

SICUREZZA IN RETE

panoramica sugli strumenti

A cura di:
Ing. Michele Mordenti

Forlì, 27 Marzo 2006



**In collaborazione con il
Comune di Forlì**

SOMMARIO

- Presentazione del FoLUG
- Software libero
- Password
- Firewall
- LOG/IDS
- Antivirus / Antispyware
- Parental Control

Presentazione del FoLUG

Forlì Linux User Group

- L'Associazione si propone di promuovere e diffondere la conoscenza e l'uso dei moderni strumenti telematici ed informatici, con particolare attenzione al "*software libero*"

<http://www.folug.org>

Software Libero

- 1) Libertà di utilizzo del software per qualsiasi scopo lecito;
- 2) Libertà di modificare il programma;
- 3) Libertà di distribuire copie, gratis o dietro pagamento;
- 4) Libertà di distribuire versioni modificate.

Hacker

- *Riabilitare la parola Hacker*
- Hacker: dall'inglese *To hack*, smontare - fare a pezzi. E' amante della tecnologia, di fatto l'ha creata:

Internet, GNU/Linux
modello etico innovativo

- Cracker:
chi penetra e rompe sistemi altrui.

Sicurezza del FLOSS

FLOSS: *Free/Libre Open Source Software*

- Software aperto:
stabilità, sicurezza e controllo del programma
- Software proprietario:
non sappiamo nulla su cosa faccia il
programma, il calcolatore è in mani altrui!

Spyware & Virus

La Sicurezza non è un prodotto

- La sicurezza non è un prodotto in vendita negli scaffali dei negozi.
- La sicurezza è un processo, un insieme di azioni, regole e comportamenti.
- Sicurezza inversamente proporzionale alla comodità di accesso al calcolatore.

Gestione delle password

- Cambiare frequentemente l'uso delle password (non più di tre mesi)
- Utilizzare Password robuste

Niente nomi propri, nomi di oggetti comuni (es. frutti, stagioni).
Usare almeno 8 caratteri alternando caratteri e numeri.

- Ordinare le password in base alla importanza del dato da proteggere

GNUPG

- Protezione della propria privacy
Cifrare elettronicamente i propri dati sensibili
Firmare digitalmente i documenti

<http://www.gnupg.org/>



Navigazione sicura

- Protocollo HTTPS

Inserire dati personali solo in pagine criptate.

- Posta elettronica sicura POP3S

Utilizzare protocolli criptati ove supportati dal proprio internet provider.

Sconsigliamo l'utilizzo dei prodotti Microsoft, come alternativa consigliamo:

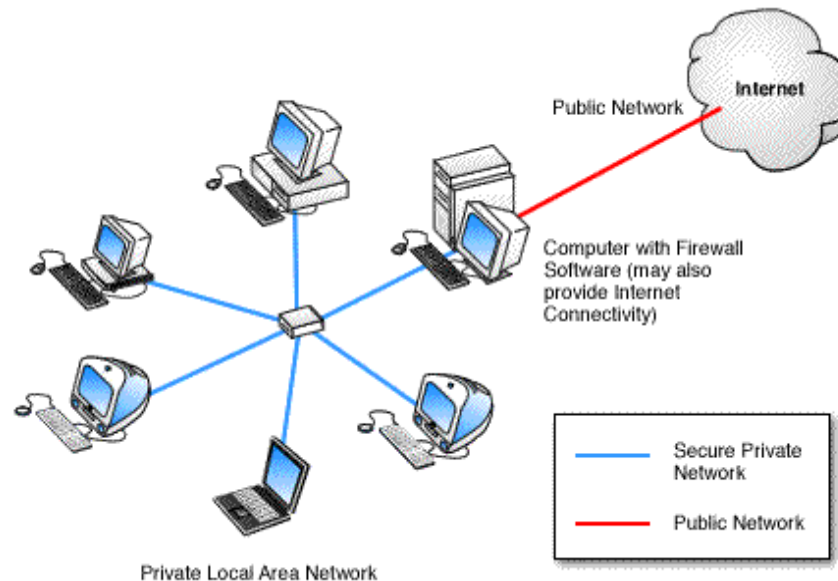
- Browser Web: Mozilla Firefox
- Posta elettronica: Mozilla Thunderbird



Firewall

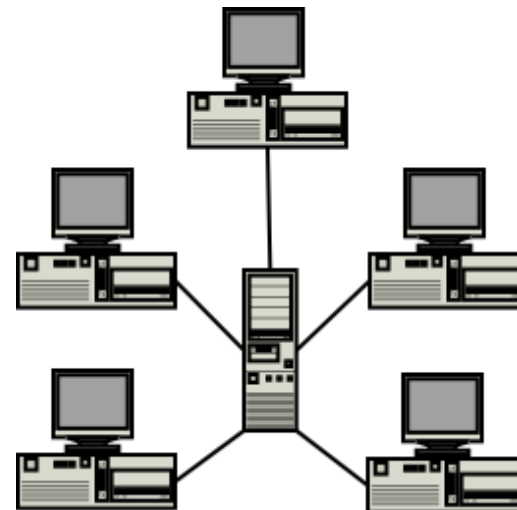


- Dotare di firewall il proprio calcolatore
proteggere le porte di comunicazione esterne



Disattivare servizi inutili

- Lasciare in esecuzione sul proprio elaboratore solo i servizi di rete strettamente necessari.



Antivirus



- Dotare di antivirus il proprio calcolatore
proteggere l'esecuzione di software maligno in ambiente
Windows

- Antidoto:

ClamAV (software libero)



<http://www.clamav.net/> - <http://www.clamwin.com/>

in alternativa

Antivir: gratuito per uso personale

<http://www.free-av.com/>

SPYWARE

- Gli spyware sono software che inviano segretamente informazioni sull'utente.

Forma comune di finanziamento del software
freeware/shareware

- Antidoto: **spybot** (free software)

<http://www.safer-networking.org/>

in alternativa

ad-aware: gratuito per uso personale

<http://www.lavasoftusa.com/software/adaware/>

LOG / IDS

- Controllare periodicamente i LOG di sistema per scoprire eventuali anomalie
- Intrusion Detecting System: analisi approfondita del sistema per la ricerca di **rootkits**



Parental Control

- Ad oggi non esiste un software al quale delegare l'educazione del minore
- Filtri che agevolano il controllo, ma nessuna garanzia di funzionamento al 100%
- Non esiste la sicurezza assoluta, in base alla valutazione del pericolo si procede di conseguenza

Metodi di filtraggio tramite PROXY

- **WHITELIST**

Si imposta il proxy per navigare esclusivamente su siti accreditati (A volte chiamato “*metodo della biblioteca di casa*”).

- **BLACKLIST**

Si imposta il proxy per navigare ovunque tranne che su alcuni siti noti.

Generalmente si implementano soluzioni proxy per reti di calcolatori.

Proxy OpenSource: SquidGuard e DansGuardian



Metodi di filtraggio dinamico

- Esistono software che effettuano il filtraggio dinamico

Problema della accuratezza:

mancato allarme e/o falsi positivi.

ESEMPI: NAOMI (freeware)

<http://www.radiance.m6.net/italian.html>

Notizie utili su:

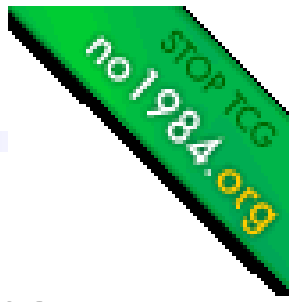
<http://www.ilfiltro.it>

<http://www.davide.it>

Buon Senso

- Ancora una volta: utilizzare sempre il buon senso e non farsi prendere o da paure ingiustificate o da falsi sensi di sicurezza
- Tenere sempre un comportamento sobrio anche in rete
- Non lasciare soli i bambini (davanti al PC, come davanti alla TV come per strada)
- Internet riflette la nostra società, nel bene e nel male. Non demonizzarne l'utilizzo

Trusted Computing



- Consorzio di produttori Hardware/Software per creare una piattaforma sicura

Sicura per chi?

- Non siete voi a decidere quali programmi far eseguire al vostro elaboratore, ma le industrie scelgono per voi
- Il PC non è più sotto il vostro controllo
- Tecnologia inutile per filtrare il contenuto delle pagine web

<http://www.no1984.org>

SICUREZZA IN RETE

...FINE

Contatti: Ing. Michele Mordenti

e-mail: michele.mordenti@tin.it

web: <http://xoomer.virgilio.it/michele.mordenti>

FoLUG: <http://www.folug.org>

Il materiale presentato è rilasciato su licenza Creative Commons



Attribution



Share-Alike



Non-Commercial