LA SICUREZZA DELLE RETI: LE VULNERABILITA'

27 marzo 2007

Fondazione Ordine degli Ingegneri di Milano
Corso Venezia

Relatore Ing. Sommaruga Andrea Guido

presentazione realizzata con OpenOffice

http://www.openoffice.org/

sommaa@stcom.com

Le informazioni digitali devono fare quotidianamente i conti con il loro mondo virtuale pieno di insidie.

Anche per i bit abbiamo bisogno di porte, sistemi di sicurezza, guardiani...

sommaa@stcom.com

L'infrastruttura informatica oggi deve essere:

- **Sicura**
- **Affidabile**
- **Disponibile**

Un aspetto fondamentale, spesso sottovalutato, è la sicurezza fisica degli apparati in particolare modo server ed apparati di rete.

sommaa@stcom.com

La sicurezza si ottiene con:

- **Misure fisiche**
  (gruppo continuità, locali blindati ...)
- **Misure logiche**
  (istruzione agli utenti, diritti ...)
- **Strumenti software**
  (firewall, IDS, antivirus ...)
- **Analisi dei LOG e monitoraggio**

sommaa@stcom.com

L'affidabilità si ottiene con:

- **Qualità delle attrezzature**
- **Aggiornamento periodico Hardware**
- **Manutenzione preventiva (aggiornamenti software)**
- **Eliminazione singoli punti di guasto (dischi in RAID, server in mirror ...)**

sommaa@stcom.com

La disponibilità è una diretta conseguenza di sicurezza ed affidabilità.

Una rete sicura è meno soggetta a fermi causati da virus, attacchi e problemi di configurazione.

Una rete affidabile è meno soggetta a fermi dovuti a guasti hardware.

Sicurezza ed affidabilità sono un costo!

sommaa@stcom.com

Al crescere della dimensione dei sistemi cresce la complessità delle difese.

sommaa@stcom.com

Singolo PC isolato dal mondo internet

In questo caso la protezione della macchina è molto semplice:

- **Gruppo di continuità**
- **Backup dei dati**
- **Antivirus per controllo Floppy, CD ecc.**

I virus abitano anche nelle memorie USB

sommaa@stcom.com

Rete di PC isolata dal mondo internet

La protezione della rete cresce in complessità:

- **Gruppo di continuità (per tutte le macchine)**
- **Certificazione cablaggio di rete (spesso trascurato e causa di guai)**
- **Backup dei dati (di tutte le macchine,più complesso)**
- **Antivirus residenti su tutta la rete**
- **Limitazione ai diritti degli utenti**

sommaa@stcom.com

Gli utenti lavorando sui loro calcolatori possono:

- Danneggiare/cancellare dati condivisi (Errori: backup, Virus: antivirus)
- Installare software non funzionante (verifica periodica software installato)
- Collegare alla rete dispositivi che la danneggiano o ne provocano blocchi (IP duplicati, apparati che disturbano)

sommaa@stcom.com

I server devono quindi essere protetti con:

- **Antivirus**
- **Backup**
- **Autorizzazioni agli utenti**
- **Analisi dei log**
- **Attività di monitoraggio**

sommaa@stcom.com

Il mondo Internet

Una rete locale isolata dal mondo deve proteggersi solo da eventi interni.

Una connessione verso Internet è una seria minaccia per la sicurezza della rete: devo proteggermi anche da attacchi esterni.

sommaa@stcom.com

...ma sulla mia rete non c'è nulla da rubare...nulla da nascondere....

Errore: la mia rete è soggetta ad attacchi per i più svariati motivi....anche solo per prova da parte di persone che si allenano.

In qualsiasi caso devo proteggere la mia identità: è una cosa che, ad alcuni, può interessare molto

sommaa@stcom.com

Rete di PC collegata al mondo internet

Per difendere la rete dal mondo internet devo aggiungere alle protezioni:

- **Firewall per proteggere la rete dagli attacchi esterni**
- **Backup dei log di accesso ad internet (oltre ai dati!)**
- **Analisi dei log di accesso ad internet**
- **Antivirus ed antispam**

sommaa@stcom.com

La rete deve essere protetta con un Firewall ovvero una barriera che protegge la rete dagli attacchi esterni.

La configurazione del firewall è una fase critica: un firewall mal configurato è praticamente un dispositivo inutile.

Non basta installare il firewall per essere protetti ma si deve fare manutenzione e verificare i LOG.

sommaa@stcom.com

Tipi di firewall

Firewall software a livello personale (programma da installare sul PC)

Firewall software o hardware a livello di rete

sommaa@stcom.com

Firewall software sul PC

Vantaggi:

- utile per proteggere un solo PC connesso ad internet con un modem
- se ben configurato offre informazioni utili anche alla diagnosi di problemi

Svantaggi:

- rallenta il PC
- raramente è configurato bene
- scarsa efficacia
- necessità di istruire gli utenti

sommaa@stcom.com

Firewall di rete

Vantaggi:

- gestione centralizzata
- non richiede software sui PC
- non richiede formazione agli utenti

Svantaggi:

- difficile da configurare
- richiede manutenzione continua (aggiornamenti e verifica log)

sommaa@stcom.com

IDS (Intrusion Detection System)

E' un dispositivo di analisi delle intrusioni, consente di identificare accessi non autorizzati alle reti.
E' un dispositivo di monitoraggio complesso da configurare, oneroso da mantenere e che richiede una costante analisi dei LOG.
E' idoneo a strutture di grande dimensione.

sommaa@stcom.com

Wireless.....

Nel caso di reti senza fili devo ricordarmi che, oltre ai rischi precedentemente illustrati si deve aggiungere il rischi legato al mezzo di trasporto.

L'etere non offre protezione ai dati quindi è necessario attivare tutti i meccanismi di autenticazione previsti dagli apparati in uso.

sommaa@stcom.com

Wireless

vantaggi:

- **Economica da installare, non richiede cavi**

svantaggi:

- **velocità inferiore al cavo**
- **difficoltà di protezione**
- **vulnerabilità a disturbi esterni**
- **molto rischioso se mal configurato**

sommaa@stcom.com

ADSL, FASTWEB e banda larga

Oggi c'è disponibilità di connessioni ad internet a banda larga a costi ragionevoli.

La configurazione base degli apparati come installati dai provider, anche se sono le grosse compagnie telefoniche, spesso è insicura.

.....

sommaa@stcom.com

FASTWEB

Fastweb usa portare, per le configurazioni di tipo domestico, degli apparati chiamati HAG a cui si collegano direttamente i PC.
Questa connessione non offre protezioni dal mondo Fastweb.

Il PC è raggiungibile facilmente dagli altri utenti FASTWEB collegati alla stessa rete.

sommaa@stcom.com

ALICE e connessioni ADSL

Le offerte commerciali di ADSL con fornitura di un solo modem ADSL a cui connettere il PC, non offrono alcun tipo di protezione.

Un PC, o peggio un server, collegato ad un modem ADSL è costantemente esposto ad INTERNET ed è difeso solo dal suo sistema operativo e dalle password se l'utente le ha assegnate.

sommaa@stcom.com

P2P

La sigla indica Peer To Peer, ovvero una rete basata su tanti nodi tra loro equivalenti (peer). Nasconde tutto un mondo legato ad internet che consente di fare degli scambi di file (musica, film e virus a volontà)

Se si vuole mantenere un minimo di sicurezza nella rete qualsiasi software per il P2P, (come winmx, emule ecc...) deve essere vietato

sommaa@stcom.com

Shareware, freeware ecc.

E' molto semplice scaricare software da internet.

Installare software di incerte origini o peggio software dal quale sono state rimosse le protezioni, può essere una seria minaccia per la sicurezza della rete.

I programmi possono contenere codice malevolo (trojan) o aprire porte esterne (back door).

sommaa@stcom.com

In conclusione, per un minimo di sicurezza occorre:

- connessione internet solo con router
- attivare le eventuali funzioni di firewall del router
- controllare i log del firewall (l'assenza di tentativi di intrusione non è un buon segno!)
- installare e mantenere aggiornato l'antivirus
- mantenere aggiornati i sistemi operativi ed il software utilizzato

sommaa@stcom.com

Sicurezza reti: La Licenza

Come tutte i documenti anche questa presentazione è coperta da licenza d'uso:

Copyleft 2007 – Ing. Sommaruga Andrea Guido

è garantito il permesso di copiare, distribuire e/o modificare questo documento seguendo i termini della **Licenza per Documentazione Libera GNU**, Versione 1.2, oppure ogni versione successiva pubblicata dalla Free Software Foundation;

- senza Sezioni Non Modificabili
- senza Testi Copertina
- senza Testi di Retro Copertina
- Mantenendo intatte il riferimento all'autore originale del documento

la versione originale in inglese della licenza è disponibile su www.gnu.org/copyleft/fdl.html