

# Le principali tipologie di attacco ai sistemi aziendali e personali

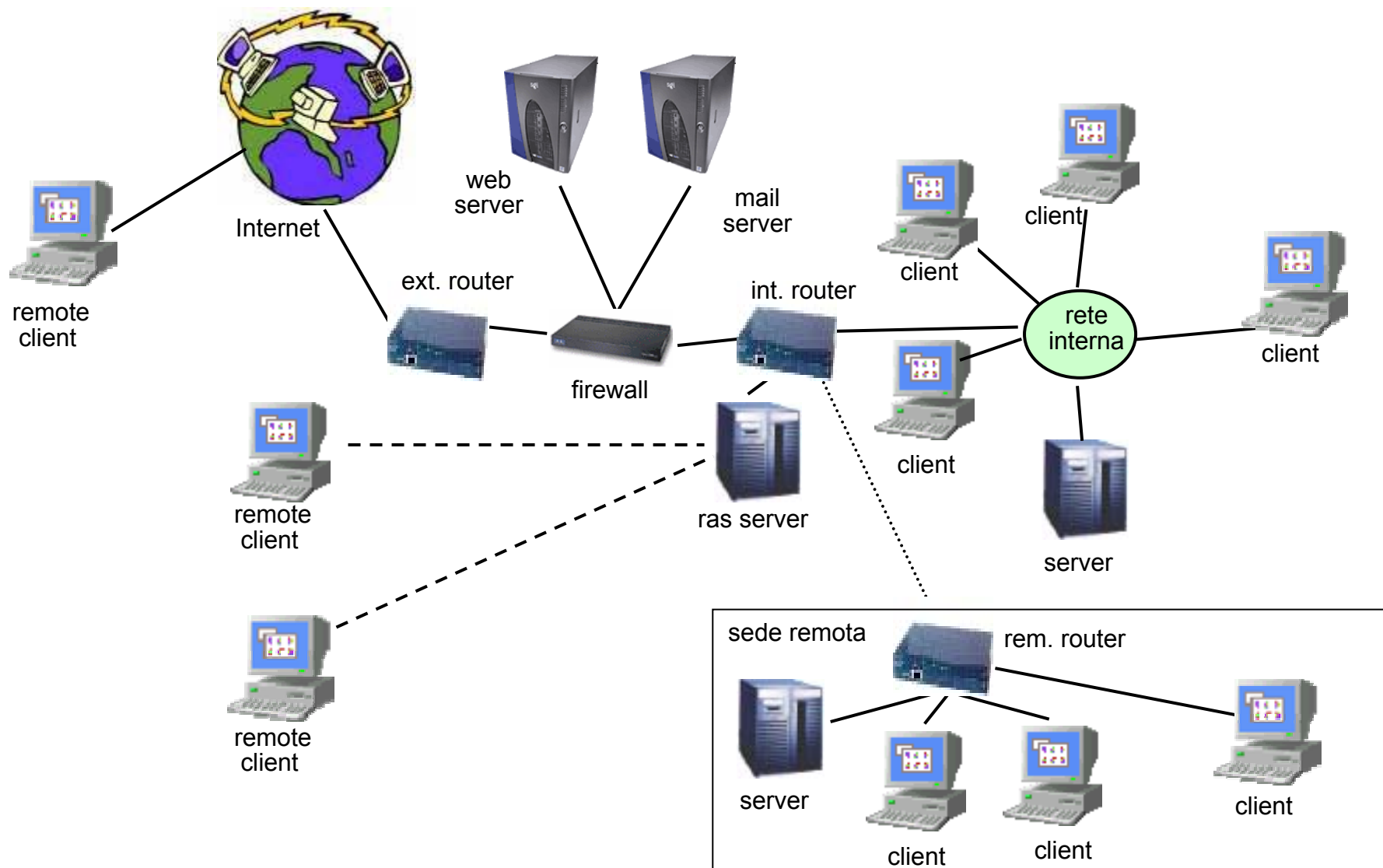


<http://www.infosec.it>

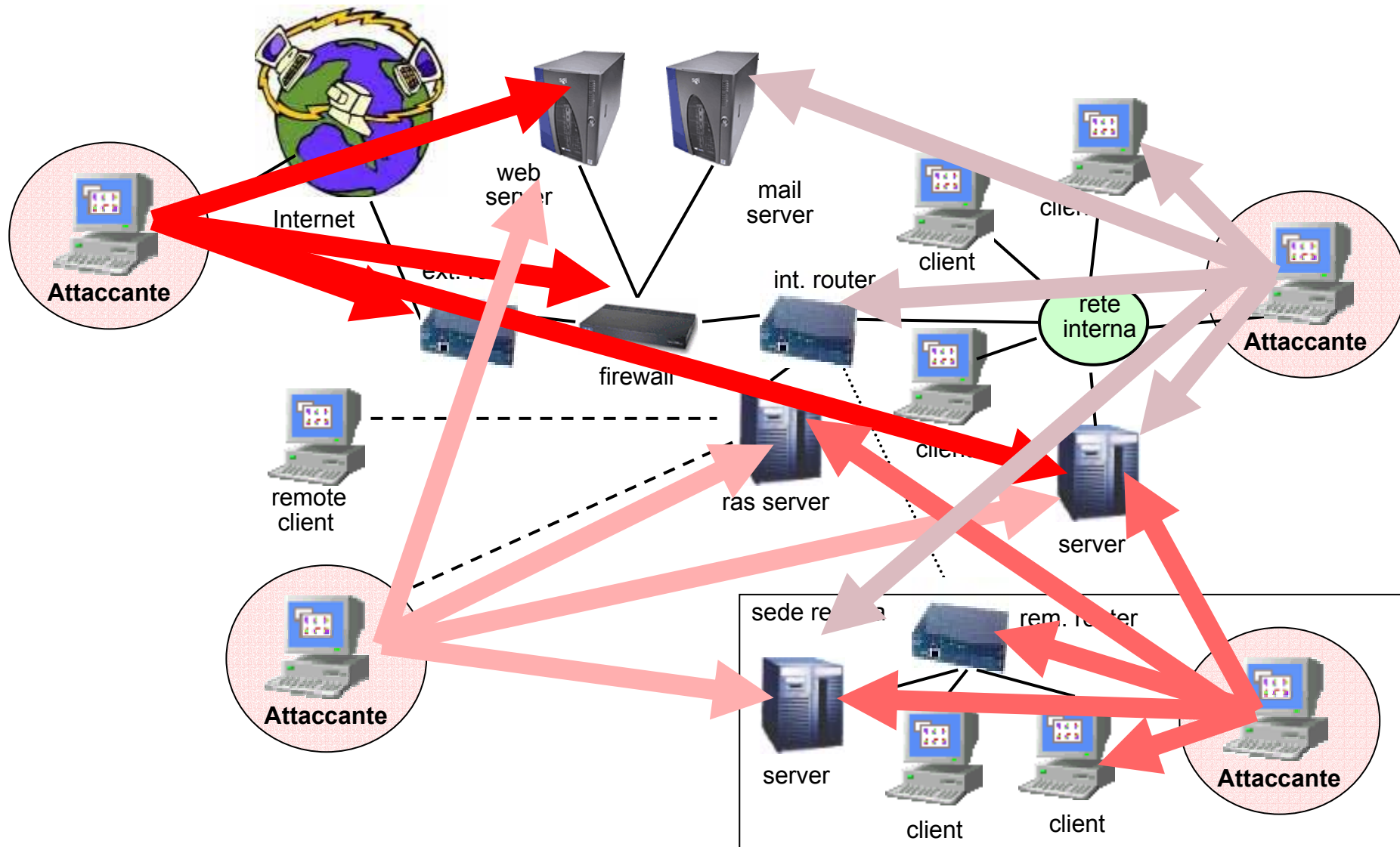
[info@infosec.it](mailto:info@infosec.it)

**Relatore : Stefano Venturoli – General Manager Infosec**

# Questa rete funziona...



# ...ma è sicura?



# Chi sono gli attaccanti?

## Finalità di un attacco

- ❑ rubare informazioni
- ❑ provocare danni e/o disservizi (Denial of Service)
- ❑ utilizzare risorse e/o servizi altrui per i propri scopi

## Chi sono gli attaccanti?

- ❑ chiunque abbia le capacità o le occasioni per accedere ad informazioni e risorse altrui

### **La definizione comune di "hacker" è spesso errata.**

Un hacker può essere chiunque:

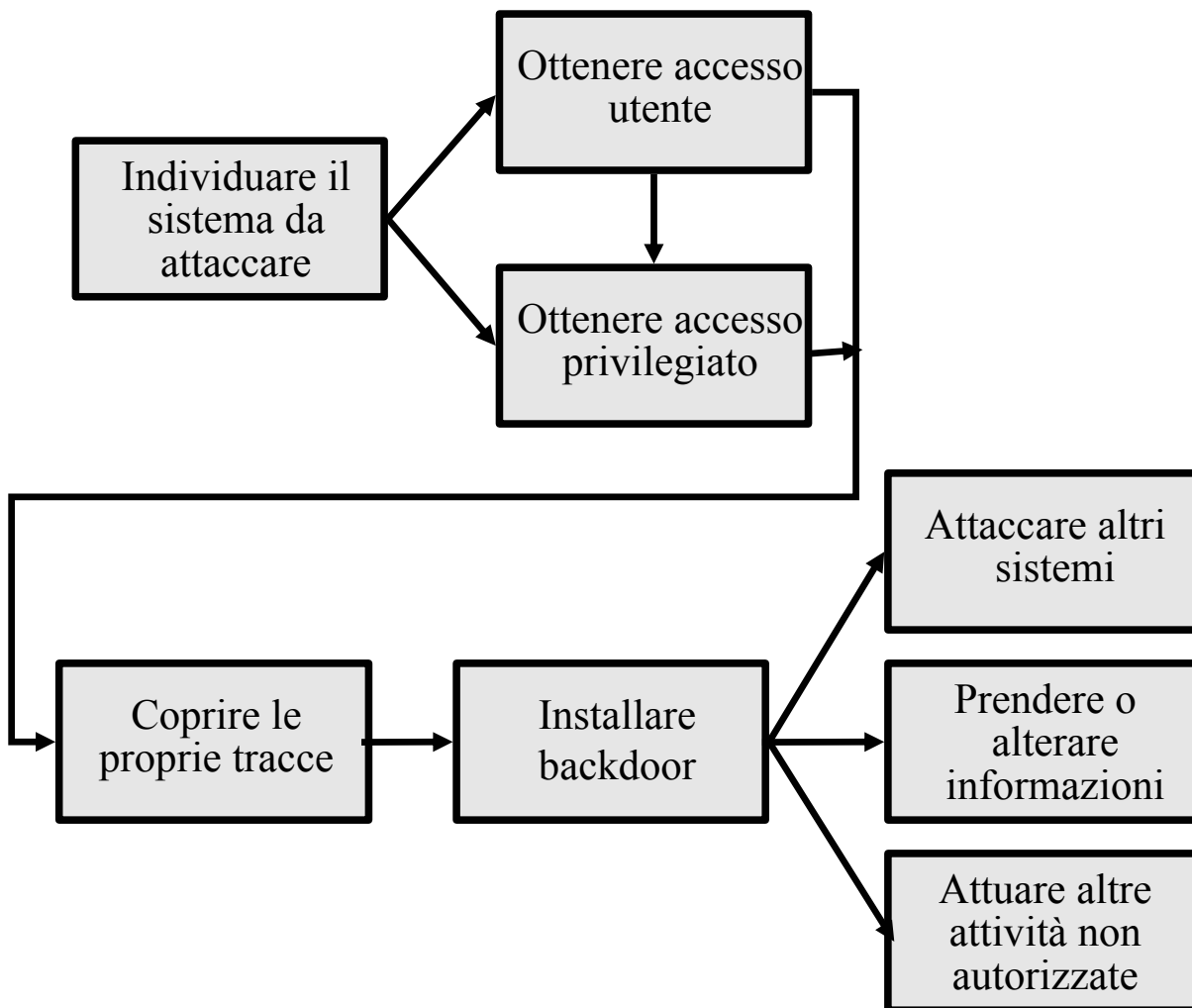
- una donna delle pulizie che "ruba" informazioni rovistando sulle scrivanie, nei cassetti, nei cestini della carta straccia, etc.
- un (ex) dipendente insoddisfatto che utilizza le sue conoscenze per "vendicarsi" di qualcuno o qualcosa
- un ragazzino quindicenne che utilizza qualche tool trovato "in rete" per "giocare" con i sistemi altrui
- un navigatore occasionale che trova per caso un malfunzionamento in un sistema e lo utilizza a proprio vantaggio
- un professionista pagato per penetrare nei sistemi della concorrenza

**Gran parte dei crimini informatici sono perpetrati da dipendenti o ex dipendenti insoddisfatti!**

# Come agiscono gli attaccanti?

- ❑ scelta del bersaglio  
generalmente un attacco mirato viene effettuato verso un bersaglio preciso (sia esso un sistema, una rete, una ditta, etc.);
- ❑ raccolta informazioni  
verranno raccolte quante più informazioni possibili sul bersaglio, sui sistemi utilizzati (OS, software, servizi, etc.), sugli amministratori e gli utenti (dati anagrafici, abitudini, etc.) analizzando tutte le possibili fonti di informazioni e cercando di non lasciare traccia di questa attività
  - "indirette"  
archivi di mailing list, newsgroup, pagine web, motori di ricerca, etc. è impressionante quanto sia facile raccogliere informazioni semplicemente usando, per esempio, altavista, anche senza nemmeno mai collegarsi al web-server del potenziale bersaglio) e altre fonti, anche non "informatiche" (elenchi del telefono, giornali, pubblicazioni, etc.)
  - "dirette"  
analisi dei sistemi (portscan, os fingerprint, analisi dei servizi, mappa della rete e dei sistemi, etc.), social engineering, trashing, etc.
- ❑ intrusione  
una volta identificate una o più potenziali vulnerabilità, l'hacker tenterà di introdursi nel sistema bersaglio (un esperto agirà solamente quando è praticamente sicuro di riuscire) o in un sistema con cui il bersaglio potrebbe avere "relazioni particolari" (stessa rete fisica, politiche firewall più favorevoli, utenti condivisi, file system condivisi, etc.).  
Qualora il sistema compromesso non fosse direttamente quello desiderato, l'hacker raccoglierà altre informazioni e continuerà a perseguire il suo obiettivo (il bersaglio o un sistema che lo "avvicini" ulteriormente) sfruttando la posizione di vantaggio acquisita
- ❑ guadagno di privilegi  
l'hacker cercherà di ottenere il controllo completo del sistema, qualora non avesse ancora i privilegi necessari
- ❑ eliminazione delle tracce  
l'hacker cercherà di eliminare ogni traccia della sua intrusione e delle sue precedenti attività nel sistema ed eventualmente installerà software apposito (backdoor) per facilitare una successiva intrusione

# Attacco tipico alla rete



## I passi tipici di un attacco:

- 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)

# Quali sono i rischi reali?

## ❑ frodi a danno dell'azienda o dei suoi clienti

per esempio tramite informazioni acquisite (password per e-banking, numeri di conto, numeri di carte di credito, etc.) o azione diretta (manipolazione transazioni, ordini, fatture, bilanci, etc.)

## ❑ perdita di informazioni sensibili

potrebbero venire distrutti o rubati (e diffusi) dati sensibili o vitali quali corrispondenza, bilanci, fatture, database di clienti/fornitori, progetti, documenti interni, etc.

## ❑ impossibilità di fornire servizi/beni ad utenti legittimi

per esempio a causa di un DoS oppure per il "downtime" necessario a ripristinare i servizi dopo un'intrusione

## ❑ responsabilità legali civili e penali

responsabilità per azioni commesse dai propri utenti/dipendenti ed adempimenti previsti dalla legge 675/96.

## ❑ perdita d'immagine

i vostri clienti (o futuri clienti) potrebbero trovare i vostri servizi poco affidabili o poco sicuri; immaginate solamente quale potrebbe essere la fiducia della clientela verso un sito di e-business in cui gli hacker abbiano scorrazzato liberamente

## ❑ calo del valore delle azioni

in moltissimi casi le società che hanno subito attacchi hanno visto crollare il valore delle loro azioni

Non è semplice "monetizzare" immediatamente i dati causati dall'attività degli hacker, salvo forse nel caso di frodi (storno di fondi, acquisizione illegale di beni/servizi, etc.). Certamente si tratta sempre di cattive notizie; anche semplici tool (DoS, etc.) usati per gioco da un ragazzino possono causare problemi notevoli e i danni di un attacco "mirato" condotto da un hacker esperto possono essere incalcolabili (perdita d'immagine, spionaggio industriale, etc.)

## Un'intrusione illegale può provocare danni incalcolabili!

*ICLC 2002 - Le principali tipologie di attacco ai sistemi aziendali e personali - Pagina 7*

# Chi sono i potenziali bersagli?

## Chiunque può rimanere vittima di un'intrusione o 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 hacker tool che permettono di verificare con estrema facilità ed in breve tempo la presenza di determinate vulnerabilità partendo da un elenco "pseudocasuale" di ip (per esempio, tutti i domini .it, oppure tutte le macchine della subnet 151.4.\*.\*, etc.)
- le informazioni che consideriamo banali o di scarsa importanza, possono risultare invece estremamente interessanti per altri

**Un qualsiasi sistema facilmente vulnerabile è un'occasione estremamente appetibile per un malintenzionato:**

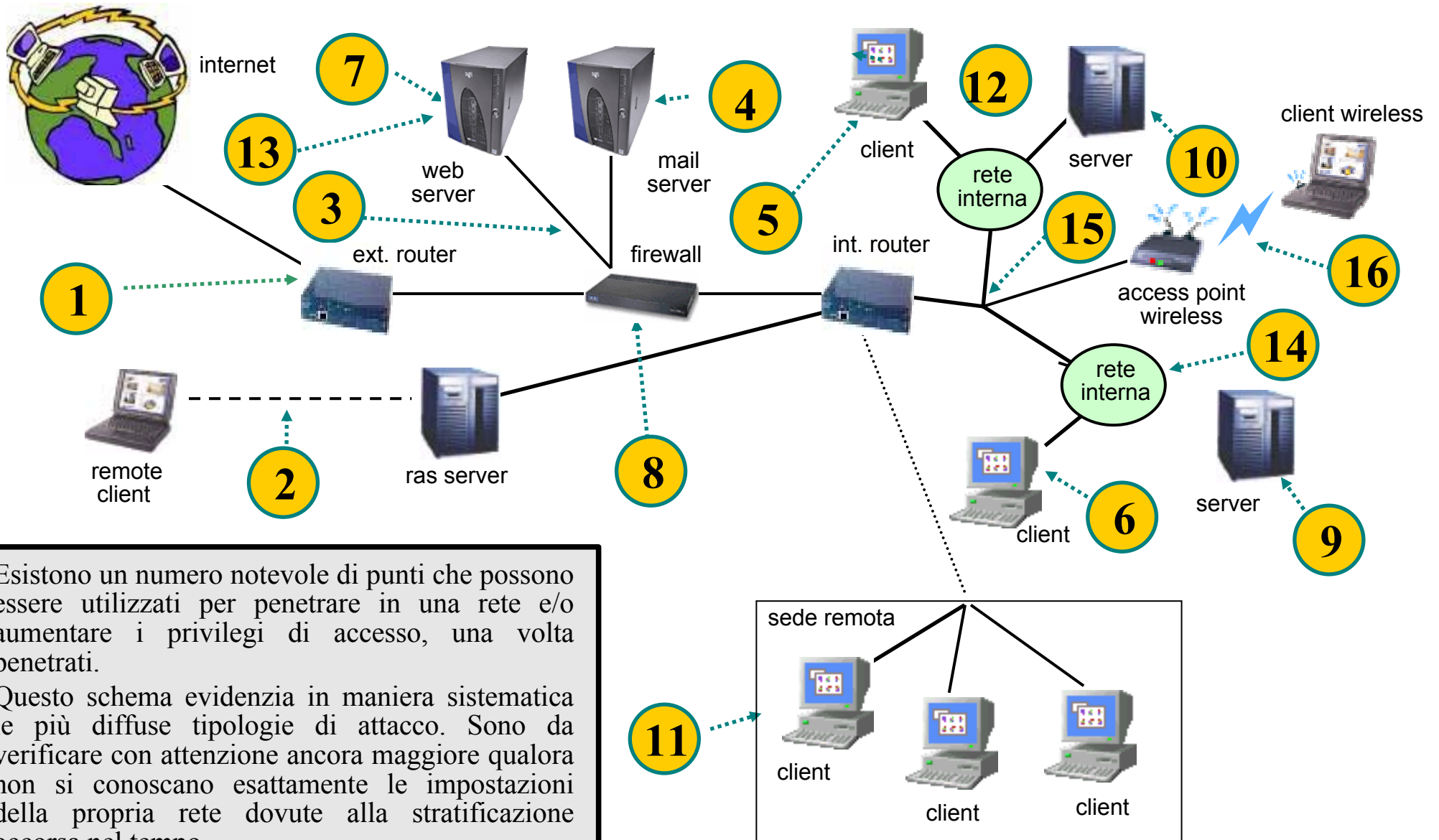
- può penetrarvi con facilità ed in breve tempo
- può cercare informazioni "interessanti"
- può utilizzarla come "trampolino di lancio" per raccogliere informazioni e attaccare altri sistemi nascondendo le proprie tracce
- può utilizzarne a proprio vantaggio le risorse (potenza di calcolo, bandwidth, etc.)
- può utilizzarla come "merce di scambio" per ottenere informazioni o "prestigio"

**Pensare di non essere un bersaglio appetibile per un attacco è quanto di più sbagliato ci possa essere!**

# Quali sono le corrette modalità di approccio al problema?

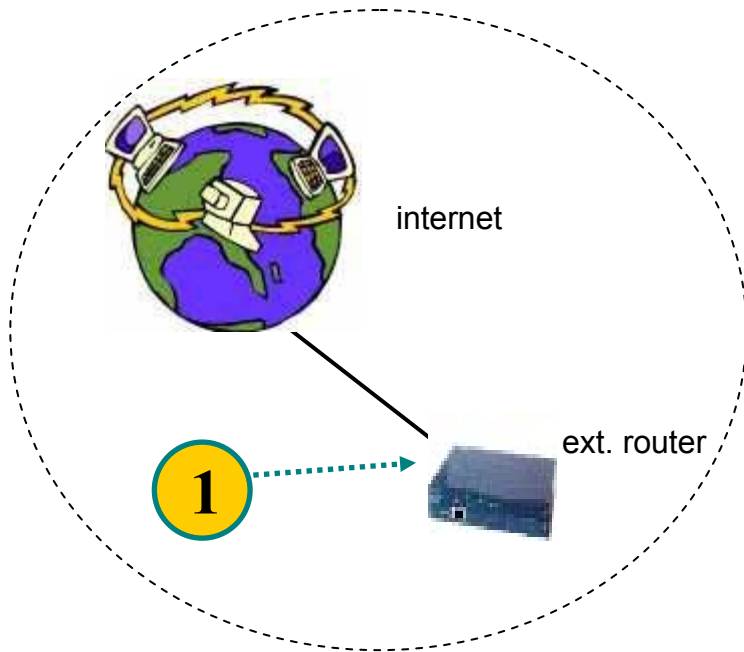
- Esistono soluzioni hardware e software ma, per la natura intrinseca di questi prodotti, non saranno **mai sufficienti** al problema.
- Non esiste e non esisterà **mai** una **soluzione definitiva**.
- La sicurezza di un sistema viene valutata dalla resistenza del suo **anello più debole**.
- Per ottenere un sistema che riesca a garantire al meglio gli obiettivi di sicurezza richiesti, bisogna valutare nelle varie componenti i **rischi** che si vengono a generare, tenendo conto dei livelli di protezione che vengono garantiti.

# Vulnerabilità maggiori



- Esistono un numero notevole di punti che possono essere utilizzati per penetrare in una rete e/o aumentare i privilegi di accesso, una volta penetrati.
- Questo schema evidenzia in maniera sistematica le più diffuse tipologie di attacco. Sono da verificare con attenzione ancora maggiore qualora non si conoscano esattamente le impostazioni della propria rete dovute alla stratificazione occorsa nel tempo.

# Router



Il router è il primo strumento che si trova sulla rete di una azienda, una configurazione inadeguata o erronea può permettere il passaggio di una serie di informazioni riservate che tramite i diversi protocolli viaggiano liberamente sulla rete.

Non devono essere presi in esame esclusivamente i principi di funzionamento della rete ma anche i principi basilari di sicurezza, in particolare tutto il traffico non necessario deve essere bloccato e devono essere implementate almeno le misure minime di monitoraggio per tenere sotto controllo il funzionamento e gli attacchi che vengono portati al router stesso.

Su molte apparecchiature è possibile sfruttare funzionalità di logging su sistemi esterni per registrare gli eventi riscontrati e le eventuali anomalie del sistema e della linea, difficilmente notificabili in maniera diversa. A seconda delle tipologie di router installati vi sono diverse funzionalità: di base dovrebbero essere attivati routing statico, logging e sistemi di filtraggio dei pacchetti (qualunque tipo supportato...).

E' possibile ottenere facilmente le seguenti informazioni da una rete configurata in maniera non ottimale:

- Subnet sulla rete
- Presenza di firewall
- Stato di manutenzione degli host della rete
- Host/segmenti di rete raggiungibili

...e sono possibili i seguenti attacchi:

- Denial of service basati su protocolli IP
- Amplificazione di attacchi verso altre reti
- Possibilità di abusi da parte degli utenti della rete interna verso host esterni

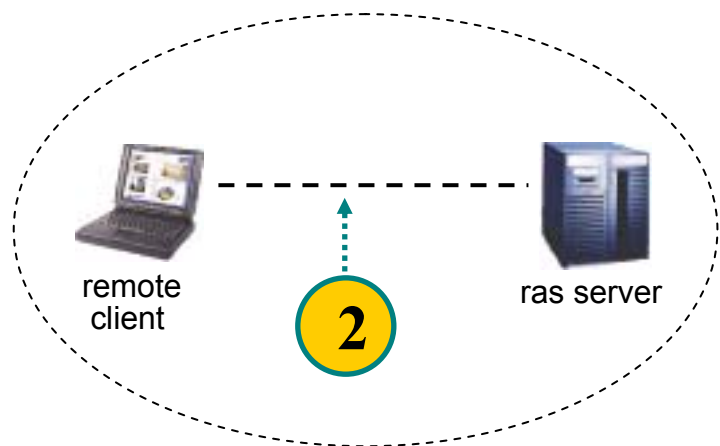
Nel caso in cui vi siano poi degli errori di configurazione sul router è possibile:

- Redirigere il traffico della rete
- Attaccare la rete connessa a monte
- Utilizzare le risorse della rete per fini personali
- Accedere in maniera indebita ai server della DMZ o della rete privata

# Collegamenti dial-in

Vengono spesso sottovalutati i pericoli derivanti dagli accessi "secondari" alla rete aziendale. Solitamente si tratta di punti di accesso non monitorati e da cui è facile penetrare direttamente sulla rete privata. In particolare è necessario tenere sotto controllo accessi e traffico generato dai client su queste linee secondarie e tenerle alla stessa considerazione di un firewall o di un punto di accesso principale alla rete aziendale. Erroneamente non vengono considerati accessi dial-in i

modem connessi a PC che permettono ai fornitori di "mantenere" le stazioni di lavoro da remoto, oppure modem utilizzati "solo in uscita" malconfigurati (risposta automatica attiva, possibilità di login, etc).. tutte situazioni che possono portare ad una compromissione.



E' consigliabile monitorare e registrare le connessioni degli utenti dialup e gli accessi ai server della rete aziendale per avere comunque le informazioni necessarie in caso di compromissione o fughe di notizie, ed impedire agli utenti di utilizzare modem senza un'adeguata policy di sicurezza

Cercare di ricostruire un avvenimento a posteriori quando si è in una condizione di carenza di dati è sicuramente più difficile che in una situazione dove siano impostati monitoraggio e logging efficacemente.

Spesso si pensa che non sia facile indovinare i numeri telefonici dedicati ai dati, invece è possibile:

- Fare ricerche sulle radici aziendali
- Fare ricerche nelle numerazioni dati delle compagnie telefoniche
- Ottenere il numero con tecniche di "Social engineering"

...e sono possibili i seguenti abusi:

- Utilizzo improprio di linee telefoniche aziendali
- Utilizzo di risorse aziendali (come connessione ad internet e relativi servizi)
- Possibilità rendersi anonimi sfruttando le strutture aziendali

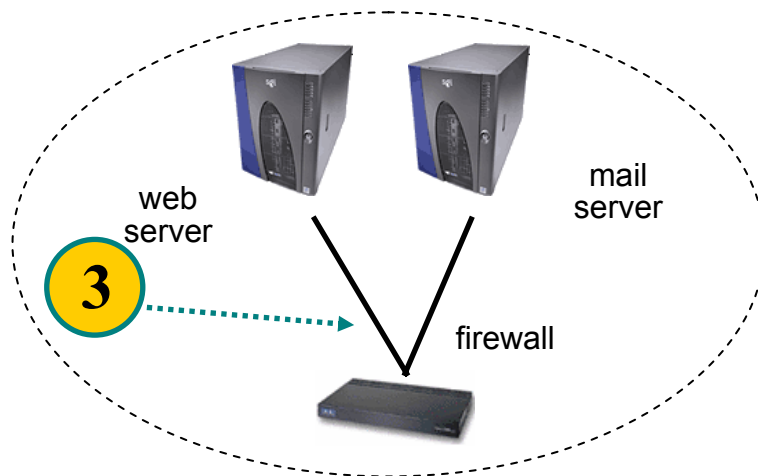
Nel caso in cui vi siano poi degli errori di configurazione sui server è possibile:

- Ottenere informazioni riservate
- Attaccare la rete connessa a monte
- Accedere in maniera indebita ai server della rete privata o della DMZ

# Sovrabbondanza di informazioni

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
- configurazione zone DNS
- configurazione SMTP
- servizi di informazioni erroneamente accessibili da Internet come SNMP, NetBIOS, sunrpc, finger



**Tutti i servizi superflui e le informazioni che sono liberamente accessibili sono un potenziale problema per la sicurezza dell'intero sistema.**

La non conoscenza o la diffusione di informazioni false aiuta in minima parte a mantenere la sicurezza e viene definita come "Security through obscurity" e guardata con superiorità dai puristi della sicurezza, comunque può essere uno degli strumenti utili per ottenere lo scopo di sicurezza che ci si prefigge.

E' comunque consigliabile impedire l'accesso a tutte le informazioni superflue per mantenere la sicurezza dei sistemi.

Spesso si pensa che non sia facile conoscere sistema operativo e relativa versione su una macchina remota invece:

- E' possibile fare dei test sullo stack TCP/IP per individuare il S.O.
- Aprire delle connessioni legittime verso il server per individuare il S.O. tramite "passive fingerprint" dello stack TCP/IP
- Connettersi ad applicativi e ricevere versione del S.O. e dell'applicativo

...una volta individuato S.O. ed applicativi è possibile portare attacchi mirati:

- a prendere il controllo della macchina
- a rendere la macchina inattiva
- ad ottenere altre informazioni

Nel caso in cui vi siano poi degli errori di configurazione sui server è possibile:

- Prendere il controllo del server
- Accedere ad informazioni riservate
- Attaccare altri server sulla rete

# Sovrabbondanza di servizi

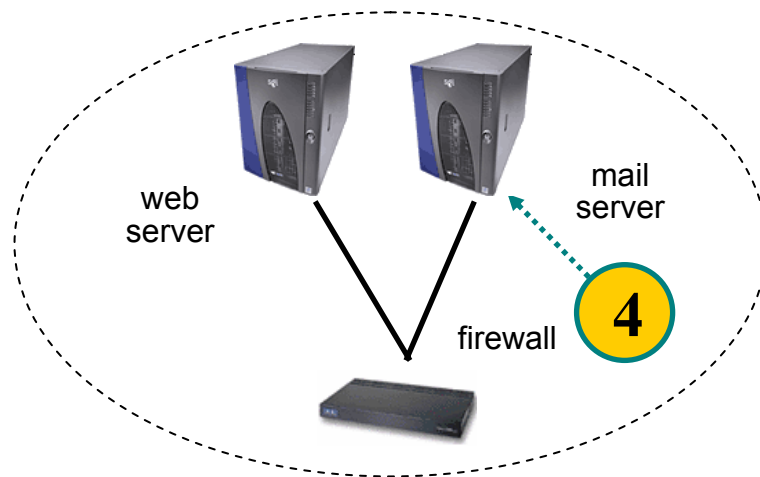
Spesso si ignora quale sovrabbondanza di servizi vengano attivati nelle configurazioni standard dei diversi S.O.

Sia per mantenere la sicurezza dei sistemi, che le loro prestazioni è bene disabilitare tutti i servizi superflui e/o inutilizzati.

Servizi superflui non mantenuti dagli amministratori si trasformano a breve termine in pericoli per la sicurezza della rete dal momento che vengono trovati quotidianamente problemi per i più diversi sistemi operativi e servizi sia "di marca" che "opensource".

**Tutti i servizi superflui sono un potenziale problema per la sicurezza dell'intero sistema.**

La mancanza di responsabili e del tempo per occuparsi della manutenzione e dell'aggiornamento dei server porta le macchine "ad invecchiare" e ad essere soggette a possibili esposizioni a livello di sicurezza che possono portare ad una compromissione dell'intero sistema.



Ci sono siti specializzati che riportano quotidianamente la scoperta di problemi di sicurezza in S.O. ed in applicativi con lo scopo di fornire agli amministratori gli strumenti per difendere la loro rete conoscendo i possibili attacchi.

Alcuni tra i migliori sono:

- <http://www.securityfocus.com>
- <http://packetstorm.securify.com>
- <http://www.nipc.gov>
- <http://www.ciac.org>
- <http://www.sans.org>

Ci sono anche diversi siti che ospitano mailing list dedicate alla sicurezza, tra cui segnaliamo:

- <http://www.sikurezza.org>
- [http://www.teach.it/liste/sicurezza\\_reti.htm](http://www.teach.it/liste/sicurezza_reti.htm)
- Bugtraq seguendo i link da Securityfocus
- <nntp://it.comp.sicurezza> (sottogruppi)

Molti riportano vulnerabilità ed exploit per chi volesse sperimentare praticamente la sicurezza dei propri sistemi.

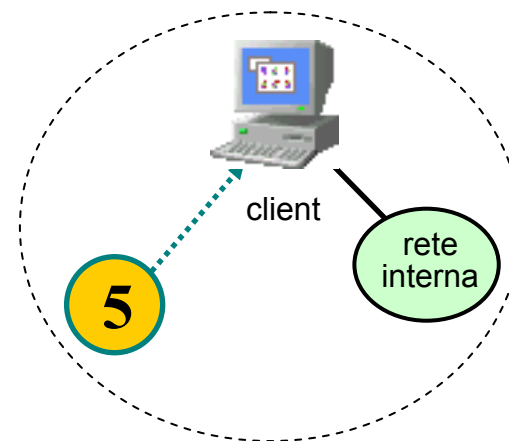
# Password facilmente deducibili

La mancanza di una politica relativa alla scelta, all'impiego e alla manutenzione delle password spesso "autorizza" gli utenti (e gli amministratori!) a scegliere ed utilizzare password "facili" (da ricordare, da digitare, etc.), comuni a tutti gli ambienti indistintamente dalla loro importanza e che spesso diventano di dominio pubblico all'interno dell'ufficio. Questi comportamenti rendono particolarmente facili i tentativi di forzatura delle password da parte di intrusi, senza considerare cosa questo rappresenti per la sicurezza della rete aziendale.

Nel caso di password per gli utenti è necessario cercare principalmente di insegnare un buon modo per inventare e ricordare password "sicure". Per esempio al posto di utilizzare "mario" si può scegliere "Mari0++" o "=M4r10=". Concettualmente sono quasi la stessa cosa da ricordare, ma la resistenza ad attacchi mirati ad indovinare le password aumenta notevolmente.

E' inoltre importante impostare nelle politiche di gestione delle password un numero minimo di caratteri (p. es. non inferiore a 5, o maggiore in situazioni dove sia richiesto un grado di sicurezza particolarmente elevato) in modo da impedire tentativi di violazione tramite "brute force" ed impostare un ciclo di vita delle password compreso tra i due ed i tre mesi in modo che la conoscenza "indebita" di una password da parte di un utente non si trasformi in un "permesso di accesso" perenne.

Deve essere anche considerata una violazione del regolamento aziendale utilizzare account e password altrui per accedere alla rete (la gravità della violazione varia in funzione degli utilizzi e dell'importanza delle password).



Bisogna scegliere un giusto compromesso tra la "robustezza" delle password e la capacità degli utenti di utilizzarle (anche in funzione del livello di sicurezza che si vuole ottenere).

Impostare delle password troppo complesse in un ambiente di lavoro spesso porta gli utenti a scriverle su bigliettini, generalmente attaccati sul monitor o "nascosti" sotto la tastiera, nei cassetti o semplicemente "svolazzanti" in giro per l'ufficio.

Esistono diversi sistemi per garantire la sicurezza in maniera efficace investendo in tecnologia e rendendo la rete particolarmente sicura. (Chiavi hardware e/o certificati digitali, etc.)

# Account di prova

Utilizzando ambienti di sviluppo o di test bisogna considerare il fatto che, se inseriti in una rete di produzione (integralmente o parallelamente), devono essere prese in considerazione una serie di misure per ridurre al minimo l'esposizione a problematiche di sicurezza.

Per esempio, la creazione di un account di prova con privilegi di amministratore (U:Pippo P:pippo) sul dominio espone ad un pericolo di sicurezza tutte le macchine dello stesso.

Anche la creazione di account di prova su applicazioni o computer della rete può aprire la porta a possibili tentativi di intrusione.

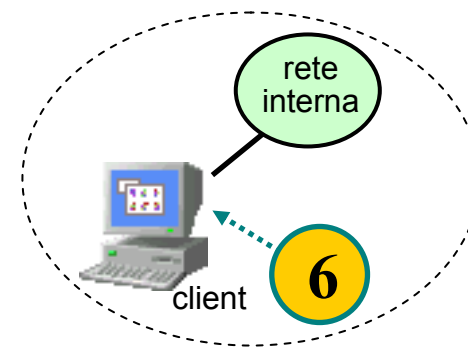
Nella stessa categoria rientrano anche tutti gli account e sistemi che hanno password di default e che sono da conoscere e verificare per i diversi applicativi.

Non esiste una soluzione "universale" per gli account di prova o di default se non quella di utilizzare le stesse politiche (robustezza delle password, scadenza, controllo, etc.) degli account "normali". E' opportuno nominare dei responsabili che monitorizzino e mantengano questi account e a cui rivolgersi in caso di necessità o problemi.

E' altrettanto importante sospendere e/o cancellare questi account quando sia terminato lo scopo per cui erano stati creati.

Un "super-account" o un account di servizio sono abbastanza facili da individuare una volta che si riesca ad accedere al sistema o che si abbia possibilità di vedere il traffico che viene generato sulla rete.

Gli account non documentati con password di default sono facili da individuare una volta identificati i servizi stessi.



Una alternativa è quella di provare account "tipo" e vedere se esistono sui vari servizi del sistema:

- administrator, admin, root, postmaster, mail, pippo, prova, prova1, prova99, prova00, user, guest, ced, NomeDitta, NomeProgramma, etc.
- lista delle password di default su vari sistemi:  
<http://www.securityparadigm.com/defaultpw.htm>

# Configurazioni interne

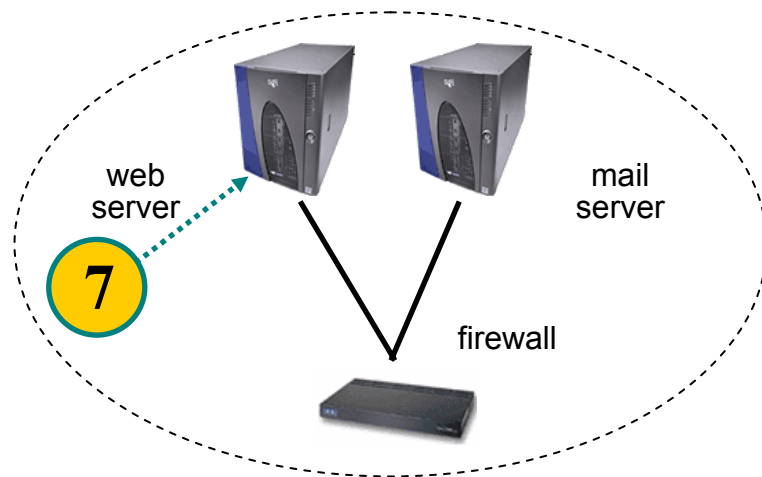
Spesso si ignora lo stato delle configurazioni interne dei server, p. es. relativamente agli script CGI, alle directory di lavoro di servizi quali FTP anonimo o simili, etc.

Questi sono potenziali pericoli per la sicurezza

del server che potrebbero portare ad una compromissione del sistema su cui girano queste applicazioni.

In particolare tutte le parti che vengono sviluppate da webmaster o programmatori che non abbiano cognizioni di sicurezza o che utilizzino degli strumenti automatizzati devono essere riviste in ottica di sicurezza pena il fatto di esporre potenzialmente a compromissione la riservatezza e l'integrità delle informazioni originali.

La messa in sicurezza di una macchina esposta alla rete internet si dà per scontata; è invece necessaria una preparazione particolare per garantire un livello ottimale di tutela delle informazioni e dell'immagine aziendale.



La pericolosità nella configurazione superficiale o errata in un servizio pubblicamente accessibile rende quel servizio pubblicamente attaccabile.

Sono all'ordine del giorno problemi di questo tipo anche sui siti delle grandi firme dovuti al fatto di non considerare correttamente le possibilità legate ad input non standard (p. es. "..", ".", "/", "&", "|", ";" e relative corrispondenze in UNICODE, etc.).

Relativamente a directory di lavoro di FTP e programmi simili, molti problemi di sicurezza sono legati al fatto di forzare la scrittura di file e cartelle con lunghezze superiori a quelle previste nei buffer, o utilizzare comandi che non controllano adeguatamente l'input fornito dagli utenti.

La configurazione dei servizi deve essere impostata utilizzando i minori privilegi possibili per esporre i sistemi ad un rischio minore, anche in caso di compromissione.

# Firewall

Il firewall non deve limitarsi a proteggere la rete DMZ dagli attacchi esterni ma deve difendere anche la LAN sia dagli attacchi da Internet che dalla DMZ, nel caso in cui un server pubblico venga compromesso.

Deve essere visto in una ottica particolarmente restrittiva dal momento che su questo strumento si basa almeno il 75% della sicurezza aziendale.

Il controllo degli accessi, il monitoraggio e la registrazione degli eventi

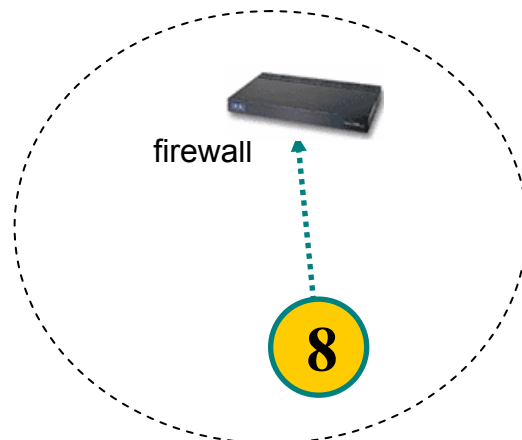
degni di nota devono essere effettuati in maniera particolarmente accurata e documentata.

Sarebbero da evitare tutti i servizi che forniscano accesso diretto (p. es. da Internet) o indiretto (p. es. dalla DMZ) a macchine sulla rete interna, anche se spesso non è possibile per necessità logistiche varie.

In questi casi è necessario valutare molto attentamente quale sia la soluzione che fornisca il migliore compromesso tra sicurezza e funzionalità, le eventuali alternative, i potenziali di rischio.

**Deve essere nominato un responsabile del firewall che si occupi di mantenerlo e leggere gli eventi della rete per reagire opportunamente a ciò che avviene, sia attacchi, che analisi pre-attacco.**

Le configurazioni devono essere impostate per permettere solo il traffico necessario dall'interno verso l'esterno e viceversa. Tutto il resto deve essere bloccato, segnalando attacchi e traffico anomalo o sconosciuto.



E' importante capire che buona parte dei firewall si occupano principalmente di permettere o bloccare a livello di protocolli IP il traffico, non di analizzare il contenuto per valutare se ci si trovi in presenza di una "sessione con scopi malevoli". Alcuni firewall più avanzati sono in grado di effettuare anche "content inspection" più o meno accuratamente, non è comunque buona norma basare la sicurezza della propria rete esclusivamente su questa protezione.

E' possibile filtrare il contenuto della posta elettronica o di file inviati sui server o scaricati dai client tramite software appositi (p. es. antivirus) che devono comunque essere adeguatamente e costantemente aggiornati (p. es. tramite apposite strutture di rete o con installazioni distribuite) per essere efficaci.

Le regole di firewalling devono essere valutate avendo consapevolezza dei diversi tipi di traffico da permettere, valutando anche la pericolosità generica dei servizi che si aprono e quella specifica dei software adottati.

# Manutenzione e aggiornamento

Un grave pericolo per la sicurezza è dovuto alla scarsa (o assente) cura prestata nell'aggiornamento e manutenzione dei vari server (software, configurazioni, etc.). L'invecchiamento e la mancata applicazione delle patch di sicurezza aumentano enormemente i rischi.

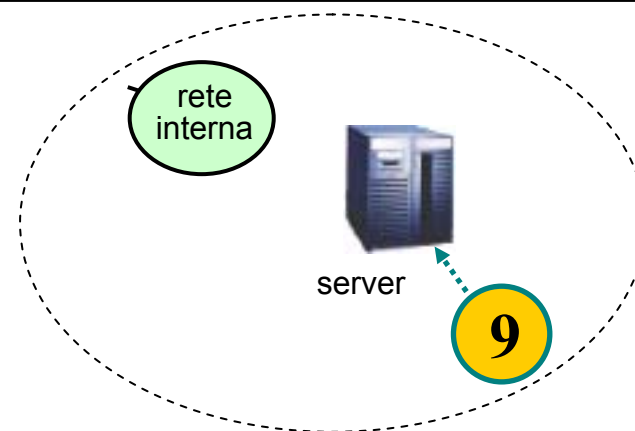
Trovare la giusta via tra aggiornamenti e sistemi stabili è abbastanza complesso, soprattutto nel caso di aggiornamenti cumulativi che risolvono problemi di sicurezza, ma aggiungono anche funzionalità nuove (spesso non volute o non necessarie). Non è caso infrequente che aggiornamenti rilasciati in fretta e furia dai produttori per supplire a vulnerabilità appena scoperte abbiano introdotto nuove vulnerabilità o instabilità più o meno gravi.

E' necessario dedicare risorse al monitoraggio dei sistemi, alla loro manutenzione, allo studio degli aggiornamenti (di sicurezza e non) e al loro impatto nella struttura di rete.

A volte un'alternativa può essere quella di anteporre dei sistemi robusti e leggeri davanti ai server reali, stessa tecnica che si può utilizzare per una DMZ su Internet. Le problematiche per mantenere questa doppia struttura spesso sono tali da renderne sconsigliabile o non conveniente l'utilizzo.

E' anche necessario essere continuamente aggiornati sulle problematiche di sicurezza: pubblicazione di nuove vulnerabilità, metodologie e "strumenti di attacco" (exploit), etc. . Spesso gli aggiornamenti vengono rilasciati **dopo** la diffusione "pubblica" della vulnerabilità, aprendo una "finestra temporale" di rischio reale ed immediato.

Vengono scoperti quotidianamente problemi di sicurezza, sia nei sistemi commerciali che in quelli open source. L'invecchiamento di un sistema è dovuto alla mancanza di aggiornamenti e controlli per le problematiche dei servizi, delle applicazioni e del sistema operativo.



E' necessario considerare nel bilancio di sicurezza anche il periodo di esposizione alle vulnerabilità prima del rilascio di un'apposita patch o soluzione da parte del fornitore. Spesso in questo lasso di tempo è necessario disabilitare il servizio, provocando danni all'utenza e all'immagine aziendale.

# Mancanza di controlli di accesso

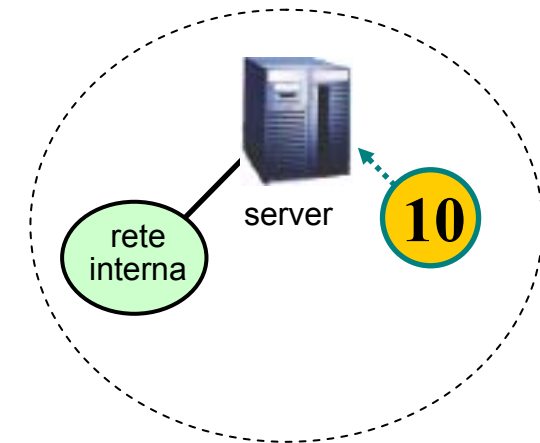
Per aumentare la facilità d'uso, spesso gli amministratori di sistema o direttamente i progettisti di software non implementano (o non abilitano di default) politiche d'accesso restrittive, permettendo agli utenti di "scorrazzare liberamente" su reti e sistemi.

Altrettanto spesso non si implementano adeguate politiche di monitoraggio dell'accesso alle risorse, almeno fino a quando non si rimane "scottati" (per qualche utente "smanettone" o qualche intruso).

Configurazioni restrittive e monitoraggio degli accessi sono pratiche particolarmente importanti nell'implementazione delle politiche aziendali di sicurezza, di cui devono essere una manifestazione applicata.

La mancanza di controlli lascia agli utenti la libertà di accedere a tutti i dati presenti sui sistemi. Spesso e volentieri è possibile accedere ad informazioni importanti e/o riservate semplicemente "curiosando" per i vari file server aziendali. La mancanza di un adeguato monitoraggio impedisce di verificare eventuali violazioni o tentate violazioni e di risalirne agli autori.

L'assenza di controlli sugli accessi impedisce anche di mantenere un adeguato livello di riservatezza tra i vari gruppi di utenti legittimi: tutti possono accedere senza restrizioni o differenziazioni (p. es. i tecnici possono accedere ai dati della contabilità, il reparto spedizioni può accedere alle configurazioni dei server, i grafici possono accedere alla posta del direttore generale, etc.).



Esistono una serie di strumenti atti ad identificare, in funzione del traffico di rete o semplicemente eseguendo delle query opportunamente strutturate, il numero e la tipologia di file server, le condivisioni che non richiedono autenticazione o quelle con password facilmente deducibili, procedendo eventualmente a simulare un attacco con forzatura delle password per ottenere accesso alle informazioni sul server.

Sono disponibili per diversi sistemi operativi e diverse tipologie di servizi (SMB, NFS, pop3, web, rlogin, etc.).

# Eccessive relazioni di fiducia

Vengono definite relazioni di fiducia quelle relazioni che autorizzano un gruppo di host, client o utenti ad effettuare determinate operazioni senza ulteriori autenticazioni che non siano l'appartenenza ad uno dei gruppi specificati. Vengono dette "eccessive" quando non sono state calcolate accuratamente tutte le implicazioni legate a queste relazioni, o quando "l'appartenenza" può essere facilmente falsificata, come nel caso di relazioni basate su indirizzi IP, su autenticazioni "lato client" (ident, etc.) e simili.

P. es.: il gruppo amministratori ha la possibilità di accedere a tutti i dati del sistema e chiunque appartenga ai sistemi informativi appartiene al gruppo amministratori. **Tutti** gli utenti dei sistemi informativi (indipendentemente dalle mansioni o dal livello di responsabilità) hanno accesso a **tutti** i dati del sistema.

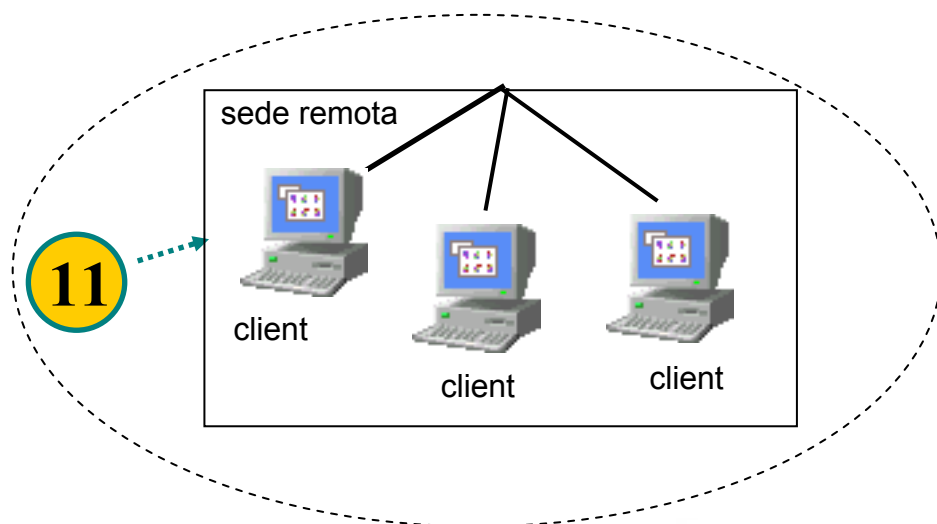
Altri esempi di eccessive relazioni di fiducia potrebbero essere discriminazioni su indirizzi IP, appartenenza al dominio, utilizzo di un dato programma o altre assunzioni "generiche" basate su controlli banali e facilmente superabili.

Per limitare queste problematiche è possibile:

- utilizzare gruppi e sottogruppi per tipologie di utenti
- suddividere la rete in settori diversi con accessi differenziati
- affidare la scelta e la gestione delle tipologie di utenti ad un responsabile "tecnico" qualificato

Stabilire relazioni di fiducia troppo permissive su una rete permette di ottenere maggiore "elasticità" di utilizzo, ma porta frequentemente ad una mancanza di controlli e limitazioni.

In particolare, l'estensione dei "domini" di gruppi di lavoro a rami della rete o estensioni geografiche che non hanno una struttura CED è spesso una necessità, si devono però considerare molto attentamente le implicazioni per la sicurezza dei dati e delle risorse aziendali.



# Servizi non autenticati

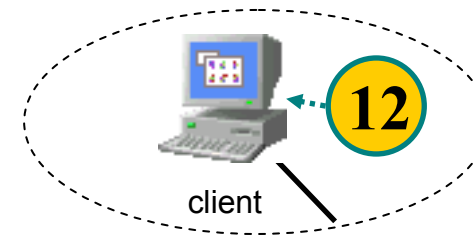
Esistono una serie di servizi che per convenzione o comodità si basano su protocolli non autenticati (ovvero non richiedono username e password per l'accesso o la fornitura del servizio).

In alcuni casi è comunque possibile implementare una verifica "preventiva", basandosi su un sistema di autenticazione globale (single sign-on, domini, directory services, etc.).

E' di fondamentale importanza conoscere quali servizi utilizzati sulla propria rete siano basati su protocolli non autenticati (prendendo anche coscienza di quali utilizzino sistemi di autenticazione in chiaro, soggetti ad intercettazione).

I servizi non autenticati possono essere utilizzati in maniera "sicura" solamente in quelle situazioni dove non sia assolutamente possibile che avvengano "contaminazioni" da parte di soggetti non autorizzati, p. es. reti "chiuse", VPN, etc.; oppure in quelle situazioni dove potrebbe non essere necessaria un'identificazione delle parti in causa (utilizzo di un proxy server per l'accesso ad Internet, p. es.). In ogni caso, tutti coloro che hanno accesso ai segmenti di rete dove vengono utilizzati protocolli non autenticati devono essere assolutamente fidati. Non sarà possibile ricostruire "a posteriori" gli accadimenti, in caso di violazioni o problemi.

Per esempio si potrebbero utilizzare servizi non autenticati in una rete sconnessa dalla rete aziendale e dove sia predominante il lavoro di gruppo o dove l'accesso a questa rete sia garantito da sistemi di autenticazione sicura come chiavi hardware, certificati o altri strumenti che garantiscano un livello simile di sicurezza.



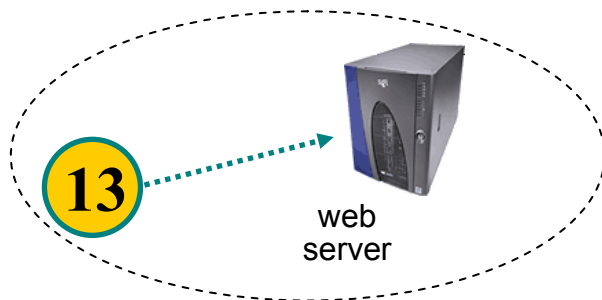
Vi sono una serie di servizi che sono non autenticati: per il loro utilizzo non è necessario fornire un account valido, perché si basano su assunzioni di fiducia derivanti da relazioni quali:

- la richiesta di un utente
- la richiesta di un computer della rete interna
- una richiesta opportunamente composta

in particolare possono verificarsi una serie di condizioni che, opportunamente sfruttate, possono fornire accesso non autenticato a risorse o servizi "sensibili" all'interno della rete, ad esempio:

- utilizzo di meccanismi di impersonazione per emulare altri utenti
- utilizzo di un proxy (che autorizza tutte le richieste interne)
- composizione di richieste ad hoc

# Monitoraggio inadeguato



Il grado di consapevolezza degli amministratori relativamente al traffico ed alle attività di rete è in buona parte dovuto alle segnalazioni degli utenti e alla lettura dei log. Spesso le segnalazioni degli utenti sono un campanello di allarme che può spingere gli amministratori a scoprire cosa non funziona.

I log sono i "testimoni oculari" di quanto avviene sulla rete, ma spesso "guardano" esclusivamente in un'unica direzione. Quando vengono installati sistemi operativi e applicazioni, i rispettivi log si occupano di registrare e raccogliere determinati eventi. Ci sono però molte informazioni importanti che di default non vengono registrate da nessuna parte.

Per evitare di trovarsi in spiacevoli situazioni deve essere prestata attenzione alla configurazione dei log e alle casistiche e tipologie di eventi che questi sono in grado di individuare e registrare.

Si ricorda che per monitorare traffico ed attività di reti e sistemi con un dettaglio tale da permettere di determinare con esattezza l'utente coinvolto è necessaria una liberatoria (che deve essere prevista nel regolamento di sicurezza aziendale e fatta firmare ai dipendenti).

Avere dei sistemi di cui nessuno si occupa è uno dei modi migliori per lasciare che degli intrusi possano accedere alle risorse informative aziendali, agire indisturbati e cancellare le loro tracce, magari senza che l'intrusione venga mai scoperta.

Presenza dei log, lettura dei log, reazione in caso di "eventi", riscontro alle reazioni sono attività quotidiane che devono essere effettuate per "sapere" cosa avviene sulla propria rete.

Esistono appositi strumenti (software e/o hardware) che si occupano esclusivamente di monitorare il traffico sulla rete con una casistica di tipologie:

- IDS (sistemi di individuazione delle intrusioni)
- Monitor del traffico per:
  - banda utilizzata
  - protocolli utilizzati
  - indirizzo sorgente o destinazione
- Strumenti di controllo sui contenuti del traffico per parole chiave

# Politiche di sicurezza

L'amministrazione delle macchine viene semplificata e razionalizzata quando vengono implementate politiche di sicurezza che regolamentano l'uso della rete e delle risorse aziendali.

Le politiche di sicurezza che regolano l'uso di sistemi e risorse devono intervenire a livello di regolamento aziendale, definendo sanzioni e restrizioni da applicare per le violazioni accertate.

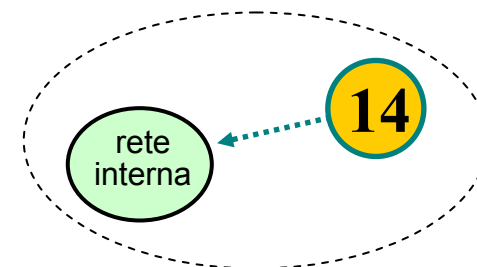
Da un punto di vista tecnico bisogna considerare che utilizzare un computer e poter accedere alle reti aziendali ed extra-aziendali sono strumenti indispensabili per i dipendenti. Non è possibile negare questi strumenti completamente, ma deve essere chiaro che comportamenti indisciplinati o palesemente malevoli sono pericolosi per i dati ed il lavoro proprio ed altrui, sia in caso di abusi "con dolo", sia nel caso di semplice imperizia o incoscienza.

Questi comportamenti devono essere ripresi e "limitati" con restrizioni quali p. es.:

- impossibilità di installare programmi
- impossibilità di modificare le "impostazioni aziendali" (configurazione, desktop, sfondi, screensaver, tool)
- impossibilità di sfruttare servizi e risorse aziendali a fini personali

E' importante far comprendere agli utenti che i computer sono strumenti di lavoro aziendali e come tali vanno trattati. Vi è un'abitudine diffusa a considerare i computer come "cosa propria"

Le politiche di sicurezza integrano il regolamento aziendale con norme e discipline che regolano l'utilizzo della rete e dei sistemi riguardo alle modalità d'installazione ed utilizzo e disciplinano il comportamento degli utenti: dalla scelta del software, all'utilizzo di password, etc.



Le politiche di sicurezza dovrebbero arrivare a definire diversi livelli necessari a garantire la tutela delle informazioni in funzione della loro riservatezza.

Dalla definizione dei livelli di sicurezza dovrebbero risultare la suddivisione in gruppi di utenti e tipologie di permessi negli accessi alle risorse aziendali.

Generalmente non si effettuano queste analisi, a discapito della sicurezza.

# Partizionamento fisico

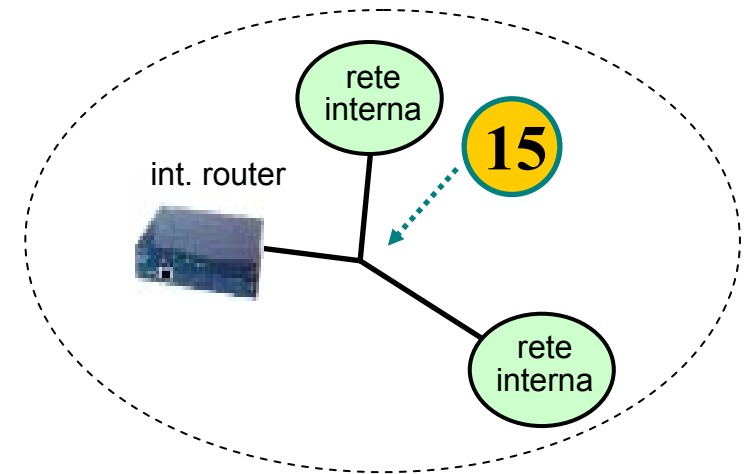
Per partizionamento fisico delle reti si intende: mantenere su segmenti di rete fisicamente separati host e servizi logicamente diversi tra loro.

Questo discorso si può applicare ai vari dipartimenti e/o sedi di un'azienda in cui si voglia garantire l'impossibilità di accedere a determinate informazioni, ma si deve applicare particolarmente a zone di rete quali DMZ e LAN, dove separare il traffico IP proveniente da Internet (scremato ma comunque potenzialmente pericoloso) e quello delle reti private è una necessità e non un'opzione.

Il partizionamento fisico delle reti aiuta:

- ad identificare a priori i punti deboli e monitorarli
- a dimensionare correttamente la rete
- ad analizzare a priori i servizi permessi (in concomitanza con la politica aziendale) e valutare il loro impatto sulla rete
- ad avere la capacità di circoscrivere eventuali penetrazioni a zone non vitali della rete
- ad avere consapevolezza dei pacchetti che devono viaggiare sui distinti segmenti e quindi individuare situazioni anomale

E' importante considerare che la divisione "fisica" deve essere reale, non basata su tecnologie quali VLAN o segmenti "switched" (queste barriere possono essere superate abbastanza facilmente da un attaccante motivato e tecnicamente preparato).



E' un errore dettato dalla sottovalutazione delle possibilità tecniche non partizionare fisicamente le reti lasciando dati, servizi e server "logicamente" separati sullo stesso segmento fisico di rete.

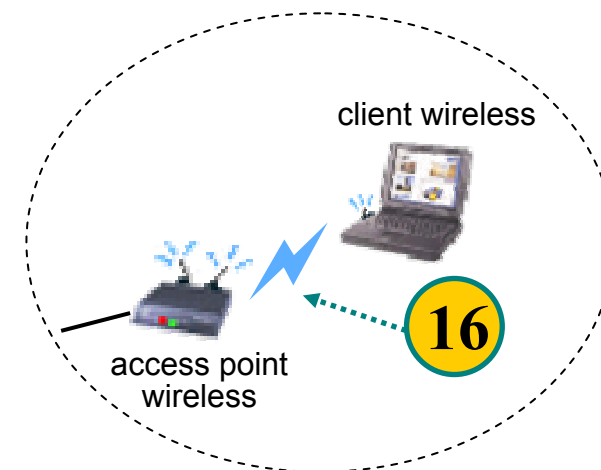
Questo errore diventa grave nel momento in cui le reti in oggetto sono una la DMZ difesa dal firewall, ma accessibile pubblicamente per alcuni servizi e un'altra la LAN totalmente difesa dal firewall e custode dei progetti e delle informazioni aziendali.

# Wireless (802.11)

Le reti Wireless, in particolar modo quelle basate sul protocollo 802.11b (Wi-Fi) sono sempre più diffuse, nelle realtà aziendali.

Esistono varie problematiche di sicurezza nelle configurazioni "by default" delle apparecchiature e delle reti Wi-Fi.

- trasmissioni in chiaro  
possibilità di analizzare tutto il traffico in transito, anche all'esterno del perimetro aziendale
- assenza/carenza di autenticazione  
possibilità di inserirsi sulla rete locale ed attaccare gli host presenti sulla LAN, sulla DMZ e su Intranet/Internet.  
Molto spesso gli AP sono posizionati direttamente sulla LAN, senza particolari filtri sul traffico.
- attacchi all'AP o alle stazioni  
spesso gli AP e/o i computer dotati di scheda Wireless sono attaccabili con i metodi standard
- trasmissioni cifrate con WEP  
il protocollo WEP (Wired Equivalency Privacy) presenta varie vulnerabilità nell'implementazione, con chiavi sia a 40 che a 128 bit. Per un attaccante potrebbe essere possibile, analizzando una discreta quantità di traffico effettuato con la stessa chiave WEP, decifrare i dati trasmessi ed entrare in possesso della chiave per decifrare il traffico futuro oppure inserirsi sulla rete.



<http://www.infosec.it/download/Infosecurity2002-Wireless.pdf>

Le reti Wireless malconfigurate sono potenzialmente molto pericolose... spesso è possibile portare questi attacchi direttamente dall'esterno dell'azienda ("parking lot attack").

Per le loro caratteristiche, le onde radio attraversano muri, pareti, spazi aperti, vetri, etc.

E' possibile portare gli attacchi con apparecchiature standard e poco costose. Aggiungendo un'antenna, anche a distanze considerevoli (3-400 metri).

# Is your Business Internet exposed?



<http://www.infosec.it>

[info@infosec.it](mailto:info@infosec.it)

*Noi possiamo aiutarvi*

Questa presentazione sara' liberamente scaricabile dal nostro sito web la prossima settimana