazione con l'utilizzo dello sniffer quale strumento utile all'identificazione dei protocolli dannosi o applicazioni mal configurate. L'uso di sistemi come le chat, diffuse in molti social network, potrebbe aprire altre porte di comunicazione che, senza un controllo adeguato, potrebbero rappresentare una strada per fare entrare software molto pericolosi. Al fine di ridurre il livello di potenziale vulnerabilità delle macchine di una rete (ma anche di una singola macchina), è opportuno verificare che siano attivi soltanto i servizi e/o protocolli necessari. La presenza di elementi superflui, infatti, rappresenta una grave minaccia alla sicurezza.

Una buona abitudine è quella di verificare periodicamente questo genere di cose sia durante il processo di installazione del sistema operativo, sia in seguito, al fine di assicurarsi che non siano stati attivati, anche involontariamente, servizi e/o protocolli non necessari. La presenza di elementi del genere non utilizzati, apre verso l'esterno un certo numero di porte TCP/IP, che diventano fonte di numerosi problemi sia sotto l'aspetto delle prestazioni, in quanto la loro presenza consuma risorse di sistema, sia sotto quello della sicurezza. Siccome l'utente ignora la loro presenza non si farà neppure carico di applicare le patch per la sicurezza rilasciate dal produttore, dando così spazio agli exploit dei potenziali aggressori.

Facciamo un esempio pratico:

- mediante l'attivazione di uno sniffer verifichiamo il traffico che transita dalla nostra scheda di rete non connessa in stealth (in modo furtivo sulla rete tramite hub o monitor port) ma in modo tradizionale alla rete;

- mediante uno strumento di port scan analizziamo le porte aperte dei client connessi alla nostra rete.

I risultati del test potrebbero essere i seguenti, lo sniffer rileva un traffico UDP di tipo multimediale (voce o video) broadcastato sulla rete come di seguito indicato:

24/11/2010 - 11:56:40	24/11/2010 - 11:56:40	192.168.20.106:52834 (MPA,90Khz,Mono)	224.0.0.252:5355	IP1 codec n...
24/11/2010 - 13:03:05	24/11/2010 - 13:03:05	192.168.20.5:58667 (LPC,8Khz,Mono)	224.0.0.252:5355	IP1 codec n...
24/11/2010 - 16:12:13	24/11/2010 - 16:12:13	192.168.20.5:56894 (GSM,8Khz,Mono)	224.0.0.252:5355	IP1 codec n...
24/11/2010 - 18:08:14	24/11/2010 - 18:08:14	192.168.20.5:56631	224.0.0.252:5355	
24/11/2010 - 19:00:40	24/11/2010 - 19:00:40	192.168.20.5:49671 (QCELP,8Khz,Mono)	224.0.0.252:5355	IP1 codec n...
24/11/2010 - 22:24:01	24/11/2010 - 22:24:01	192.168.20.5:52789 (PCMU,8Khz,Mono)	224.0.0.252:5355	
25/11/2010 - 02:44:35	25/11/2010 - 02:44:35	192.168.20.5:50587 (G722,8Khz,Mono)	224.0.0.252:5355	
25/11/2010 - 08:58:29	25/11/2010 - 08:58:29	192.168.20.5:50616 (G728,8Khz,Mono)	224.0.0.252:5355	IP1 codec n...
25/11/2010 - 09:30:25	25/11/2010 - 09:30:25	192.168.20.5:59011 (G729,8Khz,Mono)	224.0.0.252:5355	IP1 codec n...
25/11/2010 - 10:14:21	25/11/2010 - 10:14:21	192.168.20.5:57548 (LPC,8Khz,Mono)	224.0.0.252:5355	IP1 codec n...

Verificando quali porte sono aperte su uno dei client che genera quel tipo di traffico riscontriamo:

IP Address	MAC Address	Open Port
192.168.20.5	00-0F-20-CF-B6-50	21, 443, 80

Analizzando le porte di un client in rete ci chiediamo il motivo per cui siano in ascolto le porte 80 e 443 non essendo un web server o non erogando alcun servizio. La risposta è molto semplice……..**SKYPE!**

In pratica il client ha installato **Skype**. Aziendalmente le policy non consentono l'utilizzo di questo strumento inibendo tramite firewall il suo utilizzo, ma il client cerca comunque di terminare le connessioni per conto terzi continuando a trasmettere pacchetti broadcasting in rete non potendo portare a termine le connessioni richieste a causa del firewall stesso.

E' possibile verificare di come l'accesso a **Skype** apra porte in modalità "ascolto" sul client in grado di bypassare il firewall (80 e 443). Il client in queste condizioni si comporta come un "**super nodo**" al quale terzi possono collegarsi per effettuare chiamate. Queste connessioni generano traffico e aprono falle di sicurezza. Per questo alcuni enti hanno bandito **Skype** dalle proprie reti aziendali in quanto giudicata come un'applicazione precaria in termini di sicurezza.

Se sul nostro client proviamo a verificare il numero delle porte in ascolto, con e senza **Skype** avviato, potremo appurare che l'applicazione in oggetto ha aperto un certo numero di connessioni che rimangono "pericolosamente aperte" nonostante non sia utilizzata. Davvero un'amara sorpresa.

Condivisioni di rete

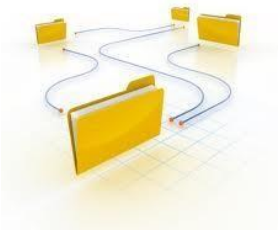
Durante gli audit ci capita sovente di riscontrare configurazioni di autorizzazioni non corrette, che di fatto consentono a chiunque l'accesso alle cartelle di rete. Esistono due scenari tipici per cui potrebbe risultare necessario tenere sotto controllo le autorizzazioni di accesso:

1. se il nostro PC è condiviso da più persone;
2. se condividiamo file su una rete.

In entrambi i casi ciò che vogliamo evitare è che un utente non autorizzato possa dare una sbirciatina ai nostri file o che, ancora peggio, possa involontariamente cancellarli. Ma ancora più pericoloso è che quando i file sono condivisi in rete il cestino non funziona e così l'operazione di eliminazione di un file lo "distrugge" immediatamente.

Le opzioni di controllo attribuibili possono essere le seguenti:

- Controllo completo.
- Modifica.
- Lettura ed esecuzione.
- Visualizzazione contenuto cartella.
- Lettura.
- Scrittura.
- Autorizzazioni Speciali.



Ognuno di queste opzioni comprende delle regole che debbono essere consentite o negate. Nella maggior parte delle situazioni è sempre sufficiente applicare il comando "Consenti". Raramente è necessario utilizzare le "Autorizzazioni Speciali" ma soprattutto è sconsigliabile il loro impiego qualora non si comprenda appieno il significato delle impostazioni.

Durante l'utilizzo delle opzioni di controllo potrebbe succedere che alcuni segni di spunta non siano disponibili e quindi impostabili. Questo succede quando l'oggetto su cui si sta operando eredita le opzioni dall'oggetto padre. Per modificare anche queste impostazioni è necessario cliccare sul comando "Avanzate" e quindi procedere a rimuovere le **Autorizzazioni Ereditabili dal Padre.**

Non è oggetto della lezione quello di insegnare come applicare le policy, cosa molto semplice se si è all'interno di un Dominio AD (Active Directory), ma che un utente ospite, sfogliando la rete possa accedere a cartelle condivise, rappresenta sicuramente un fatto molto grave.

Possono presentarsi diversi casi:

- Le cartelle contengono documenti aziendali.
- Le cartelle contengono documenti personali. ➢ Le cartelle non contengono nulla.

Inoltre:

- L'utente ha creato in autonomia la condivisione.
- L'amministratore di rete non ha configurato correttamente le policy.

Quanto sopra può esprimere responsabilità aziendali e rientra nella violazione del codice privacy, oppure nelle responsabilità personali sempre previste dal codice in quanto:

tutti gli utenti sono incaricati al trattamento dei dati.

Attenzione: anche l'esposizione di una cartella vuota può essere un grosso problema in quanto può consentire di scriverci dentro oppure di depositare file compromettenti che potrebbero poi essere utilizzati contro di noi in quanto proprietari della rete.

Conclusioni

In questa lezione abbiamo potuto constatare come gli strumenti usati solitamente per attaccare e creare danni ad una rete aziendale, possono, anzi **devono**, essere usati per controllare l'affidabilità e la corretta configurazione della propria rete.

Sottovalutare porte aperte, protocolli non sicuri od esporre le proprie informazioni, rischia di tradursi in un danno che alle volte può diventare irreparabile per cui…….

Molto meglio porvi rimedio per tempo!!!

Lesson 6: Pubblicazione Servizi

Internet

Durante le precedenti lezioni abbiamo preso in considerazione la sicurezza lato interno alla rete evidenziando il fatto che la percentuale di attacchi informatici effettuati partendo dall'interno è enormemente superiore rispetto a quelli effettuati dall'esterno alla rete stessa.

E' comunque un dato certo che la crescente disponibilità di banda passante, unita ai sempre minori costi di connettività ed alla disponibilità sempre maggiore dei punti d'accesso, ha reso di fatto internet il principale mezzo di comunicazione tra le aziende ed il mondo esterno che viene sfruttato per la pubblicazione dei servizi.

Purtroppo come tutte le cose anche questa magnifica costruzione ha il suo **tallone d'Achille**: "la sicurezza".

Proprio perché "reti aperte", le reti digitali sono intrinsecamente insicure non essendo state progettate in modo da garantire autoprotezione e difesa contro eventuali abusi.

Come abbiamo avuto modo di evidenziare nelle precedenti lezioni le reti dati sono particolarmente sensibili all'intercettazione ed all'alterazione dei dati trasmessi nonché alla violazione dei supporti informatici ad esse connessi.

A seconda dell'applicazione realizzata il problema può essere più o meno sentito in funzione della tipologia di dati trasferiti. Quando si parla di commercio elettronico, o più in generale quando i dati trasferiti contengono informazioni riservate, la sicurezza diventa il presupposto fondamentale sul quale si fonda il rapporto fiduciario fra acquirente e venditore, fra banche e correntisti, fra azienda e collaboratori esterni. Senza la fiducia, ispirata dalla sicurezza delle transazioni, non può essere instaurata nessuna relazione.

Senza garanzie adeguate l'utente non avrà incentivi all'utilizzo di tali tecnologie che, sebbene più convenienti, sono anche più insicure.

Inoltre, il desiderio di garantire il proprio anonimato da parte dell'utente, mal si concilia con la necessità del sistema informatico che rende obbligatoria l'imputazione dei dati. Di fatto questa operazione se captata potrebbe svelare l'identità degli utenti e le operazioni fatte.

Anche il tentativo di creare siti completamente anonimi va contro le esigenze di imputabilità, autenticità, integrità, revocabilità o non ripudiazione e non può certo essere in armonia con la necessità di applicare la legge a fronte di frodi più o meno significative.

L'ideale è trovare un giusto bilanciamento fra tutte le diverse esigenze, ma tale compromesso dove essere adeguatamente protetto.

La protezione delle informazioni trasmesse via Internet, oltre a richiedere tutte le attenzioni normalmente dedicate ai corrispondenti documenti cartacei, richiede anche quelle necessarie a garantire la sicurezza dell'intero processo trasmissivo.

Il passaggio dai documenti tradizionali al relativo documento elettronico deve venire gestito in maniera tale da conservare, ed eventualmente migliorare, le tradizionali politiche di sicurezza al fine di rendere l'intero sistema di comunicazione sicuro.

Il WEB

L'efficacia del Web come mezzo di divulgazione delle informazioni o come strumento per la vendita di prodotti/erogazione di servizi è ormai nota a tutti e spinge, giorno dopo giorno, sempre più entità ed organizzazioni a scegliere Internet come canale preferenziale di contatto con il pubblico.

L'uso di questo canale, se da un lato apre la strada a possibilità di sviluppo prima impensabili, per converso, presenta dei rischi che non possono essere sottovalutati.

Le cronache di tutti i giorni riportano sempre con maggiore frequenza notizie relative ad intrusioni perpetrate ai danni di sistemi informatici più o meno noti. Non passa settimana in cui, attraverso la pubblicazione dei principali bollettini di sicurezza, non venga data rilevanza della scoperta di pericolosi "bug od exploit" destinati ad essere sfruttati per compiere attacchi informatici di vario genere.

Ma cosa rende un server Web una risorsa così appetibile ed esposta agli attacchi esterni? Sicuramente una combinazione di molteplici fattori tra i quali vanno citati i seguenti:

- i server Web spesso rappresentano delle vere e proprie porte di accesso alla rete interna (LAN) nella quale sono custodite le informazioni più svariate (informazioni aziendali, dati sul personale, sulla clientela, dati di rilevanza economica e legale, etc..).
- La sottovalutazione dei rischi e la mancanza di risorse economiche ed umane da dedicare al potenziamento delle politiche di sicurezza e la scarsa progettazione e qualità del software possono determinare l'insorgere di una condizione di intrinseca vulnerabilità dei servizi Web resa ancora più grave dalla loro esposizione al pubblico.
- Condurre con successo un attacco sul Web utilizzando le classiche porte del servizio http (80, 81, 8000, etc..) è molto più facile dal momento che nella stragrande maggioranza

dei casi il traffico veicolato in questo modo non è bloccato dai dispositivi di controllo degli accessi (router e/o firewall).

Dalla combinazione di questi ed altri fattori possiamo trarre lo spunto per fare una semplice osservazione: via via che si acquisisce visibilità in Internet si accrescono anche le probabilità di vedere, prima o poi, il proprio server violato.

Il rischio di subire intrusioni od attacchi di altro genere non è soltanto circoscritto ai grandi portali del Web ma si estende anche alle semplici risorse di carattere statico le quali, se non debitamente protette, possono attirare l'attenzione non proprio benevola di qualche male intenzionato.

Sfortunatamente non esistono nè rimedi nè tecniche tali da poter rendere sicuro al 100% un server contro gli attacchi provenienti dall'esterno, ma si può operare nella direzione di rendere più sicuro il proprio server iniziando con il tenere lontani problemi e vulnerabilità.

Per fare ciò occorre innanzitutto comprendere la natura e la portata dei pericoli ai quali ci si espone e successivamente adottare delle precauzioni di carattere generale dirette a circoscrivere i rischi suddetti entro limiti accettabili in relazione alla natura degli interessi da proteggere.

Individuazione dei rischi

Fondamentalmente i pericoli derivanti dalla mancata adozione di adeguati criteri di sicurezza nell'allestimento e nel mantenimento di un sito Web pubblicato sono riconducibili alla possibilità di un abuso del servizio da parte di soggetti malintenzionati. Questo abuso può essere perpetrato in svariati modi ma molto spesso viene concepito sfruttando gli errori di configurazione o le vulnerabilità esistenti a livello di:

- sistema operativo;
- servizio http od altri servizi di rete (smtp, database, ftp, etc..);
- programmi/interpreti e script utilizzati per la generazione del contenuto del sito; ➢ dispositivi di controllo degli accessi (routers e firewalls).

In linea generale il percorso che un aggressore tenta di seguire nell'attacco di un sistema può essere riassunto nel seguente modo:

- accesso al sistema attraverso l'esecuzione di exploit;
- sfruttamento di condizioni di buffer overflow in script e programmi;
- cattura o intercettazione del file delle password;
- attacchi a forza bruta;
- scalata dei privilegi e/o impersonificazione degli utenti con privilegi amministrativi attraverso il crack delle password e/o l'esecuzione di exploit successivi;
- occultamento delle tracce tramite la cancellazione dei logs;
- uso di rootkits e sfruttamento di particolari caratteristiche del sistema operativo;
- installazione di backdoors cioè di programmi nascosti che permettono all'aggressore un ritorno ed una ripresa del controllo del sistema in un secondo momento.

Come conseguenza di queste azioni, l'aggressore può essere portato ad eseguire delle attività che rientrano nelle seguenti aree:

- attività che comportano una manipolazione del server e/o un trafugamento di informazioni:
- atti di vandalismo come la modifica dei contenuti delle pagine Web o la cancellazione del contenuto dell'intero sito;
- trafugamento di informazioni sensibili concernenti l'organizzazione, la configurazione di rete oppure la clientela o gli utenti;
- uso dell'host come base per lanciare attacchi contro altri sistemi (attacchi D.D.O.S - Distributed Denial of Service);
- installazione di strumenti per il monitoraggio del traffico di rete e la cattura di informazioni di autenticazione (sniffing);
- attività che producono una situazione di indisponibiltà del servizio (D.O.S. - Denial of Service) cioè l'impossibilità per gli utenti di accedere alle risorse messe a disposizione dal server.

Il diniego del servizio (D.O.S) rappresenta per l'aggressore una soluzione estrema che, oltretutto, richiede spesso competenze tecniche davvero minime. Le conseguenze di simili attacchi sono veramente molteplici e vanno dalla sopportazione dei costi per il ripristino delle risorse al mancato realizzo di introiti. Ma l'aspetto più grave è la perdita di credibilità nei confronti del pubblico che può arrivare anche a conseguenze che implicano una responsabilità di carattere legale (perdita o trafugamento di informazioni sensibili a causa di una negligente gestione del sito).

Strumenti di Sicurezza

La DMZ: cos'è e perché si usa

Dividere la rete in zone è una tecnica considerata base che presenta l'immediato vantaggio aumentare la sicurezza. Cerchiamo di capire cos'è e come funziona la DMZ il cui acronimo significa "zona demilitarizzata".

La sicurezza perimetrale si occupa di proteggere una rete nei punti in cui essa è a contatto con il mondo esterno. In base al tipo di traffico e alla funzione si identificano diverse zone; nei casi più semplici, le uniche due zone, LAN e WAN sono attestate sui due lati del firewall.

Il lato LAN (local area network) è il segmento privato e protetto, e ad esso appartengono tutti gli host ed i server i cui servizi sono riservati all'uso interno. Nelle lezioni precedenti abbiamo parlato di come implementare la sicurezza mediante l'uso delle VLAN per suddividere anche la rete interna.

La zona WAN (wide area network) è la parte esterna, e ad essa appartengono uno o più apparati di routing che sostengono il traffico da e per la rete locale, sia verso internet che verso eventuali sedi remote dell'azienda.

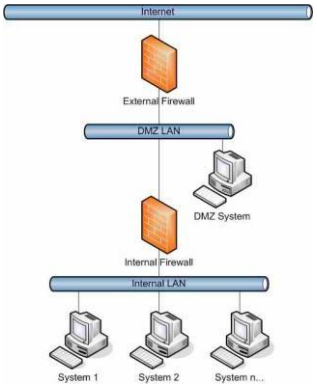
Non appena l'architettura della rete comincia ad evolversi, ci si trova nella necessità di esporre all'esterno alcuni servizi. Il caso più comune è la posta elettronica di cui abbiamo ampiamente discusso nella lezione 2.

L'installazione di un mail server "in casa" comporta la pubblicazione del servizio SMTP. Quando la struttura ed il budget non sono particolarmente importanti, spesso si decide di fidarsi del firewall e delle sue tabelle di NAT.

Pubblicare direttamente la porta SMTP del server di posta non è ortodosso dal punto di vista della sicurezza. Questa soluzione è molto spesso adottata dalle piccole aziende che non possono sostenere costi di infrastruttura troppo elevati.

Non appena possibile è fortemente consigliata la creazione di una terza zona: la DMZ.

Una DMZ rappresenta di fatto un'area in cui sia il traffico WAN che quello LAN sono fortemente limitati e controllati. In pratica, si tratta di una zona "cuscinetto" tra interno ed esterno, che viene attestata su una ulteriore interfaccia di rete del firewall, oppure creata ex novo aggiungendo un firewall, come nello schema di seguito riportato.



Generalmente si installano in DMZ i server detti front-end, a cui corrispondono i relativi back-end in LAN.

Anche in questo caso l'esempio tipico è la posta elettronica. Il server che pubblica il servizio SMTP ed eventualmente la webmail, l'antispam e l'antivirus vengono posti sulla DMZ, mentre in LAN rimane il server che ospita il database delle caselle e gli altri servizi.

Altro caso tipico sono gli "application server", che isolano un database residente in LAN ma ne offrono una interfaccia come servizio verso l'esterno.
Quali sono i vantaggi per la sicurezza?

Nel malaugurato caso in cui un servizio in LAN risultasse compromesso a seguito di una vulnerabilità, l'aggressore potrebbe raggiungere anche gli altri host della rete, dato che in LAN non esiste isolamento tra il server e gli altri nodi. Ma se lo stesso problema si verificasse in DMZ, l'attaccante avrebbe grosse difficoltà a raggiungere la LAN, poiché il traffico tra i server front-end e back-end è fortemente limitato dal firewall. In genere un server di front-end comunica solo con il suo back-end, e solo con le porte TCP e/o UDP strettamente necessarie.

Ricapitolando: la DMZ è un'area pubblica protetta, dove il traffico è strettamente regolato da entrambi i lati, è utile per pubblicare servizi verso l'esterno minimizzando i rischi per la rete interna. E' possibile realizzare architetture più complesse che possono implicare la presenza di più zone DMZ distinte, con il relativo controllo del traffico su tutti i lati.

Configurazione di base del server

In linea teorica il server Web dovrebbe operare nell'ambito di una configurazione di rete e di sistema davvero minima. Il rispetto di questa semplice regola è effettivamente in grado di produrre come risultato un sensibile miglioramento dei livelli di sicurezza attraverso degli espedienti quali:

- la disabilitazione di tutti i servizi di rete non essenziali ed, in particolar modo quelli affetti da vulnerabilità conosciute sotto il profilo della sicurezza.
- La rimozione dal sistema dei files corrispondenti ai servizi disabilitati.
- L'eliminazione delle porte TCP ed UDP in ascolto superflue.
- La rimozione o disabilitazione di tutte le risorse non richieste in relazione al ruolo dell'host (compilatori, interpreti, shell, scripts ed altri strumenti analoghi).
- La corretta gestione degli utenti e dei loro privilegi.
- La predisposizione di regole adeguate per l'accesso e l'uso delle risorse.

I primi 4 punti sono particolarmente importanti non soltanto in un ottica generale di riduzione dei rischi di compromissione del sistema ma anche in vista di uno snellimento delle attività di amministrazione e, quindi, della minore probabilità di commettere errori di configurazione che possono essere prontamente sfruttati dagli aggressori.

A tal fine, proprio per evitare di commettere dimenticanze, è conveniente adottare un approccio del tipo "deny all, then allow" che consiste prima nel disabilitare indistintamente tutti i servizi e le porte TCP/UDP e poi nel riabilitare, dopo un attenta analisi e valutazione, soltanto ciò che è veramente essenziale.

Anche per quanto concerne la gestione degli utenti e dei loro privilegi vanno prefissate regole improntate a criteri restrittivi quali:

- impedire che il "servizio http" venga lanciato da un utente con privilegi amministrativi che potrebbe comportare l'acquisizione del controllo completo del sistema in caso di exploit eseguito con successo.
- Disabilitare o rimuovere tutti gli account inutili, installati dal sistema operativo o da altri software,in modo da ridurre il rischio di un' "impersonificazione" o scalata di privilegi nel caso di intrusione.
- Modificare il nome dell'account di amministratore.
- Adottare criteri di "robustezza password" sotto il profilo della lunghezza (almeno 8 caratteri), complessità (alfanumerica con un mix di caratteri maiuscoli e minuscoli e l'uso di caratteri non stampabili), riutilizzo (da evitare) e durata (mediamente 30-120 giorni).
- Verificare "direttamente le password", preferibilmente mediante gli stessi strumenti usati dagli hackers, per accertarsi che esse rispondano ai criteri voluti.
- Impostare il "blocco degli utenti" dopo un certo numero di tentativi falliti di login.

N.B: il blocco degli utenti è una misura da adottare con cautela dal momento che costituisce un'arma a doppio taglio che potrebbe spingere l'aggressore a provocare una situazione di D.O.S (Denial of Service) attraverso una serie di tentativi di connessione falliti.

I singoli processi coinvolti nella gestione del servizio http devono avere accesso soltanto ai file ed alle directory necessari al loro funzionamento e per i quali occorre specificare delle regole di

accesso (acl o access control list) che, oltre ad offrire una maggiore granularità nel controllo dell'uso delle risorse, sono in grado di scongiurare o mitigare gli effetti derivanti da un eventuale attacco D.O.S diretto a provocare una situazione di indisponibilità dell'intero sistema proprio attraverso l'esaurimento delle sue risorse.

Per ridurre significativamente gli effetti derivanti da attacchi di questo genere, è sempre consigliato il ricorso ad ulteriori interventi correttivi che consistono nel:

- creare una singola directory radice e da essa far derivare una gerarchia di sottodirectory nelle quali suddividere le risorse che costituiscono il contenuto pubblico del Web.
- Limitare ad una sola directory, opportunamente configurata e protetta, tutti i programmi "esterni" eseguiti come parte integrante del servizio Web.
- Limitare l'uso dei file temporanei da parte dei singoli processi all'interno di apposite directory opportunamente protette consentendone l'accesso soltanto ai processi stessi.
- Impedire che file e risorse esterne alla gerarchia di directory del server possano essere forniti come risposta alle richieste degli utenti.
- Disabilitare l'uso dei link simbolici per evitare che risorse facenti parte del contenuto del Web possano puntare a file di sistema o ad altre risorse all'interno della LAN. ➢ Aggiustare le priorità dei vari processi di sistema.

Uso di programmi esterni

L'installazione e l'uso di programmi esterni quali "interpreti, plug-in e script" può letteralmente aprire una breccia nei livelli di protezione di qualsiasi server Web. Anche gli host apparentemente più inviolabili possono infatti cadere a causa di un banale exploit che sfrutta un semplice script "cgi" per eseguire localmente sul server comandi diretti ad ottenere l'accesso al sistema.

Siccome la storia è piena di esempi di questo genere, prima ancora di decidere se sfruttare le funzionalità aggiuntive fornite da script, plug-in ed altro, è sempre opportuno valutare complessivamente i benefici ed i rischi che ne derivano optando per l'adozione soltanto quando i primi siano realmente superiori ai secondi.

In ogni caso la preoccupazione principale deve sempre rimanere quella di ridurre i rischi entro limiti accettabili e per far ciò occorre:

- evitare, se possibile, l'uso di script di terze parti oppure accertarne l'esatta provenienza ed autenticità del codice.
- Fare uso soltanto dei programmi e degli script veramente indispensabili disabilitando tutti gli altri (ad esempio quelli dimostrativi spesso causa di molteplici problemi).
- Impiegare tecniche di programmazione ortodosse nella scrittura del proprio codice prestando la massima attenzione ad aspetti quali la lunghezza e la complessità finale, la presenza di opportuni controlli per la validazione dell'input e l'interazione con altri programmi esterni o l'accesso in lettura e/o scrittura al file system.
- Valutare attentamente la presenza di queste stesse caratteristiche anche negli script di terze parti.

- Usare possibilmente una macchina di test per verificare il funzionamento di tutti i programmi e degli script prima ancora di impiegarli in una macchina di produzione.
- Evitare di collocare i programmi e gli interpreti all'interno della stessa directory dove risiedono gli script (ad esempio la CGI-BIN) e posizionarli invece in una directory separata opportunamente protetta ed accessibile soltanto agli utenti amministratori.
- Circoscrivere l'accesso di programmi ed interpreti ai soli file e directory indispensabili al loro funzionamento e comunque soltanto a quelli all'interno del contenuto pubblico del Web.
- Verificare costantemente l'integrità degli eseguibili relativi a programmi ed interpreti e degli script.

Firewall

Con il termine FIREWALL si tende ad identificare in modo generico tutta una serie di funzioni e di apparecchiature che servono a proteggere un determinato dominio o rete privata.

E' fondamentale stabilire e creare una politica di regole (policy) per poter compiere le seguenti operazioni:

- determinare i servizi di cui si ha bisogno.
- Determinare il gruppo di persone che da servire.
- Determinare a quali servizi ogni gruppo ha necessità di accedere.
- Descrivere per ciascun gruppo come rendere sicuro il servizio.
- Scrivere un'espressione che renda tutte le altre forme di accesso una violazione.

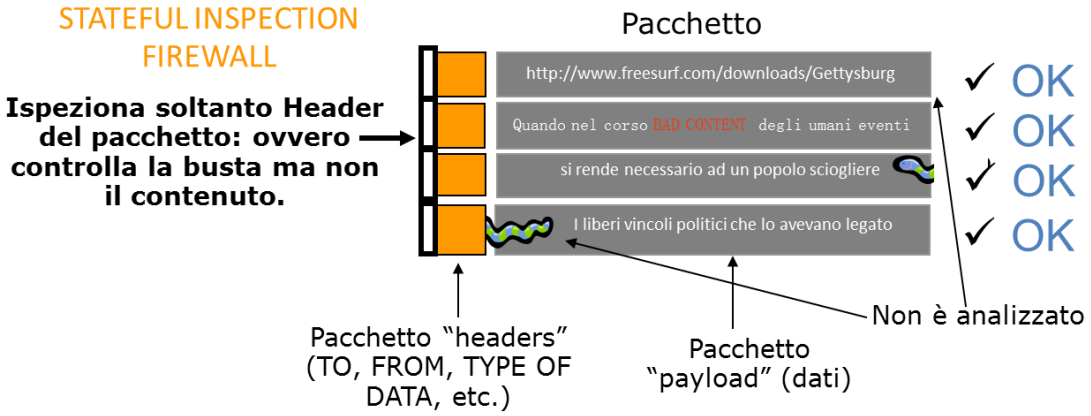
Le policy adottate diventeranno con il trascorrere del tempo e con l'aumentare dell'esperienza sempre più complicate e sempre più efficaci nel loro lavoro di prevenzione a protezione dei dati.

Esistono due tipologie di firewall:

- Firewall Filtranti - che bloccano i pacchetti di rete selezionati; ➢ Proxy Server (talvolta detti firewall).

Firewall Filtranti (Packet Filtering Firewall)

Il Packet Filtering è il tipo di firewall presente nel kernel Linux. Un firewall filtrante funziona a livello di rete. I dati possono lasciare il sistema solo se lo permettono le regole del firewall. I pacchetti che arrivano sono filtrati in base alle informazioni sul tipo, sull'indirizzo di provenienza e di destinazione e sulle porte contenute (TCP/UDP) in ciascuno di essi. Molti router di rete hanno la capacità di effettuare servizi firewall. E' possibile immaginare un "firewall filtrante" come un particolare tipo di router, ma per poterci lavorare è necessaria una profonda conoscenza della struttura dei pacchetti IP.



Poiché sono analizzati e registrati pochissimi dati, i firewall filtranti occupano meno la CPU, e di conseguenza creano minor latenza all'interno della rete. Non forniscono nessun controllo a livello di password in quanto gli utenti non possono identificarsi perchè la sola identità che un utente ha consiste nell'indirizzo IP assegnato alla sua macchina. Attenzione se si intende usare il servizio DHCP (assegnazione dinamica dell'IP) in quanto l'indirizzo assegnato all'utente non è univoco ma variabile ed assegnato in modalità Random dal servizio e siccome le regole sono basate sugli indirizzi IP, dovranno essere aggiornate ogni volta che vengono assegnati nuovi indirizzi.

I firewall filtranti sono più trasparenti per gli utenti in quanto non richiedono nessuna impostazione di regole per utilizzare Internet.

Proxy Server

I Proxy sono apparati H/W e S/W che vengono principalmente usati per controllare, o monitorare, il traffico. Alcuni proxy di applicazioni possono fare la cache dei dati richiesti (memorizzazione in locale), ciò abbassa le richieste di banda e diminuisce il tempo d'accesso per il successivo utente che vuole accedere agli stessi dati fornendo nel contempo un'evidenza inequivocabile su quanto trasferito.

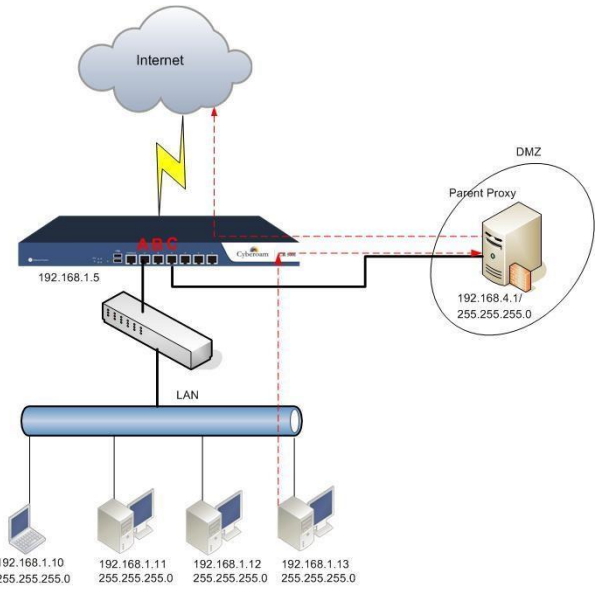
Esistono due tipi di proxy server:

- Application Proxy (Proxy di Applicazione);
- Proxy SOCKS - che "incrociano" le comunicazioni.

Application Proxy

Prendiamo in esame il caso di una persona che effettua un telnet su un altro computer e poi da qui al resto del mondo. Solo attraverso un proxy server di applicazione è possibile automatizzare il processo:

- non appena si fa telnet verso l'esterno il client indirizza al proxy;
- il proxy si connette al server richiesto (il mondo esterno) e restituisce i dati.



Poiché i proxy server gestiscono tutte le comunicazioni, sono anche in grado di registrare qualsiasi parametro si voglia e ciò può includere qualsiasi URL visitata "proxy HTTP (web)" o qualsiasi file si scaricato "proxy FTP".

E' possibile anche filtrare parole "inappropriate" dai siti che si visitano, controllare la presenza di virus ed effettuare l'autenticazione degli utenti prima che questi ultimi effettuino una connessione verso l'esterno. Il server prima della connessione potrebbe richiedere all'utente di effettuare un login. Si potrebbe addirittura arrivare a richiedere un login per ogni sito che desidera visitare.

Proxy SOCKS

Un server SOCKS è molto simile ad una vecchia "switch board", che semplicemente incrocia, attraverso il sistema, i "cavi" della propria connessione con un'altra connessione esterna.

La maggior parte dei server SOCKS funziona solamente con connessioni di tipo TCP e come i firewall filtranti non fornisco l'autenticazione degli utenti. Hanno comunque la possibilità di registrare il sito a cui si è connesso l'utente.

Sistemi anti-intrusione

Il rilevamento delle intrusioni, come suggerisce il nome, è quell'attività volta a scoprire tentativi di intrusione, o di intrusioni già avvenute, nei sistemi di calcolo e di avviare azioni appropriate in risposta agli attacchi.

Per il rilevamento delle intrusioni s'impiegano molte tecniche che si differenziano a seconda del fattore che viene preso in esame per rilevare l'aggressione.

Di seguito alcuni di questi fattori:

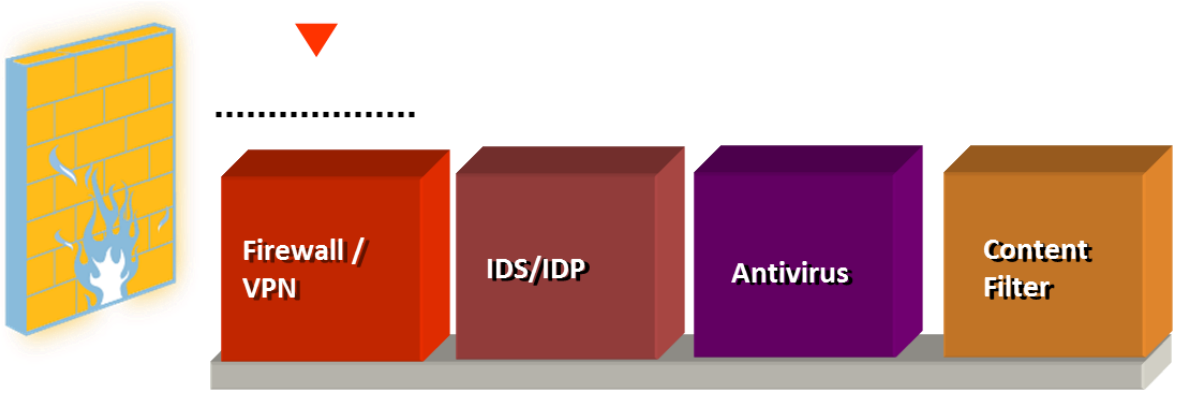
- Fase in cui è avvenuto il rilevamento dell'intrusione: mentre si stava verificando, o solo successivamente;
- Le informazioni esaminate per scoprire l'attività intrusiva.

Queste potrebbero comprendere comandi per l'interprete impartiti dall'utente, chiamate del sistema da parte dei processi, oltre a intestazioni e contenuto dei pacchetti di rete. Alcune forme d'intrusione si possono rivelare solo attraverso una correlazione delle informazioni acquisite da più di una sorgente.

- L'ampiezza della capacità di risposta.

Alcune semplici forme di risposta consistono nell'informare l'amministratore del sistema della potenziale intrusione oppure nel bloccare in qualche modo la potenziale attività intrusiva, ad esempio arrestando un processo impiegato in un'attività apparentemente intrusiva. Questi gradi di libertà nella progettazione di sistemi impieganti tecniche per il rilevamento delle intrusioni hanno portato a un'ampia gamma di soluzioni che vanno sotto il nome di sistemi di rilevamento delle intrusioni (intrusion-detection systems - IDS).

Esistono anche sistemi che opportunamente istruiti possono identificare a priori e quindi prevenire attacchi informatici. Questi sistemi sono detti "intrusion prevention systems – IPS"



Conclusioni

Gli argomenti trattati nelle precedenti lezioni diventano fondamentali per la verifica della sicurezza dei propri servizi pubblicati sul WEB. Il Man in te Middle trattato durante la prima lezione e la sicurezza della posta elettronica trattata nella seconda lezione, si calano perfettamente in questo ambito.

La nostra esperienza ha evidenziato che portali ritenuti sicuri da test di penetrazione o di vulnerabilità, erano invece attaccabili in quanto semplicemente pubblicati mediante protocolli non sicuri attraverso i quali risultava facile acquisire le credenziali degli utenti connessi al sistema. In altre parole sicuro e protetto il server a livello di configurazione, ma esposto a rischi a livello di infrastruttura.

Quanto trattato nella lezione 5 sugli "Scan Ports" è fondamentale per la verifica della sicurezza dei nostri sistemi. Ci è capitato più volte di riscontrare che i router ed i Firewall forniti dai provider sono configurati in modo non propriamente corretto in quanto settati con SNMP abilitato

su rete pubblica e accesso non controllato. Un'autentica autostrada d'accesso per un male intenzionato.

Quindi che fare? Il consiglio che possiamo dare è il seguente:

solo un audit mirato consente di avere una fotografia dettagliata dello stato della nostra architettura di rete e delle sue vulnerabilità.

Lesson 7: Congestione di rete e mappatura

Premessa

Nei capitoli precedenti abbiamo dato ampio risalto ai problemi che possono scaturire a fronte di configurazioni non appropriate di apparati e devices di rete. Questi argomenti sono molto legati alla sicurezza ed alla protezione della rete, problematiche in grado di creare danni all'immagine dell'Azienda. La lezione attuale si concentra sulla disponibilità e produttività della rete aziendale e di come, la riduzione o la mancanza di uno o di entrambi gli elementi, costituisca un grave danno per l'organizzazione .

All'interno di questo documento analizzeremo le modalità di progettazione ed implementazione di una "corretta architettura di rete" in grado di garantire la continuità di servizio. Evidenzieremo nel contempo come la funzione di "monitoring" applicata alla stessa diventi parte fondamentale della sua gestione. Per gestione non si intende solo la sua amministrazione quotidiana, ma anche la "prevenzione attiva" dei problemi ed il rilievo delle performances.

Uno dei problemi maggiormente evidenziato durante gli audit è relativo ad errori di collegamento o configurazione degli apparati di rete che ne possono mettere a repentaglio la stabilità. Grazie a sistemi di controllo, "**come quello proposto in allegato alla lezione"**, abbiamo evidenziato colli di bottiglia tra apparati o tra loro e Key device (server applicativi o sistemi Core). In prima analisi questi errori provocavano un crollo delle prestazioni della rete ma alle volte andavano a variare le operazioni di Back-up alterandone le finestre temporali.

E' di fondamentale importanza mappare gli utenti connessi (Network Assessment) tracciando con precisione la loro connessione in modo da sapere sempre ed esattamente da dove si connettono e verso quale risorsa/applicazione di rete. Tale operazione consente di identificare ed isolare i problemi molto rapidamente ottimizzando così i tempi di intervento e di DOWN della rete o di parte delle sue risorse.

Una volta tracciata la mappatura della rete è fondamentale controllarla continuamente ed eventualmente aggiornarla possibilmente in tempo reale. Questa operazione è appannaggio del sistema di monitoring.

Il sistema di monitor può essere indifferentemente implementato all'interno o all'esterno dell'azienda, fondamentale è il suo settaggio (tuning) attraverso il quale è possibile rendere il sistema **proattivo** profilandolo sulle policy aziendali e sulla propria architettura di rete. A proposito è fondamentale ricordare che le policy di rete così come la sicurezza non sono un prodotto finito, ma un progetto che si trasforma nel tempo. Credere di installare un sistema di monitoraggio una volta per tutte senza aggiornarlo costantemente **significa gettare quattrini tempo ed esporre il proprio sistema informativo a rischi enormi.**

Architettura di rete

Alta affidabilità

Il tema della continuità di servizio è particolarmente sentito nelle reti e soprattutto in quelle Ethernet (IEEE802.3) che rappresentano circa il **99,8%** del totale installato nel mondo. Nonostante questa diffusione uno degli aspetti ancora oggi purtroppo sottovalutato in fase di progettazione è quello relativo alla messa in sicurezza dell'infrastruttura. Per sicurezza si intende la protezione della rete rispetto agli incidenti che possono impattare sulla continuità di servizio. Solo una minima parte (**meno del 4%)** delle reti è progettata per "resistere" in caso di guasti su uno o più componenti che la costituiscono. Da una recente indagine condotta sulle cause di disservizio alla rete locale compaiono, in ordine di frequenza, il guasto all'alimentazione (Power Supply) e l'errore di configurazione (Misconfiguration).

Di seguito riportiamo una lista delle problematiche più comuni che si possono rilevare:

Blocco delle operazioni – Incidenti al Centro stella

- **Mancata alimentazione** - Failure dell'alimentatore Centro stella
- **Mancata alimentazione** – Interruzione nella erogazione dell'energia elettrica (assenza UPS).
- **OverTemp** (temperatura eccessiva) – Guasto alla ventola del Centro stella
- **Errata tensione di alimentazione** – VA difformi dovuti al provider dell'energia elettrica (assenza stabilizzatore).
- **OverTemp** (temperatura eccessiva) – Guasto al condizionamento wiring closet (circuito elettrico).
- **Guasto della switch fabric** del Centro stella.
- **Guasto sul modulo** porte utenti o server.
- **Guasto sulla porta** del downlink verso utenti o server.
- **Interruzione della connessione** dovuta al cablaggio (agenti esterni o operazioni accidentali)
- **Interruzione della connessione** sul Patch Panel o sulla porta switch dovuta al cablaggio (tensione e curve cavi nel rack).
- **Reboot del sistema** – dovuto a Loop di pacchetti o frame (software).
- **Misconfiguration** – dovuto ad errore nella configurazione dello Spanning Tree o del VRRP.

Spesso si verificano incidenti in successione che paiono spesso concatenati tra di loro in una sorta di effetto domino difficile da risolvere in tempi accettabili utili per non impattare negativamente sulla operatività dell'organizzazione.

Facciamo un esempio:

Si guasta il condizionamento del wiring closet e le temperature di esercizio causano un guasto alla fabric (il componente più fragile e sofisticato del centro stella). Potrebbe succedere che, ancora prima della segnalazione di guasto al condizionamento, l'amministratore di rete venga

travolto dalle problematiche relative al blocco del centro stella causato dal crash della Fabbric. Ma cosa sta succedendo nella realtà:

- **L'attenzione dell'amministratore è distolta dal guasto principale** in quanto quello secondario sta provocando il fermo della rete.
- La sostituzione della Fabbric non ha risolto ma è servita solo ad eliminare uno degli effetti del problema principale. **La causa è rimasta**.
- Si manifesta a questo punto il secondo effetto. L'amministratore di rete si accorge dell'aumento della temperatura dovuto al bocco del condizionatore.
- Si provvede al ripristino dell'elettricità in modo che il condizionatore riprenda a funzionare. **Adesso si eliminato il problema principale**.

E se nel frattempo la temperatura non scendesse abbastanza velocemente in modo da scongiurare il guasto della Fabbric appena installata?

Oppure:

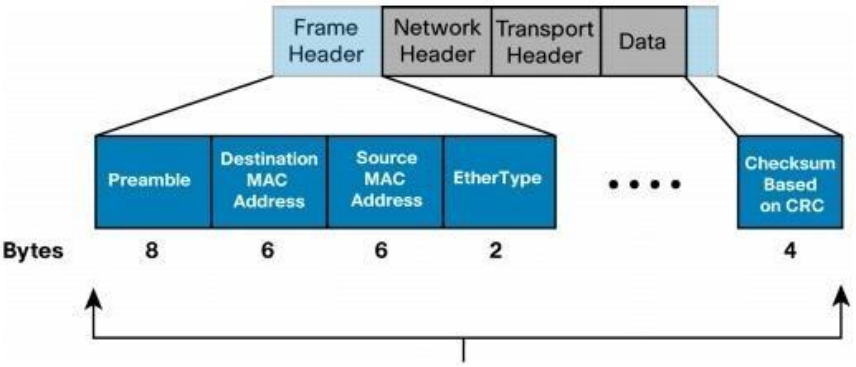
si verifica uno spike sulla rete elettrica (sovratensione) con la conseguenza attivazione delle protezioni del Power supply ed il blocco dell'alimentazione. Alla ripartenza, eseguita in modalità automatica senza prevedere la disinserzione delle utenze e la loro progressiva riattivazione, si verifica un problema sulle ventole e…….

della serie, i guai non si presentano mai soli!!!!!!!!!!!!!

Ma è solo causa della malasorte oppure anche noi abbiamo le nostre responsabilità? Andiamo con ordine.

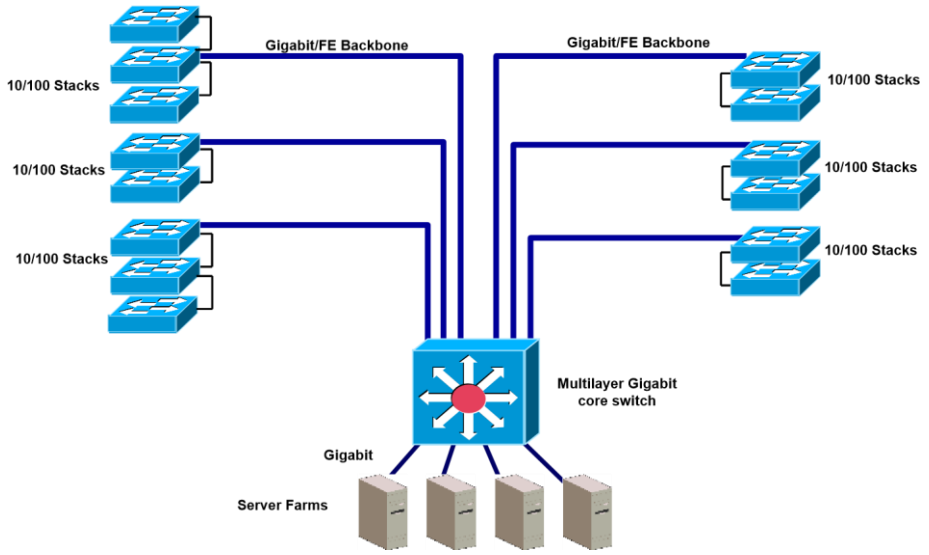
L'infrastruttura tradizionale

La maggior parte delle topologie di rete disegnate dai progettisti risente ancora oggi di nozioni e metodiche apprese negli anni '90, quando il design di rete imponeva delle scelte pressoché obbligate. Il modello dominante per certi versi si ricollega ancora all'epoca in cui la maggior parte delle funzioni di rete venivano espletate da un router o meglio da "one armed router" che svolgeva principalmente le seguenti attività: **esaminare pacchetti di livello 2 e instradarli alle Subnet o alle VLAN di riferimento.**



Peccato che, per tale attività, fosse impiegata una tecnologia che ispezionava il pacchetto alla ricerca non solo della destinazione e del mittente, ma pure del contenuto stesso dell'informazione. Questa procedura veniva ripetuta per ogni frame e su ogni pacchetto nella sessione attiva a detrimento delle velocità di smaltimento delle trame Ethernet che vanno da e verso il centro stella. La logica era appunto quella di **creare una rete intelligente in uno solo dei componenti** (l'elemento al centro della rete) circondandolo da una serie di dispositivi più o meno stupidi. Tale metodologia ha subito poche variazioni anche quando la stupidità della "periferia" si è andata tramutando in una sempre maggiore sofisticazione, al punto di processare direttamente tutte le operazioni inerenti il riconoscimento degli utenti e il tagging (etichettatura) delle applicazioni. In seguito sono stati sostituiti i Router con i ben più agili "Switch Layer 3" (**1997**) che oggi rappresentano la totalità degli apparati posti al centro stella di una rete locale.

Possiamo quindi sintetizzare l' approccio "conservatore" in un disegno come quello sotto riportato, che vede appunto la "periferia stupida" totalmente asservita ad un solo chassis di centro stella che si rende di proposito il più possibile "robusto" attraverso l'adozione di doppia CPU e doppia alimentazione.



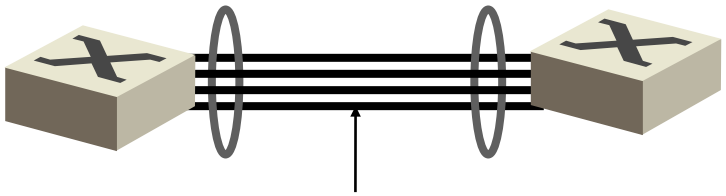
(fig. 1) La progettazione tradizionale

E' evidente nella rete rappresentata in fig.1 la somma dei "vizi" progettuali ereditati dal periodo pionieristico delle reti, allorquando la loro robustezza era decisamente meno importante rispetto all'elemento sperimentale che ne caratterizzava l'implementazione. Vediamo infatti che gli switch periferici sono connessi con una sola scheda in fibra al centro stella. In tal modo si penalizzano le prestazioni e, soprattutto, si determina un pericoloso "vulnus" costituito appunto da quell'unica scheda che è in grado di isolare, nel caso di guasto, tutti i client attestati in periferia. Questo modo di progettare è contro le più elementari regole che sovrintendono una rete con **Mission Criticality superiore al 99,99%.**

Link Aggregation (IEEE 802.3ad)

Altrimenti conosciuto come "trunking", la link aggregation opera a livello 2 del modello Open Systems Interconnection (OSI) ed è in grado di aggregare link multipli Fast Ethernet o Gigabit Ethernet tra diversi dispositivi quali Client, Server e Switch, creando di fatto un unico "trunk" che moltiplica la banda passante disponibile per il numero di porte che vengono così aggregate.

- Combina due o più Fast Ethernet (nell'esempio 4) links con un unico link da 800Mbps tra 2 switch (i link sono da 100Mbps ed essendo full duplex portano la banda supportabile a 200Mbps ciascuno).
- Combina due o più Gigabit Ethernet link tra due apparati attivi.
- È uno standard (IEEE 802.3ad) dal 6 Marzo 2000.



(fig. 2) Link Aggregation – schema

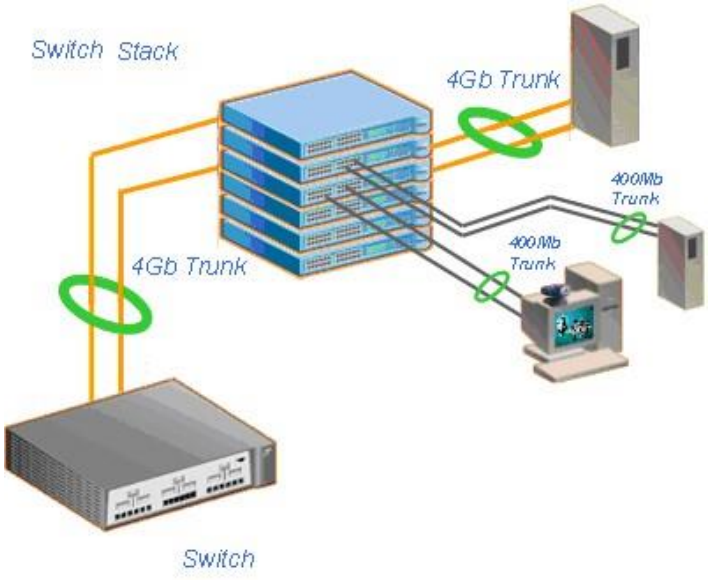
Se uno dei link fisici (cavo) o una delle porte dello switch dovesse guastarsi, il trunk realizzato manterrebbe in vita le connessioni pur riducendo il data rate. In questa modalità la banda tra due switch può essere incrementata aggiungendo un link ulteriore, senza dover sostituire il dispositivo con un più moderno switch dotato di connessioni high speed.

Attenzione però al conto economico, perché con la riduzione dei prezzi relativi alla tecnologia Gigabit, l'esercizio del truncking sta iniziando a mostrare la corda. Il costo incrementale di una connessione nativa Gigabit su 1000BaseT è già inferiore rispetto ad una doppia connessione Fast Ethernet 100BaseT. Il risultato è evidentemente sfavorevole al trunking nel momento in cui si debbano "aggregare" due o più link Fast Ethernet. Con il prezzo di due porte Ethernet (che poi diventano 4 considerando i due lati della connessione) si può acquistare un "Uplink Gigabit" come modulo opzionale, in dotazione ormai a tutti gli Switch di ultima generazione.

Se la Link Aggregation viene vista invece come resilienza, il quadro cambia in quanto rientra in una corretta politica di gestione delle risorse di rete. Nelle soluzioni odierne il Trunking 802.3ad è utilizzato per connettere in modo "sicuro" gli switch periferici verso un server piuttosto che verso il centro stella Layer 3. In quest'ultimo caso è bene rimarcare un'importante prerogativa che hanno alcuni switch rispetto ad altri apparati.

Trunking multistack

Con questo termine si configura un comportamento particolare che consente a una pila di switch collegati tra loro di poter comunicare in modo contemporaneo attraverso due o più "calate"(connessioni) verso il centro stella.

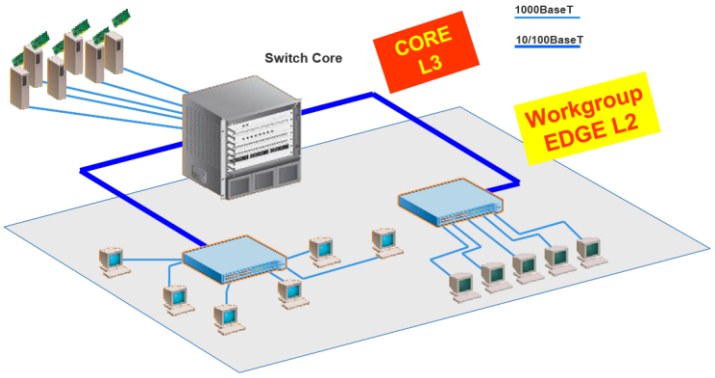


(fig. 3) LACP 802.3ad – le capacità degli switch intelligenti

Nell'esempio in Fig. 3 vediamo che la "pila" o stack che dir si voglia, costituita da 5 switch è in grado di gestire un totale di otto connessioni verso dispositivi esterni alla "pila" attraverso la metodologia **802.3ad.** Con questa modalità si assicura un doppio link verso lo switch di centro stella ed un doppio link verso il server dotato di due schede Gigabit "Dual Homing" (in grado cioè di bilanciare il carico sulle due diverse interfacce).

La progettazione Core Chassis tradizionale

La rete rappresentata in fig. 4 ha un numero elevato di "single point of failure". Generalmente il progettista di tale soluzione si limita a rinforzare il centro stella con un doppio Power Supply ed una Fabric supplementare (molto costosa). In pratica si realizza un raddoppio di CPU, che subentra nel caso in cui la fabric principale dovesse guastarsi. Con questa configurazione si pagano due engine (fabric) molto costose e si finisce per usarne una sola che è quella in produzione. L'altra engine, infatti, rimane in stand by, ed entra in azione solo a fronte in di un evento infausto che causa la disattivazione della principale. In pratica funzionano solo una alla volta. Le workstation hanno una singola scheda di rete connessa ad un unico switch di Layer 2. Anche lo switch ha un'unica connessione verso "**l'unico**" centro stella 3.



(fig. 4) Progettazione ONE Core CHASSIS – l'approccio tradizionale

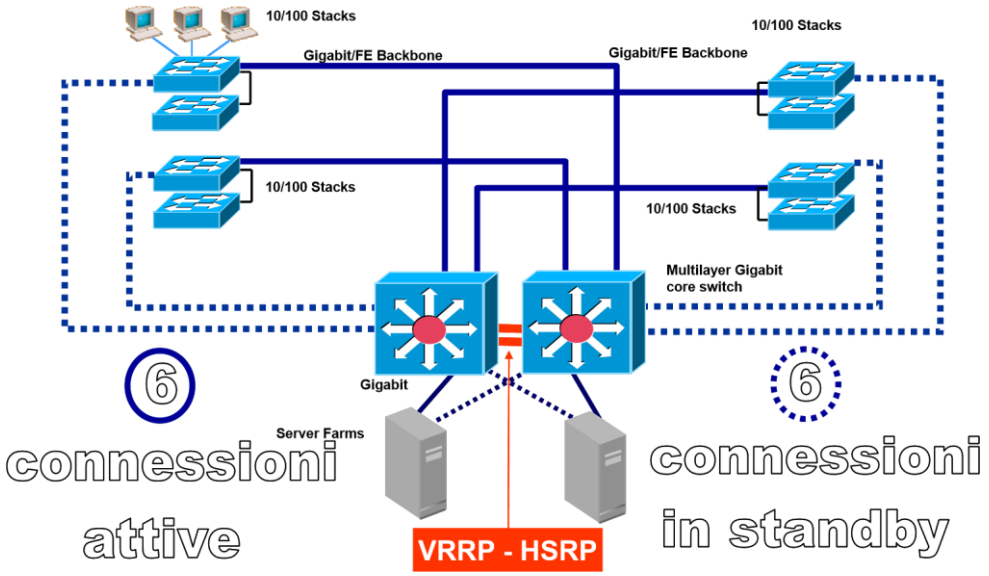
Questa rete non garantisce la continuità operativa delle 12 condizioni sotto riportate che definiscono la Mission Criticality di una rete distribuita di classe enterprise. Le condizioni che è in grado di sopportare a livello di eventi negativi sono solo le due evidenziate in grassetto, la numero 9 e la numero 10:

1. Rottura di una scheda di rete nella WST.
2. Interruzione della connessione tra WST e Switch di Periferia (Workgroup L4).
3. Guato di una porta nello switch di periferia.
4. Rottura di uno switch di periferia.
5. Guasto dell'interfaccia di collegamento tra periferia e centro stella.
6. Interruzione di un link fisico tra periferia e centro stella.
7. Guasto di una porta/modulo del centro stella su cui è attestato il link alla periferia.
8. Rottura di uno switch di centro stella.
9. **Guasto della scheda principale (Fabric) del Centro stella.**
10. **Guasto di un Power Supply del Centro stella.**
11. Interruzione di un link tra centro stella e Server.
12. Rottura di una scheda server.

Due condizioni su 12 sono davvero troppo poche per potersi proporre con efficacia in una logica di Mission Critical, e sono da considerarsi a tutti gli effetti totalmente inadeguate alle odierne richieste di continuità operativa.

La progettazione DUAL Core Chassis tradizionale

La rete rappresentata in fig. 5 abbassa il numero di single point of failure, in quanto raddoppia i "CORE SWITCH modulari", evitando peraltro l'inserzione di un doppio Power Supply e di una Fabric supplementare su ognuno degli switch di centro stella.



(fig.5) Progettazione DUAL Core CHASSIS – l'approccio tradizionale

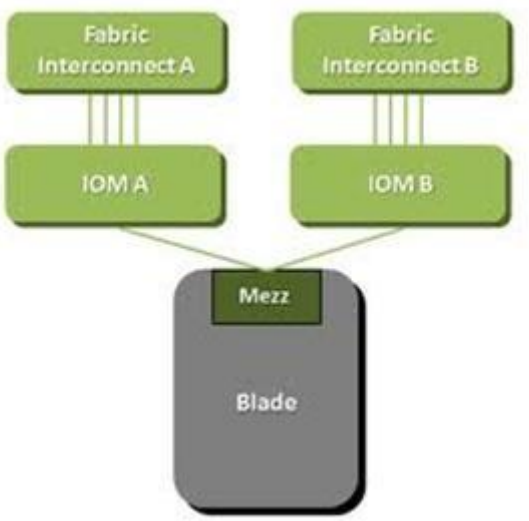
Le linee tratteggiate danno l'idea di come questa topologia funzioni. Di solito, per evitare complicazioni nella configurazione, si mettono in stand by le connessioni tratteggiate in modo tale da non usarle effettivamente (tali connessioni tutti gli effetti in grado di spostare pacchetti esattamente come le connessioni "piene"). Questa condizione impiega i protocolli VRRP o HSRP per attivare la "ridondanza" tra i Core switch.

La rete con due chassis ha un minore numero di single point of failure e continua a funzionare anche quando le condizioni enumerate qui di seguito si realizzano:

1. rottura di una scheda di rete nella WST.
2. Interruzione della connessione tra WST e Switch di Periferia (Workgroup L4).
3. Guasto di una porta nello switch di periferia.
4. Rottura di uno switch di periferia.
5. Guasto dell'interfaccia di collegamento tra periferia e centro stella.
6. Interruzione di un link fisico tra periferia e centro stella.
7. Guasto di una porta/modulo del centro stella su cui è attestato il link alla periferia.
8. Rottura di uno switch di centro stella.
9. Guasto della scheda principale (Fabric) del Centro stella.
10. Interruzione della connessione VRRP.
11. Guasto di un Power Supply.
12. Interruzione di un link tra centro stella e Server.
13. Rottura di una scheda server.

Oltre a questo approccio ne esiste uno ulteriore che prevede doppio Chassis e che inserisce doppia CPU , Doppio Power Supply e doppio FAN su ognuno degli Chassis. Decisamente

antieconomico e statisticamente poco probabile quest'ultimo approccio è destinato soltanto a chi non ha problemi di Budget.



Software di gestione SNMP

Switch Center

Switch Center è una suite completa di gestione che aiuta a scoprire, monitorare e analizzare la connettività di rete e le prestazioni. Rappresenta una valida soluzione per la manutenzione della rete stessa. Tutte le sue funzionalità operano in tempo reale.

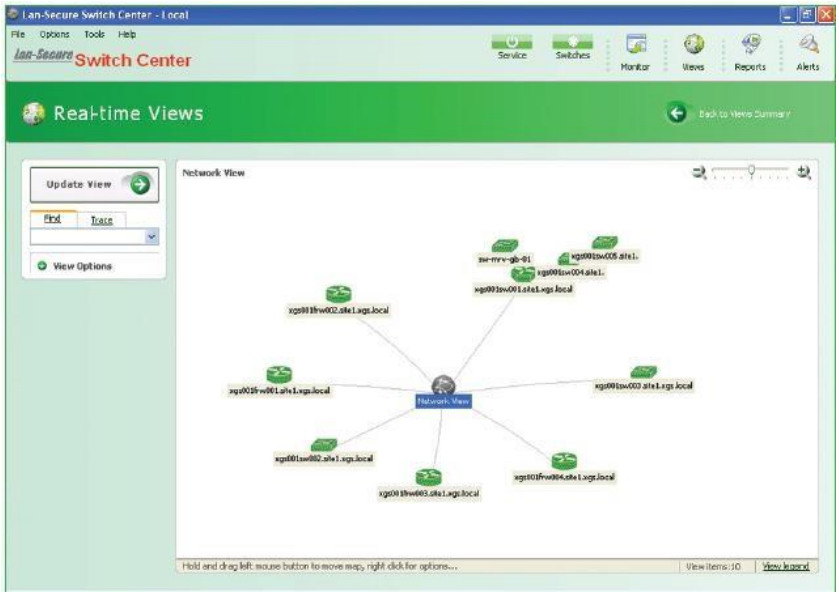
Il software mappa l'esatta ubicazione dei nodi di rete e la loro attività. Analizza il traffico in percentuali di utilizzo, di pacchetti broadcast e di eventuali errori tenendo aggiornato l'utente sui potenziali malfunzionamenti della rete.

In automatico viene effettuato il "discovery" degli apparati di rete dotati di agent SNMP (vedi importanza nella lezione inerente gli apparati attivi di rete). Presenta in modalità grafica interattiva la mappatura e le connessioni della rete. Evidenzia la tipologia delle connessioni , in modo da poter individuare con un semplice colpo d'occhio incongruenze di connessione.

Cliccando sui singoli devices mostra il dettaglio relativo all'utente selezionato evidenziando la tipologia di connessione la sua ubicazione ed i dati relativi quali Mac Address, IP Address etc..

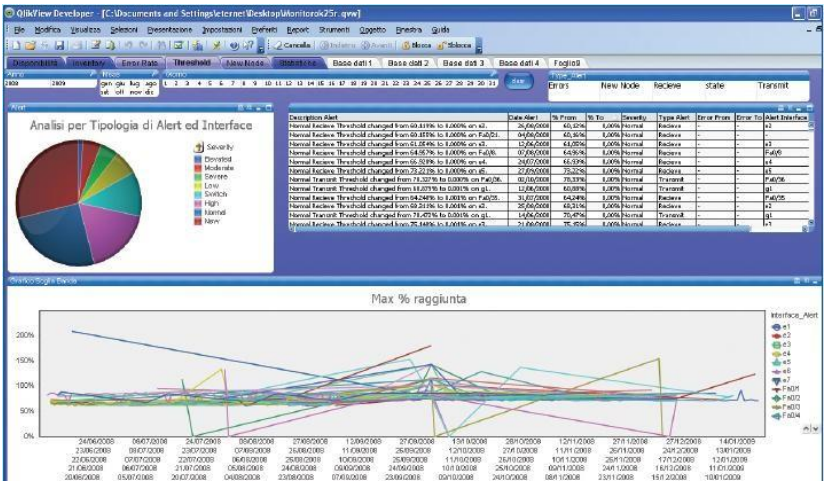
Nel caso di Monitor su di un device non SNMP viene evidenziata l'intera nuvola delle connessioni presenti sulla singola porta dello switch. Il non utilizzo dell' SNMP è fortemente sconsigliato in quanto rappresenta una connessione non gestibile.

Se settato appositamente il sistema avvisa ad ogni nuova connessione di un nuovo device fornendone immediatamente l'identità e l'ubicazione. L'amministratore di rete troverà questa funzione estremamente utile in quanto lo porrà nella condizione di controllare in tempo reale se la nuova connessione rappresenta un pericolo per la sua struttura o una nuova connessione/utente da registrare. In questo secondo caso verrà automaticamente modificata la mappatura della rete



E' possibile esportare la mappa in Visio mediante appositi tools in modo tale da poter disporre sempre e velocemente l'esatta istantanea della propria rete.

E' possibile fare attente analisi e statistiche con sistemi di business intelligence in grado di interfacciarsi con il sistema. Tutti i dati raccolti possono essere salvati su DB Access o SQL, in modo da poterli riutilizzare per effettuare analisi o una reportistica puntuale e aggiornata. E' anche possibile verificare le performances della propria rete a livello grafico identificando così immediatamente eventuali problemi o colli di bottiglia.



Conclusioni

Durante le fasi di Audit questi strumenti vengono utilizzati per fare una fotografia della rete a livello di architettura, per rilevare tutti gli apparati di rete SNMP e verificarne lo stato.

Grazie al software impiegato è possibile fornire all'amministratore di rete la mappatura di quali siano i device connessi e dove siano ubicati. Qualora ci fossero problemi di broadcast, multicast o unicast che rallentano le performance della rete sarebbero immediatamente evidenziati. Anche la presenza di eventuali errori quali allineamento, CRC etc. verrebbero evidenziati con l'indicazione del device incriminato. Infine per alcune problematiche quali i colli di bottiglia verranno forniti suggerimenti per eliminarli.

Come risulta evidente da quanto sopra esposto l'importanza dell'utilizzo di un software di monitoring e di gestione è fondamentale per tenere sotto controllo il nostro patrimonio informatico.

Ed è proprio per questa ragione che alleghiamo alla presente lezione un Link attraverso il quale è possibile scaricare un'applicazione che una volta installata permetterà all'amministratore della rete di toccare con mano l'importanza del Monitoring e di verificare che:

Lavorare senza informazioni, o peggio ancora con quelle sbagliate, **è come operare al buio**.

Lavorare invece con le informazioni giuste e aggiornate in tempo reale……..

E' tutta un'altra cosa!!!

Lesson 8: Compliance Normativa e Privacy

Premessa

L'art. 45 del decreto legge sulle semplificazioni, approvato dal Consiglio dei Ministri, abroga tutte le previsioni contenute nel Codice della privacy e nel Disciplinare tecnico sulle misure di sicurezza che si riferiscono al Documento Programmatico sulla Sicurezza (**DPS**) per il trattamento dei dati personali.

In particolare il decreto interviene all'art. 34, lett. g, comma 1 e comma 1 bis, del D.Lgs 196/2003 (Codice della Privacy) e al suo Allegato B, paragrafi da 19 a 19.8 e 26 (Disciplinare Tecnico in materia di misure minime di sicurezza), **cancellando le norme relative all'obbligo di redazione e aggiornamento del DPS** (sia in forma ordinaria che abbreviata).

Eliminato il DPS, unitamente alle modalità semplificate per la tenuta del DPS, vengono meno anche i relativi riferimenti da riportare all'interno delle relazioni accompagnatorie del bilancio sull'avvenuta redazione o aggiornamento.

Il DPS è un documento che rappresenta la politica adottata del soggetto obbligato per quanto riguarda la privacy.

In altri termini, il documento fotografa la "privacy policy" e sulla base di un'attenta analisi dei rischi procede a definire e programmare le misure necessarie per migliorare la sicurezza del trattamento dei dati personali.

Il DPS doveva essere redatto o aggiornato entro il 31 marzo di ogni anno.

Il soggetto obbligato alla redazione del DPS è il titolare del trattamento dei dati sensibili o giudiziari mediante l'utilizzo di strumenti elettronici, anche attraverso il responsabile, se designato. Il DPS non va inviato al Garante della privacy, ma deve essere conservato presso la propria struttura ed esibito in caso di controllo.

È da sottolineare che il DPS è solo una delle misure minime di sicurezza, **le altre misure previste dal D. Lgs. 196/2003 non vengono abrogate**. Tali misure comportano sanzioni sia di carattere amministrativo che penale e in particolare:

- **Redazione idonee informative** (Art. 13 DLgs 196/2003): □ Informativa dipendenti e Collaboratori;
  - informativa clienti, fornitori, potenziali clienti, terzi;
  - informativa utenti sito web; □ informativa candidati all'assunzione; □ privacy policy sito web.
- **Nomina incaricati al trattamento dati personali** (Art. 30 DLgs 196/2003):
  - redazione documento che individua l'ambito di trattamento dati personali consentito a ciascuna unità organizzativa;
  - redazione lettere d'incarico per ciascun incaricato al trattamento dati personali.
- **Nomina Responsabili al trattamento dati personali e analisi trattamenti affidati in outsourcing** (Art. 29 DLgs 196/2003):

- redazione lettera di nomina per ciascun Responsabile al trattamento dati personali;
- analisi dei casi specifici di affidamento dati personali all'esterno dell'Azienda;
- analisi dei flussi di dati intra ed extra Unione Europea;
- individuazione dell'idoneo rapporto da formalizzare con i soggetti esterni ai quali viene affidato il trattamento dati personali.

- **Disciplinare interno uso internet e posta elettronica** (Art 154 comma 1 lett. C DLgs 196/2003, Provvedimento Garante 1° Marzo 2007):
  - redazione disciplinare interno obbligatorio relativo all'uso di Internet e della posta elettronica.
- **Nuove prescrizioni in tema di Amministratori di sistema** (Art 154 comma 1 lett. c) e h) DLgs 196/2003, Provvedimento Garante 27 Novembre 2008):
  - adempimenti procedurali e redazione documentazione richiesta dal Provvedimento Generale 27 novembre 2008 – Garante privacy.
- **Nuove prescrizioni in materia di videosorveglianza** (Art. 154 comma 1, lett. C DLgs 196/2003, provvedimento garante 8 Aprile 2010):
- **Gestione privacy policy sito web, newsletter e servizi interattivi**:
  - procedure di gestione dati personali utenti sito web; procedure di attivazione e gestione servizio Newsletter;
  - procedure di attivazione e accesso aree riservate.
- **Formazione del Personale**.
- **Controllo utilizzo della rete e legge contro i crimini informatici** (L.231).
- **Gestione e procedure smaltimento o riutilizzo sistemi di rete dismessi o riassegnati** (computer, server etc…).

Con periodicità annuale, il titolare del trattamento **deve aggiornare** il "sistema privacy" in considerazione delle possibili modifiche normative avvenute nel corso dell'anno e **verificare** la rispondenza delle misure adottate riguardanti il trattamento dei dati personali **aggiornando** i documenti e i mansionari adottati.

I titolari devono continuare a mantenersi vigili e organizzati al fine di avere sotto stretto controllo l'effettivo adeguamento della struttura aziendale alla normativa vigente. In quest'ottica l'eliminazione del DPS crea un vuoto nel sistema di sicurezza per il trattamento dei dati posto in essere dall'impresa titolare dello stesso e rende molto più difficoltoso per quest'ultimo dimostrare ciò che è stato fatto in azienda. Stessa cosa per i controlli degli organi di vigilanza che saranno molto meno agevoli in quanto non ci sarà più il documento di riferimento (DPS) attraverso il quale avveniva la verifica della rispondenza alle norme, con particolare riferimento a quanto riguarda l'implementazione delle misure di sicurezza in caso di trattamento dei dati mediante strumenti elettronici.

D'ora in poi, mancando il DPS, gli organi preposti ai controlli (Guardia di Finanza o ispettori dell'Autorità Garante) non potranno più verificare la realtà tramite un documento, ma saranno costretti a fare indagini approfondite per poter accertare l'effettivo rispetto di tutte le misure indicate nel D.Lgs. 196/03, con l'ovvia conseguenza che per l'azienda "verificata" aumenteranno, e di molto, le probabilità che vengano accertate irregolarità e quindi applicate sanzioni.

Durante le lezioni precedenti abbiamo evidenziato come alcuni problemi rilevati possono cagionare danni irreparabili alle organizzazioni aziendali. L'utilizzo di strumenti non idonei possono diventare motivo di denuncia da parte di dipendenti o collaboratori insoddisfatti. Senza il DPS diventa più difficile controllare lo stato di sicurezza raggiunto dal proprio network, ragion per cui un **Audit** che contempli anche i processi aziendali ci può venire in aiuto.

La Normativa Privacy

Le responsabilità

L'art. 15 del D.Lgs. 196/03 stabilisce che "**chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile**". e l'art. 2050 c.c. precisa che "**chiunque cagiona danno ad altri nello svolgimento di una attività pericolosa** [NdR, quale il trattamento dei dati ex art. 15 D.Lgs. 196/03], **per sua natura o per la natura dei mezzi operati, è tenuto al risarcimento, se non prova di aver adottato tutte le misure idonee a evitare il danno**".

Bisogna tenere ben presente che la redazione e l'aggiornamento annuale del DPS sono sempre stati sia un obbligo di legge ma soprattutto lo strumento per il titolare del trattamento, in caso di danni conseguenti al trattamento stesso dei dati, per fornire agevolmente la prova di aver adottato tutte le misure minime e idonee (ex D.Lgs. 196/03) per evitare il danno e pertanto lo strumento per non incorrere nella condanna al risarcimento del danno ai sensi del combinato disposto dell'art. 15 del D.Lgs. 196/03 e dell'art. 2050 c.c.

In altre parole: l'aver abrogato il DPS espone immediatamente i titolari che decidono di non redigere nessun documento, o rinnovare il DPS esistente alla mancanza del miglior strumento aziendale di autoverifica per capire la rispondenza o meno con le prescrizioni della legge in materia di privacy aumentando di fatto il rischio di minor tutela per le persone fisiche (unici soggetti degni di tale tutela per la normativa vigente).
Ma non finisce qui. Infatti la mancanza del DPS espone anche le aziende titolari dei trattamenti ad un rischio in più in quanto si vedono aumentare le possibilità di irregolarità con la normativa vigente che riguarda l'implementazione delle misure tecniche ed organizzative **tuttora obbligatorie** (misure di sicurezza minime e idonee, normativa in materia di amministratori di sistema, obbligo di informativa e raccolta del consenso per il trattamento di dati relativi a persone fisiche) e quindi ……**di subire le relative sanzioni**.
A tale rischio va aggiunta anche la difficoltà oggettiva di non poter fornire la prova. In caso di controlli, ovvero di contenzioso relativo alla richiesta di risarcimento danni legata al trattamento dei dati o a quello di aver adottato tutte le misure minime ed idonee di cui al D.Lgs. 196/03 e all'art. 2050 c.c., non sarà possibile esibire il DPS come prova a Vostro discarico.

Nelle precedenti lezioni abbiamo visto che alcuni strumenti forniti ai dipendenti non sono compliance e cioè con i requisiti minimi di sicurezza, ad esempio protocolli in chiaro implementati nel servizio della posta elettronica. Per questo motivo un dipendente, le cui informazioni viaggiano in chiaro, non può essere responsabile delle informazioni se acquisite da terzi. Ma c'è di più, lo stesso dipendente potrebbe denunciare l'azienda per violazione della privacy.

Le modifiche

Gli interventi modificativi della disciplina in tema di Trattamento dei Dati Personali erano già iniziati con il cosiddetto "Decreto Sviluppo" del Governo Berlusconi (D.L. n. 70/2011) infatti:

- con il provvedimento summenzionato del maggio 2011 era stato abrogato il comma 3bis dell'art. 5 del D. Lgs. n. 196/03, escludendo così dall'applicazione del codice della privacy il trattamento dei dati personali relativi a persone giuridiche, imprese, enti o associazioni, ma solo qualora lo stesso fosse effettuato nell'ambito di rapporti intercorrenti esclusivamente tra i medesimi soggetti per le finalità amministrativocontabili;
- il decreto legge n. 138 del 13.08.2011, recante "Ulteriori riduzioni e semplificazioni degli adempimenti burocratici", aveva dato la facoltà di sostituire il DPS con "**un'autocertificazione** " per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti (d.lgs. 196/03, art. 34, co. 1-bis).

Il governo Monti aveva poi proseguito con l'art. 40 del D.L. 6 dicembre 2011 n. 201, contenente le disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici, determinando una piccola "grande rivoluzione" nella disciplina della privacy nel nostro Paese, escludendo dall'applicazione di detta normativa tutti i trattamenti di dati di persone giuridiche, enti e associazioni, pubblici e privati. In pratica, dal dicembre scorso si possono trattare tali dati senza più l'onere di fornire a tali categorie di interessati l'informativa preventiva e senza più dover chiedere il consenso di tali soggetti, nemmeno in caso di trasferimento di dati all'estero.

L'Europa

La normativa in materia di trattamento dei dati personali è in fase di revisione non solo in Italia ma anche negli altri paesi dell'Unione Europea, essendo ormai imminente l'emanazione di un regolamento comunitario che andrà a sostituire la normativa europea di riferimento (la direttiva 95/46 CE del 1995), peraltro con applicazione diretta negli stati membri. Questo regolamento comunitario è molto importante, perché oltre a uniformare le regole a livello europeo, potrebbe introdurre significative novità quali ad esempio:

- introduzione del principio dell'applicazione del diritto UE anche ai trattamenti di dati personali non svolti nell'UE, se relativi all'offerta di beni o servizi a cittadini UE o tali da consentire il monitoraggio dei comportamenti di cittadini UE;
- introduzione del diritto degli interessati alla "portabilità" del dato oltre che del "diritto all'oblio", fatte salve specifiche esigenze (ad es. per rispettare obblighi di legge, per garantire l'esercizio della libertà di espressione, per consentire la ricerca storica);

- cancellazione dell'obbligo per i titolari di notificare i trattamenti di dati personali, obbligo sostituito da quello di nominare un "data protection officer" (incaricato della protezione dei dati) per tutti i soggetti pubblici e privati al di sopra di un certo numero di dipendenti;
- introduzione del requisito del "privacy impact assessment" (valutazione dell'impattoprivacy) oltre che del principio generale detto "privacy by design" (cioè previsione di misure di protezione dei dati già al momento della progettazione di un prodotto o di un software);
- introduzione dell'obbligo per tutti i titolari di notificare sempre all'autorità competente le violazioni dei dati personali ("personal data breaches") in tempi determinati e molto ristretti (si parla di 48 ore);
- introduzione di poteri più specifici, anche sanzionatori, di requisiti di indipendenza delle autorità nazionali di controllo il cui parere sarà indispensabile qualora si intendano adottare strumenti normativi, comprese leggi, che impattino sulla protezione dei dati personali;
- introduzione dell'obbligo di adozione per le imprese e per gli enti di un vero modello organizzativo per la tutela dei dati, introducendo il principio di responsabilità (accountability), per cui nel caso di controlli saranno loro a dover dimostrare la conformità del proprio operato alle regole comunitarie;

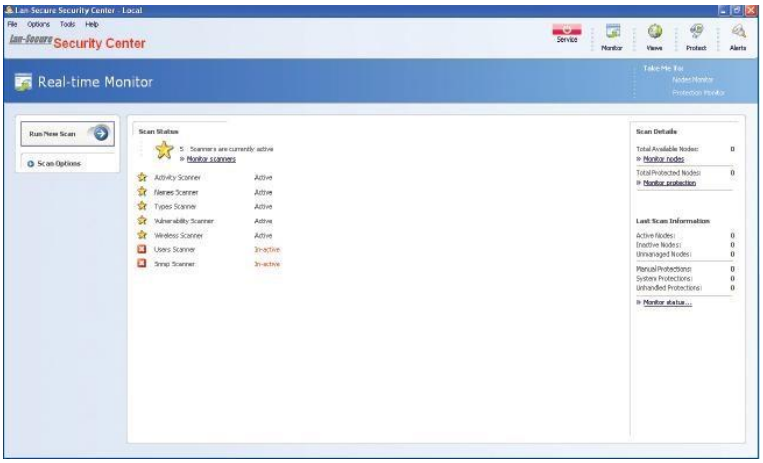
- introduzione di un impianto sanzionatorio di fonte comunitaria, a garanzia dell'efficacia di quanto prescritto, con sanzioni massime previste molto elevate e parametrate al fatturato dell'impresa sanzionata.

Alla luce di quanto sopra, forse gli interventi di "semplificazione" in materia di trattamento di dati personali del Governo Italiano dell'ultimo anno non vanno esattamente nella medesima direzione delle ormai prossime modifiche normative a livello comunitario, modifiche che parrebbero determinare l'introduzione, a breve, di maggiori e più stringenti obblighi in capo ai titolari dei trattamenti.
Si dovrà tuttavia attendere la conversione del D.L. 5/2012 nonché l'approvazione del testo definitivo del nuovo Regolamento UE per avere finalmente una visione complessiva della "nuova" normativa in materia.

Software di gestione e controllo accessi

Security Center

Come evidenziato nelle lezioni precedenti La maggior parte delle minacce si verificano all'interno dell'organizzazione stessa per cui è indispensabile controllare chi si collega alla rete per prevenire quanto previsto dalla 231 contro i crimini informatici.
Security Center è un software per la sicurezza della rete che lavora in "Real Time" in tempo reale. Rileva intrusioni (funzione di IDS e IPS) ed effettua prevenzione proteggendo le rete da potenziali connessioni non autorizzate.



Vediamo insieme cosa è possibile fare:

- bloccare ogni nuovo tentativo di connessione di devices per indirizzo IP, indirizzo MAC o nome macchina, confinandolo in area riservata inviando contestualmente un "alert" all'amministratore di rete;
- settare policy di controllo utente per l'utilizzo dei dispositivi non consentiti. Per esempio l'utilizzo dei sistemi di memoria esterni su porte USB;
- controllare se programmi vitali sono in esecuzione sui client (antivirus e firewall ad esempio);
- confinare una macchina che presenta problemi di elevati broadcast.

Nelle organizzazioni dove chiunque si connette e riceve un indirizzo da server DHCP "Security Center" diventa uno strumento indispensabile per evitare che persone esterne all'organizzazione possano connettersi alla rete arrecando danni.

Conclusioni

Dopo quanto considerato rimane il ragionevole dubbio che il DPS sia stato per anni l'incubo di tante aziende e organizzazioni italiane a tal punto da provare a cassarlo a colpi di decreto.

La bozza infatti indica l'abolizione della lettera h) comma 1 art. 43. Già… ma dell'allegato B non se ne parla. **Quindi?**

Lecito pensare che in caso di dati sensibili permanga comunque l'obbligo.

Ma se viene soppresso il concetto di DPS richiamato anche nelle semplificazioni emanate dal Garante insieme all'autocertificazione e quindi all'impianto della semplificazione stessa……,
come si considera di dover gestire i dati sensibili dei dipendenti?

Rimettendo in carreggiata il DPS??????

Non è dato sapere.

Ma non è tanto questo il problema.

Qui si sta parlando di sopprimere l'unico strumento di auto-analisi inerente la sicurezza informatica aziendale. Lo stesso strumento che, seppur tanto odiato, ha consentito ad aziende

anche di un certo livello, di mantenere nel tempo la propria sicurezza informatica stimolando investimenti che i titolari aziendali, spesso ignari del fatto che l'IT è il fulcro della vita aziendale, hanno accettato solo grazie al pungolo normativo.

Un DPS che, spina nel fianco dei responsabili, ha comunque costretto alla razionalizzazione dei criteri di assegnazione di credenziali piuttosto che alla ristabilizzazione degli idonei livelli di autenticazione secondo il ruolo aziendale, impedendo accessi non dovuti e circolazione di informazioni aziendali non opportune.

Tutti valori scontati oggi, ma assolutamente sottovalutati prima del 2004.

Il DPS è stato bollato da molti come "quel documento terribile e dispersivo", ma in realtà, se ben fatto, ha consentito negli anni di programmare investimenti informatici e far crescere nella mentalità aziende e professionisti. Ora lo si toglie o, per lo meno, lo si riduce solo ai casi di dati sensibili (resterebbe vigente infatti l'Allegato B).

Pienamente d'accordo sulle realtà minime (artigiani, aziende di produzione), ma su soggetti che fanno una ampia gestione anche solo di dati contabili!!! Un'azienda con un milione di dati su persone giuridiche non deve fare il DPS???.

I commenti nella bozza del testo sono:

- ci dobbiamo uniformare alla normativa europea.
- Ok.
- Ma la mentalità italiana in merito al dato trattato, non è quella europea.
- L'italiano parla in ambito aziendale del "suo pc", non del "pc aziendale". Dei "suoi clienti" non dei "clienti della mia azienda".
- La nostra mentalità non è quella europea, **per lo meno non ancora**.

Ci sono aziende dove l'obbligo del DPS ha costretto alla mappatura di server, di trattamenti, di soggetti autorizzati ad accedere ai dati e ai relativi livelli di visualizzazione.

Noi suggeriamo di utilizzare l'**Audit** in ambito di **Network Assessment** quale sostituto del **DPS** redigendo un documento di programmazione e autoanalisi, atto a far rilevare vulnerabilità e a programmare miglioramenti.

Nel frattempo prova a scaricare il trial di "Security Center" e a vedere quanto e come ti può aiutare nella pianificazione del tuo lavoro e nella prevenzione relativa alla sicurezza della tua rete.

Il Tuo
EterNet Team