

Internet e formazione on-line

Sicurezza:

- Tcp/Ip: le porte delle applicazioni client/server
- Le porte aperte come potenziale minaccia
 - Come evitare i rischi
 - Navigazione sicura
 - Mail sicure
 - Firewall

Computer in rete, parti in gioco

Abbiamo appreso dalle precedenti lezioni che una rete di computer e' un sistema formato da entita' interconnesse tra loro (terminali, router, pc) identificate da indirizzi , detti indirizzi IP e sono **univoci**.

Il secondo strato che permette a tali entita' di scambiarsi informazioni e' dato dalle applicazioni client/server che comunicano tra loro grazie al protocollo TCP.

Parti esposte alle vulnerabilita'

Proprio lo strato TCP, e' quello che permette a due computer di comunicare tramite un meccanismo di tipo client/server.

Il client ed il server si accordano a comunicare aprendo entrambi una stessa "porta" (il protocollo TCP ne dispone 65000) di comunicazione.

Le porte vengono cosi' aperte e le applicazioni, quindi i computer, possono iniziare la comunicazione.

Parti esposte alla vulnerabilita'

Sono proprio queste porte aperte, la causa delle maggiori intrusioni che avvengono al giorno d'oggi nei computer.

Infatti mentre un tempo il rischio dei computer era soltanto legato alla diffusione dei virus (tramite scambio di floppy, cd, dati) adesso la rete globale, le e-mail rendono sia la diffusione dei virus piu' rapida, sia il rischio di intrusione in "porte aperte" piu' frequente.

Prevenzione

- Usare un sistema operativo intrinsecamente sicuro
- Proteggere sistemi insicuri con antivirus e firewall
- Evitare di tenere porte aperte inutilizzate
- Utilizzare applicazioni di connettività **sicure** ed **aggiornate**
- Evitare le procedure automatizzate

Usare un sistema operativo sicuro

Linux e' l'alternativa sicura a Windows. La sua struttura lo rende intrinsecamente sicuro e blindato a tal punto da non richiedere antivirus o antispy.

Una comunita' mondiale lo tiene aggiornato e protetto, ed ovviamente gratuito

I vantaggi della sicurezza di Linux derivano dal fatto che e' open-source

Proteggere il sistema

Nel caso in cui e' impossibile utilizzare sistemi intrinsecamente sicuri, bisogna prevenire i rischi frequenti quali virus e spyware o cavalli di troia:

- Installare un antivirus
- Installare un firewall
- Installare un antispay

Nell'esempio di Windows, un buon livello di sicurezza si e' ottenuto con l'ultimo Windows XP Service Pack 2. Versioni precedenti sono sconsigliatissime.

Utilizzare le giuste applicazioni

Applicazioni Open-Source sono la scelta ideale da seguire
(v. vantaggi open source):

- Internet: Mozilla Firefox
- Mail: Mozilla Thunderbird
- Ftp: Filezilla
- Office: Openoffice
- Web server: Apache
- Zip archiver: 7-zip

Evitare procedure automatizzate

Procedure che da sole automaticamente, sono autorizzate ad eseguire determinate operazioni sul sistema operativo, autonomamente, sono sconsigliatissime; un esempio è dato dai controlli ActiveX di Internet Explorer (pericolosissimi) e dalla abilitazione in Outlook delle mail in formato HTML.

Sessione Pratica

- Installazione Mozilla Suite
- Panoramica sul firewall di Windows
- Ambienti di navigazione sicuri (test browser appliance)
- Live Cd di Linux