Corso Di Linux

Liceo Fermi, Bologna - Marcello Galli, novembre 2009

Internet e sicurezza

La sicurezza assoluta in informatica non esiste, e' tutto diventato cosi' complicato che programmi con errori, che diano problemi di sicurezza, ce ne sono sempre in ogni computer; forse non e' esagerato affermare che l'unico computer assulutamente sicuro e' quello spento, rotto e con gli hard disk smagnetizzati. Pero' non bisogna scoraggiarsi, ed un po' di attenzione e buon senso possono proteggervi dalla maggior parte dei pericoli.

L'uso di internet e la sicurezza informatica sono 2 argomenti collegati. Una volta, quando internet non c'era, i problemi di sicurezza erano legati alla possibilita' di prendere virus da programmi scambiati su floppy disk, ed i problemi di sicurezza in rete erano appannaggio dei server.

Ora che tutti sono in rete, i problemi vengono dalla rete, e la possibilita' di infettarsi scambiando dati su supporti rimuovobili e' limitata ad alcuni virus che infettano le chiavette usb. Un programma con bachi, che lavora in rete, puo' permettere ad un malintenzionato di entrare nel vostro computer dalla porta che tiene aperta per offrire i servizi ai suoi clienti. I computer sono sempre piu' integrati in rete ed i programmi che lavorano tramite la rete sono ormai tanti, e non sempre il proprietario del PC sa quali porte sono aperte. Anche certi virus aprono porte di rete nel computer (dette backdoors) per permettere al nemico di entrare.

In Linux il problema dei virus non esiste, la fonte piu' grossa di pericolo sono quindi gli errori nei programmi che lavorano in rete. Una PC Linux ha praticamente lo stesso software di un server, e quindi vi trovate a gestire le stesse problematiche di sicurezza di un server aziendale. In una macchina Linux ci sono molte piu' cose da badare che in Windows. Ma Windows, con la sua vulnerabilita' ai virus, le tecnologie insicure connesse ad Internet Explorer e i molti servizi di rete dal comportamento oscuro, e' quello che ha piu' problemi di sicurezza

Il problema della sicurezza e' un problema grave, non va sottovalutato. Rimettere a posto un computer infettato vi costa ore di lavoro; i dati che avete nel computer possono andare perduti, o essere rubati. Un computer violato non e' piu' sotto il vostro controllo, puo' essere usato, a vostra insaputa, per commettere veri e propri crimini; come violazioni di siti web, attacchi a computer governativi o di banche, attacchi tipo "denial of services", il computer puo' essere usato magazzino e negozio di porcherie varie, per furto di password, per furto di numeri di carte di credito, raggiri e truffe varie, invio di spam in modo massiccio, ma sopratutto puo' essere utilizzato per quello che sembra essere oggi il crimine peggiore di tutti, e quello piu' severamente perseguito: andare contro gli interessi dell'industria della musica e del cinema distribuendo gratis loro materiale. In questo caso e' possibile che la finanza venga da voi, i padroni del computer, e vi troviate ad avere problemi e spese legali non indifferenti per dimostrare che il colpevole e' qualcun'altro.

Ma non bisogna neanche essere fanatici della sicurezza; esagerare con la sicurezza e' dannoso. Piu' un computer e' *sicuro* piu' lavoro di gestione e manutenzione richiede, e peggio ci si lavora. Spesso poi si esagera con gli strumenti di sicurezza e si dimenticano delle cose elementari, di buon senso.

Una buona politica di sicurezza e' basata sulle conoscenze, sulla consapevolezza e sul buon senso. La sicurezza e' un metodo, non un prodotto; non e' comperando prodotti per la sicurezza che rendete sicuro il vostro PC, ma facendo le cose giuste.

La mia politica di sicurezza si puo' riassumere in 3 punti:

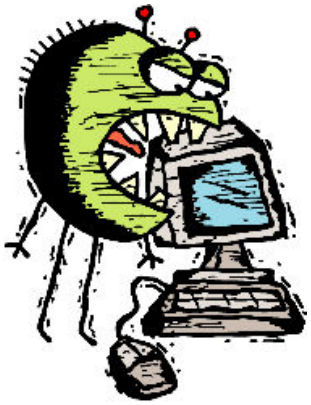
1. *conosci il tuo nemico* : per proteggersi bisogna sapere da cosa e da chi ci si deve proteggere; conviene quindi farsi un'idea di chi e' il possibile attaccante. Questo dipende da cosa avete di appetibile nel PC e da come siete connessi alla rete. Un modo che usano i professionisti per fare questa analisi e' collegare in rete una macchina senza nulla dentro, ma che registra gli attacchi (queste macchine si chiamano honeypot), e vedere cosa accade. Anche senza mettere su un honeypot, si puo' avere un'idea della situazione tenendo d'occhio i files di log, che registrano quello che succede nel computer. Configurateli in modo da vedere i tentativi di accesso dalla rete e teneteli d'occhio.

2. *conosci il tuo computer ed i tuoi utenti* : bisogna sapere cosa si deve proteggere, quali servizi di rete sono attivi sul computer e cosa combina chi lavora sul computer. Un computer e' piu' vulnerabile da *dentro* che da fuori, se poi i vostri utenti commettono ingenuita' come usare il loro nome come password il vostro sistema diventa molto vulnerabile.

3. *fai il meno possibile, ma con pignoleria* : una volta capita bene la situazione, in relazione ai *veri* pericoli cui siete esposti, va implementato il minimo indispensabile alla sicurezza del sistema, ma con estrema pignoleria. Inutile implementare misure di sicurezza se ve ne ricordate un giorno si' ed un giorno no.

Oltre a questi punti io cerco sempre di sapere cosa succede nel computer, e monitorizzo la situazione, tramite i files di log. Questo serve anche indipendentemente dalla sicurezza, per correggere errori di configurazione e prevenire malfunzionamenti.

Un ultima raccomandazione e' di fare sempre dei backup (copie di sicurezza). Fanno piu' danni i guasti hardware o gli utenti pasticcioni degli hacker e dei virus. **Fate i backup**. Oggi gli hard disk esterni, i DVD e le chiavette usb costano poco.



Classifica dei pericoli

L'industria della sicurezza ha generato una variegata nomenclatura e classificazione per tutti i tipi di problemi e di attacchi, ma per i nostri scopi possiamo esemplificare i rischi in 3 categorie:

- Virus: sono programmi malevoli che eseguiti sul vostro computer fanno danni, aprono porte etc. Questi programmi si replicano, copiandosi via rete, attaccandosi ad altri programmi, attaccandosi al programmino che hanno tante chiavette usb per farsi riconoscere da Windows e in altri modi, per cui il contagio si propaga ad altri computers. Per questo si chiamano virus.

Il problema e' praticamente inesistente per i sitemi Linux. Infatti gli utenti normali hanno privilegi limitati (spesso questo non accade su Windows), un virus "preso da un utente" puo' fare danni solo a lui e non infetta il sistema. Inoltre Linux e' poco amato dai creatori di virus perche' ancora senza grande diffusione fra i PC.

Il problema dei virus (ed il mercato dei programmi anti-virus) e' stato generato essenzialmente da alcune scelte architetturali della Microsoft, fatte per ragioni di facilita' d'uso e di mercato, che dal punto di vista della sicurezza sono delle vere follie. I problemi sono essenzialmente 2:

- cliccare su un allegato di posta lo esegue, se questo e' un programma;
- e' possibile, cliccando su pagine web, eseguire un programma sul computer (tecnologia delle pagine ASP).

In questo modo si autorizza qualcosa che arriva dall'esterno, e non e' affidabile, ad eseguire un programma sul computer. La cosa e' stata un po' mitigata dalle ultime versioni di Windows, ove di default si chiede all'utente cosa vuole fare in questi casi, ma il problema resta.

Inoltre la Microsoft si cura poco della sicurezza, vengono distribuite poche correzioni di sicurezza; ci sono siti internet che elencano numerosi problemi di sicurezza cui la Microsoft non ha mai messo rimedio. Altro problema e' che solo la Microsoft puo' fare correzioni di sicurezza ai suoi prodotti; il source non e' disponibile e come e' fatto il suo software e' segreto. Per cui quando la Microsoft decide di smettere di supportare un suo vecchio software dovete per forza comperare il suo prodotto nuovo, oppure vi riempite di virus.

Un grosso problema e' Internet Explorer, conviene preferire altri borowser ad Internet Explorer, specie se si visitano siti inaffidabili, come siti di hacker, roba piratata o siti porno. Questi siti sono noti per ospitare pagine truccate, con codici malevoli. Problemi possono sorgere anche visitando siti noti e normali; si e' verificato che banner pubblicitari fossero fatti in modo da creare problemi; i banner vengono distribuiti in modo automatico da ditte specializzate, sono fatti dal cliente, non sono controllati dal sito che li ospita e ve li fa vedere e neanche da chi li distribuisce.

Ovviamente se usate un browser diverso da Internet Explorer dovete preoccuparvi di tenerlo aggiornato. Programmi complicati come un browser web spesso hanno bachi e spesso sono bachi legati alla sicurezza. Le nuove versioni correggono i bachi anche prima che qualcuno trovi il modo di approfittarne, ma le dovete installare. Le distribuzioni Linux distribuiscono patch (correzioni) di sicurezza per i browser inseriti nella distribuzione, e fanno le correzioni in modo semiautomatico. Su Windows dovete ricordarvi voi di aggiornare il browser.

Questo problema dei virus obbliga oggi tutti i possessori di PC con windows ad avere un programma antivirus aggiornato. E' come una tassa, che chi usa Windows deve pagare.

I programmi antivirus essenzialmente analizzano i possibili virus confrontandoli con un elenco di virus noti. L'elenco deve essere aggiornato, altrimenti l'antivirus riconosce solo i virus datati e non i nuovi usciti. Molta gente compera l'antivirus e poi dimentica di aggiornarlo, con ovvi risultati.

Un antivirus analizza tutti i programmi che "entrano" nel computer ed aiuta. Ad ogni modo, se usate Windows dovete fare attenzione a:

- non aprire allegati di posta di provenienza non fidata.
- controllate con l'antivirus giochi, programmi e tutto quello che non arriva direttamente dal produttore. Specie la roba craccata da problemi.
- state attenti ai siti internet che visitate, non cliccate su banner poco fidati.

- Attacchi dalla rete. Come gia' detto programmi che lavorano in rete, possono presentare problemi che aprono la strada ad attacchi e permettere a programmi malevoli di penetrare nel vostro computers, o ad hacker cattivi di impadronirsi del vostro computer, per usarlo (via rete) ai loro fini.

  Questo problema interessava poco le vecchie versioni di Windows, che avevano una interazione con la rete molto limitata. Con Windows XP le cose sono cambiate, e adesso anche Windows ha problemi con questo tipo di attacchi. I servizi che operano in rete sono ormai tantissimi e spesso l'utente non sa neanche quali sono e cosa fanno. Quelli che non servono andrebbero disattivati. In Linux vedete le porte aperte ed i programmi che le usano con il comando netstat.

  Qui aiuta un firewall; un firewall e' un programma che controlla l'accesso alle porte del vostro computer; un firewall puo' anche essere su un router e controllare l'accesso alle porte di tutta una rete. La maggior parte dei firewall prendono le loro decisioni in base ai numeri IP ed ai numeri di porte, per cui decidete voi che macchina accede a quali servizi. Alcuni firewall vanno anche a vedere dentro i pacchetti di rete, ad esempio per bloccare pacchetti che contengano certe parole. Per configurare correttamente un firewall dovete sapere quali porte di rete usano i servizi che utilizzate. Un firewall mal configurato non aiuta molto.

  Sotto Linux il modo migliore per evitare problemi da servizi di rete e' tener aggiornato il sistema. Tutte le distribuzioni forniscono correzioni di sicurezza per il software che includono ed hanno metodi semiautomatici per installarle. Le correzioni di sicurezza **devono** sempre essere applicate. Ne escono tutte le settimane. Sotto Linux il programma sorgente e' libero e i professionisti della sicurezza cercano sempre di trovare i bachi, per farsi pubblicita', per cui ci sono sempre molte correzioni ai bachi, la maggior parte dei quali non potrebbero mai portare ad un modo di fare un vero attacco ai computers. Applicare le correzioni di sicurezza su Linux vi protegge dal 90% dei possibili attacchi, se non di piu'. Quasi tutti gli attacchi sono fatti in base a bachi vecchi, gia' noti e corretti.

  Se nel vostro sistema Linux avete del software che non fa parte della distribuzione dovete badare voi a tenerlo aggiornato, andando ogni tanto sul sito del produttore a controllare se ci sono aggiornamenti.

  Anche Windows rilascia qualche correzione di sicurezza, ad anche quelle vanno installate regolarmente

- Ingenuita' degli utenti. Potrebbe non sembrare ma e' un grosso problema. Gli utenti ne fanno di tutti i colori per favorire i malintenzionati;

  - poca cura delle passwords. E' comune avere password banali, lasciate scritte qua' e la', dare in giro le password senza controlli, tenere la stessa password per anni. Oppure capita che malintenzionati si facciano dare la password per telefono, facendosi passare per funzionari importanti o tecnici del computer.

    In Linux la password e' criptata, e viene criptata usando alcuni dei suoi stessi bytes come chiave. In questa forma e' scritta nei files di configurazione in /etc (in /etc/passwd od in /etc/shadow). Quando uno si collega, e da la password, il computer la cripta e la confronta con quella, criptata, nei files di cui sopra. Una password non puo' quindi essere decriptata e non viene mai decrittata, solo criptata. Nenache l'utente root sa le passwords, puo' cambiarle, ma non scoprire quali sono. L'unico modo per scoprire la password e' rubarla, oppure provare tutte le combinazioni di lettere e numeri fino a che non la si indovina. Quando i computer erano lenti si usavano password di 6 lettere ed era impossibile provare tutte le combinazioni di 6 lettere in un tempo ragionevole. Ora i computer sono molto piu' veloci ed una password corta puo' essere trovata in un tempo accettabile; adesso si dice che le password devono essere di almeno 8 caratteri, ed avere lettere minuscole, maiuscole, caratteri strani e numeri dentro.

I programmi che cercano di indovinare le password si aiutano anche con un vocabolario, facendo varianti a parole del vocabolario. Una buona password deve quindi avere queste caratteristiche:

  * essere lunga, diciamo almeno 8-10 caratteri;
  * non essere ricavabile da parole del vocabolario. Tanto meno dal vostro nome o cognome.
  * dopo qualche mese andrebbe cambiata.

– poca cura del computer e dei dati: spesso il PC viene lasciato acceso, con l'utente collegato, in un luogo aperto al pubblico. I browser hanno la brutta abitudine di facilitarvi il lavoro, ricordando passwords, siti visitati e quant'altro. Conservano anche in una loro memoria su disco (cache) le pagine visitate. Anche altri programmi, per aiutarvi, si ricordano le password. **Non si lasciano dati riservati nel computer**, a meno che non siate sicuri di chi accede al computer. Quindi svuotate le cache dei browser dopo l'uso e scollegatevi quando lasciate la vostra postazione.

  Tenete presente che non potrete mai proteggervi dalla donna delle pulizie; ovvero chi ha accesso fisico al computer puo', in un modo o nell'altro, leggere o modificare quello che c'e' scritto dentro. Lo stesso discorso vale per chi ha accesso ai backup. L'unico modo di proteggersi da chi ha accesso fisico al computer e' criptare i dati del disco fisso. E' una procedura complicata, che comporta la perdita completa dei dati quando vi dimenticate la password. Ma neanche questo e' sicuro (vedi figura sotto).

– Gli utenti sono spesso creduloni: girano mail con le storie piu' assure in rete: promesse di facili guadagni, catene di S.Antonio, richieste di controlli di conti bancari, inviti a visitare certi siti internet con le scuse piu' varie, alcune di queste truffe sono scritte anche in pessimo italiano, ma sembra che ci sia sempre qualcuno che ci casca.

– Gli utenti caricano sul computer le cose piu' disparate, senza controllarle. Un ottimo modo di caricarsi di virus.

– gli utenti non fanno mai copie di backup del loro lavoro, in questo modo un guasto od una disattenzione bastano per perdere ore di lavoro.

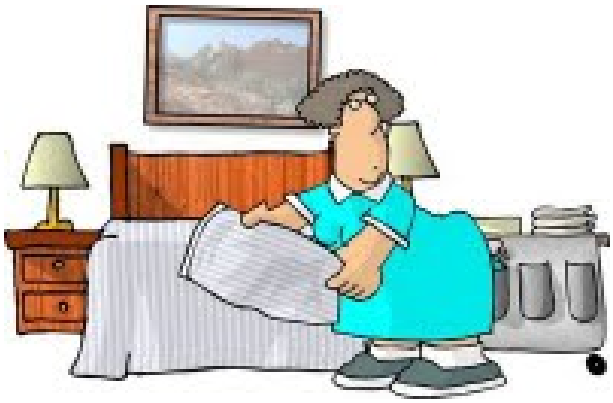


Figure 1: La donna delle pulizie malvagia, che ruba i dati anche da un disco criptato, vedi http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html

Nomenclatura

Anche se abbiamo schematizzato i pericoli in 3 grandi categorie un po' di nomenclatura non guasta; vediamo alcuni tipi di programmi malevoli e cosa fanno:

- Virus e Worm: un virus e' un software che fa danni, ed in piu' e' in grado di replicarsi, copiandosi dentro altri programmi, il boot sector o in altri posti. Alcuni scrivono perfino nel BIOS. I virus cercano di camuffarsi per non farsi scoprire, a volta aprono porte nel PC (backdoors) per far entrare i nemici, oppure mandano al loro padrone i vostri dati, i vostri files con le password etc. Ce ne sono alcuni che infettano le macro istruzioni di Office, e quindi i documenti, quando uno li apre office esegue automaticamente le macro e si infetta. Worm e' un virus che utilizza la rete per replicarsi, la distinzione ormai e' poco significativa, quasi tutti i virus moderni sono dei worm

  Sono famosi attacchi di virus che hanno fatto milioni di vittime, con vere e proprie epidemie, vediamo alcuni esempi:

  - nel 2000 il famoso virus "I Love You" , infettava la posta. Quando una apriva il mail infetto il virus veniva eseguito da Outlook automaticamente, e mandava mail con copie di se stesso a tutta la rubrica della posta (un grosso difetto di Outlook).
  - nel 2001 il virus "Code Red" infetto' in 14 ore, circa 400.000 web servers. Sfruttava un baco del server web della Microsoft, corretto il mese prima dalla Microsoft. Ma molta gente non aveva applicato la patch.
  - il virus Nimda si propagava in un sacco di modi diversi, anche via rete, sempre del 2001, infetto' almeno 100.000 macchine. Anche questo sfruttava un baco del server web della Microsoft; la rete era piena di attacchi, nell'autunno del 2001 osservavo alcune migliaia di attacchi al giorno sulle mie macchine Linux. Se uno installava il sistema della Microsoft, appena si collegava in rete per scaricare ed applicare la patch di sicurezza era infettato e doveva ricominciare da capo. Macchine infette hanno continuato a mandare in giro questo virus per anni. Si vede che molti controllano poco le loro macchine.
  - Slammer e' del 2003, sfruttava un baco del programma SQL server della Microsoft gia' corretto da 6 mesi. Infetto' 75.000 computers in 10 minuti.
  - Nel 2004 ci sono stati Sasser e MyDoom; MyDoom mandava migliaia di mail di posta infetti, velocissimo, ed apriva una backdoor nel computer. Sasser si propagava via rete e sfruttava un baco di Windows, nel programma che controllava gli utenti per l'accesso ai servizi di condivisione files e stampanti (porta 445); il baco era stato corretto 17 giorni prima dalla Microsoft. L'autore del virus era un ragazzo tedesco, che e' stato arrestato.
  - Nel 2008 c'e' Conficker, che sembra abbia infettato 5-10 milioni di computers. Sfruttava un baco dei servizi di rete di Windows (anche per questo problema la Microsoft aveva rilasciato una patch). Varianti di questo virus hanno continuato a circolare anche nel 2009.

- Denial of service (DOS) : attacchi al computer (in genere) che provocano l'interruzione di un servizio (per sovraccarico ...).

  E' praticamente impossibile difendersi da uno di questi attacchi, bisogna limitare l'accesso ai servizi attaccati, ma in questo modo, per difenderli, li si rende inutilizzabili. Alcuni di questi attacchi utilizzano computer 'zombie', organizzati in una 'botnet'. Cioe' prendono il controllo di un certo numero di computers nel mondo, collegati ad internet con reti veloci, li controllano con un programma automatico che li usa tutti insieme per fare l'attacco.

- Trojan Horses: programmi che creano "aperture" in un sistema che permettono di entrarci da fuori (aprono porte di rete), famoso "back orifice"; si propagano un po'

come i virus, ma restano nascosti, si stima che back orifice abbia infettato gran parte dei PC in rete.

- Spam mail: pubblicita' indesiderata, inviata in modo automatico ad un numero enorme di indirizzi, talvolta contiene virus o cose analoghe.
- Spyware: software che spia l'utente di un sistema e poi invia informazioni fuori senza chiedere autorizzazione. Alcuni software commerciali contengono software di questo tipo; dicono anche Windows XP ne contenga. Ci sono programmi appositi per rimuoverli. Questi non sono proprio virus, per cui i programmi antivirus non li scoprono.
- dialers: il navigatore internet disattento e' indotto, da indicazioni non chiare, a cliccare su una pagina in modo da attivare un programma che stacca la connessione internet e ricollega la macchina ad un numero telefonico a pagamento. Adesso che si usa l'ADSL per collegarsi, e non le normali telefonate, il problema e' meno grave, ma ci sono persone che si sono travate bollette telefoniche di migliaia di euro senza sapere perche'.
- rootkit: e' un virus che si rende invisibile, camuffando i camandi che si danno alla macchina ed alterandoli. Su Linux puo' essere ad esempio realizzato come un modulo del kernek, che cambia comandi come 'ls', 'top', 'ps', in modo che il virus non si veda.
- man in the middle: e' un attacco complicato, che serve ad intercettare i dati in una connesseione criptata. Un computer si mette in mezzo fra i 2 computer che comunicano, e fa credere ad ognuno di loro di essere lui il partner nella comunicazione. In questo modo cattura le chiavi per decifrare la comunicazione e legge tutto quello che viene trasmesso.

Consigli per i naviganti

- Attivita'
  - Cercate di essere utenti attivi di Internet e non semplici fruitori passivi, utilizzatela consapevolmente per distribuire i vostri lavori, farvi conoscere e diffondere le vostre idee. E' questo il suo lato interessante. Il software, ed in particolare le tecnologie legate alla rete si stanno sviluppando adesso; c'e' spazio per contribuire per chiunque abbia voglia di fare dell'informatica.
- Etichetta
  - essere corretti e cortesi: dall'altra parte del filo in genere c'e' una persona come voi.
  - Non utilizzate o diffondete materiale che non e' vostro, se diffondete materiale di altri citate l'autore.
- Privacy
  - In rete non si e' anonimi, si e' sempre rintracciabii.
  - Internet cambia il concetto di privacy, siamo diventati pubblici, adattiamoci e cerchiamo di sfruttarne i vantaggi.
  - Quello che mettete in internet e' fuori del vostro controllo, e' come se ormai appartenesse al mondo.
  - Dati riservati non vanno diffusi e non vanno lasciati in giro.
- Affidabilita'
  - Nulla che arrivi dalla rete e' affidabile:

    - facile falsificare dati digitali
    - diverse situazioni mettono in luce aspetti diversi delle persone
  - Siti illegali sono pericolosi
  - Servizi gratuiti non sono garantiti; non dovete dipendere da essi
- Limiti
  - La rete e' inadatta ad esprimere il lato affettivo delle persone. Gli amici conviene, se possibile, cercarseli nella vita reale.
  - Non siamo fatti per vivere davanti ad un video, non bisogna esagerare con la TV ed i computers, sono un bello strumento, molto utile, ma non del tutto a misura d'uomo.