

# Un mondo connesso

- In passato molte reti di calcolatori erano isolate, ma a partire dagli anni 80 comincia a diffondersi Internet.
- Internet cresce esponenzialmente, dagli anni 90 migliaia di reti e milioni di PC sono connessi attraverso Internet: i computer che prima erano isolati in piccole reti ora sono connessi nel mondo di Internet.
- Una connessione globale ha molti benefici, ma ha anche alcuni svantaggi: non tutti usano responsabilmente la rete, alcuni pensano che la connessione globale sia l'opportunità di accedere ai PC e ai dati altrui.
- **ESIGENZA:** difendersi da attacchi indesiderati.

# Hardening

- Un computer assolutamente sicuro non esiste; nemmeno un computer spento può essere considerato assolutamente sicuro.
- Inoltre, la definizione stessa di sicurezza è relativa a cosa si vuole proteggere. In pratica, più un sistema è sicuro, più è difficile il suo utilizzo poiché le procedure di sicurezza si scontrano spesso frontalmente con la fruibilità; questo significa che la sicurezza costa e riduce la produttività, ma, d'altra parte, riduce i rischi.
- Invece di partire da un sistema molto sicuro per renderlo anche utilizzabile, la prassi è di partire da un sistema facilmente utilizzabile e cercare di renderlo più sicuro: questo processo è spesso indicato con il nome di Hardening.

# Firewall

- Un firewall consente di difendersi dagli attacchi alla propria rete provenienti da Internet.
- Come il guardiano di un edificio, il firewall verifica l'identità e lo scopo della visita di ciascun visitatore, e verifica anche che il visitatore esca mantenendone traccia nei registri. Inoltre, nega l'accesso a chi non ne ha il permesso.
- Il firewall è posizionato tra la LAN aziendale e la rete in modo da ispezionare qualunque dato proveniente da o destinato ad Internet.

## Evoluzione - NIDS

- I NIDS, Network Intrusion Detection System, sono degli strumenti dediti ad analizzare il traffico di uno o più segmenti di una LAN al fine di individuare anomalie nei flussi o possibili intrusioni informatiche.
- In un sistema informatico che implementa valide politiche di sicurezza e che adotta firewall ed antivirus centralizzati i NIDS giocano un ruolo fondamentale in quanto:
  - analizzano i pacchetti identificando il traffico anomalo;
  - danno informazioni sulle scansioni che la rete ha ricevuto;
  - permettono di ricevere allarmi real-time

## Evoluzione - NIDS

- I NIDS, inoltre, permettono di monitorare il comportamento degli utenti interni alla rete:
  - rilevano eventuali attacchi provenienti dalla rete interna verso la rete esterna;
  - rilevano la presenza di eventuali worm che cercano di inviare informazioni all'esterno della rete;
  - effettuano il monitoraggio delle risorse condivise utilizzate;

## Wi-Fi

- I protocolli Wireless hanno ulteriori problemi di sicurezza rispetto alle loro controparti su cavo.
- Se una rete ha una componente Wireless, è possibile che un attaccante dall'esterno dell'edificio possa ottenere copia almeno di tutto il traffico Wireless, oppure introdursi nella rete ed utilizzarla per connettersi ad Internet o come punto di partenza per effettuare attacchi ad altri.
- A chiunque sembrerebbe dunque necessario:
  - a) che vi sia un protocollo sicuro di autenticazione ed autorizzazione, per evitare che una stazione possa connettersi alla rete senza avere le necessarie credenziali;
  - b) che tutto il traffico tra sia cifrato, per evitare che qualcuno in ascolto possa fare una copia di ciò che transita.