SICUREZZA

Quick Reference guide
Guida di riferimento rapido

Soft.Com

Indice Generale

1. Introduzione....4
2. Sicurezza Informatica....5
2.1 Il problema....5
2.2 Il personal computer....5
2.3 Scenari....6
2.4 Virus & C....6
2.5 ...e Allora ??....8
2.6 Autenticazione e Diritti....9
2.7 La Password....10
2.8 Cambiare la password in Windows....11
2.9 I sistemi Windows....11
2.10 Scelta delle Applicazioni....12
2.11 Tenere aggiornato il sistema....13
2.12 Backup dei Dati....14
2.13 Assegnazione dei Diritti Utente....15
2.14 Antivirus....16
2.15 FireWall....17
2.16 Allora....18
3. Licenza Creative Commons....19

1. Introduzione

Lo sviluppo recente delle reti di comunicazione a livello mondiale (Internet in primis, ma non solo) ha portato all'attenzione generale problemi che solo cinque o dieci anni fa sarebbero sembrati di nulla o scarsa importanza. Stiamo vivendo in un'epoca in cui sta assumendo una importanza cruciale un elemento facile da indicare, ma estremamente difficile da definire con esattezza: l'"**informazione**". Se ci riflettiamo un attimo, tutto intorno a noi è "informazione": i nostri dati anagrafici, le nostre preferenze, le storie della nostra vita, il lavoro di tutti i giorni, la televisione, la scuola etc. Si obietterà che questo è stato sempre vero, da che mondo è mondo. Giusto, ma mai come in questo momento l'"informazione" può essere scambiata, trasferita ed archiviata con velocità impensabili solo qualche anno fa.

I vantaggi di queste tecnologie sono sotto gli occhi di tutti, e non è il caso di parlarne. Piuttosto queste brevi note servono ad evidenziare i problemi che tutto questo comporta quando usiamo il Personal Computer; ci permetteremo inoltre di fornire qualche semplice consiglio che riteniamo utile per evitare conseguenze spiacevoli ed ore di lavoro perse per tentare di rimediare. Buona lettura.

2. Sicurezza Informatica

2.1 Il problema

Lo abbiamo già detto, tutto intorno a noi è informazione; una parte di informazioni ci appartiene e desideriamo tenerla riservata, oppure condividerla con pochi individui; una parte invece desideriamo scambiarla oppure renderla disponibile ad una comunità molto ampia; infine una parte non ci appartiene, ma comunque ne siamo partecipi e possiamo usarla come ci pare, oppure secondo regole ben stabilite.

Tenere riservata una informazione è sempre stato una necessità, da quando l'uomo ha cominciato a dirsi in qualche modo "civile". I sistemi di crittografia risalgono alla notte dei tempi, e famoso è quello che usava Cesare per comunicare con i suoi generali (e certo non usava il telefono...).

Oggi la parola d'ordine pare essere "connect": se non si è in qualche modo "connessi" col resto del mondo (col PC, il telefonino etc.) ci sembra di essere incompleti. Allora quali sono le regole per sentirsi "connesso" ed allo stesso tempo al sicuro ?

2.2 Il personal computer

L'era del Computer personale è cominciata circa 25 anni fa, ed all'inizio questo nuovo strumento elettronico poteva dirsi davvero "personale". Ovviamente i grandi sistemi (quelli che occupavano stanze intere) erano in qualche modo interconnessi, ma quella scatola di latta appoggiata sulla scrivania, quella era proprio "privata". Erano i tempi di Apple II e dei primi PC Ibm, quando le informazioni venivano archiviate sui "floppy disk", dischi flessibili da 5 pollici. Bastava estrarre il Floppy, ed i dati "viaggiavano" con noi, magari per finire in cassaforte.

Le cose sono assai cambiate da allora, il Personal Computer è diventato molto meno "personale", anzi in alcuni casi può divenire anche "pubblico", e questo non sempre fa piacere.

Riflettiamo un momento : di solito si usa un PC per **lavoro** oppure per **divertimento**; nel primo caso elaboriamo delle informazioni che non ci appartengono (sono dell'Azienda per cui lavoriamo), ma abbiamo il diritto di accedervi; nel secondo caso le informazioni sono di nostra proprietà o comunque possiamo legalmente utilizzarle. In tutte e due i casi i dati (ed i programmi, ed un mucchio di altre cose) risiedono nella memoria di massa (hard disk) del nostro PC. Magari abbiamo le foto della nonna, le lettere d'amore della ex, il Bilancio e gli estratti conto bancari della nostra Azienda. Sono informazioni importanti per noi; sarebbe una disdetta vederle distrutte oppure sottratte. *Lascereste aperta la porta di casa* ? Certamente no, ma è quello che di solito fate con il vostro PC, senza badarci.

2.3 Scenari

Per semplificare, facciamo alcune ipotesi:

1. *il nostro PC non ha alcun tipo di connessione*: *niente rete locale, niente internet, e* ***siamo i soli*** *che possono accedere "fisicamente" alla tastiera ed al mouse.* In questo caso possiamo sentirci abbastanza tranquilli; dobbiamo solo stare attenti alla nostra sbadataggine, ed a quello che installiamo sul PC attraverso il CD oppure i Floppy. Infatti un virus contenuto in un programma potrebbe comunque infettare il nostro computer.
2. *il nostro PC non ha alcun tipo di connessione: niente rete locale, niente internet, ma* ***NON SIAMO I SOLI*** *che possono accedere "fisicamente" alla tastiera ed al mouse.* Questo può accadere in famiglia oppure in azienda, quando condividiamo il computer con i nostri parenti ed i nostri colleghi. Qui ovviamente bisogna fare attenzione non solo a se stessi ma anche agli altri.
3. *il nostro PC è collegato ad una Rete Locale, ad esempio in Azienda, e quindi può condividere le proprie risorse con gli altri computer della "comunità"*. Qui dovremmo cominciare a preoccuparci, perché altre persone, su altri elaboratori, potrebbero accedere o tentare di accedere ai dati residenti sulle nostre memorie di massa.
4. *il nostro PC è collegato direttamente ad Internet, tramite modem analogico oppure ADSL*; durante le connessioni siamo quindi "esposti al mondo", infatti comunichiamo con la rete attraverso un indirizzo "pubblico" e raggiungibile da qualsiasi altro computer della terra collegato ad Internet. I rischi del punto 3 si moltiplicano in modo esponenziale.
5. *il nostro PC è collegato ad una Rete Locale, attraverso la quale accediamo ad internet*; di solito un "router" si occupa del trasferimento dei dati da e per la rete, e "maschera" la nostra presenza. Siamo al sicuro ? No, affatto. Inoltre dobbiamo fronteggiare due minacce: una interna (la rete locale) ed una esterna (Internet).

La morale è: **"più siamo 'collegati' più i rischi si moltiplicano"**. Quindi è necessario adottare le giuste strategie per non perdere irrimediabilmente i nostri dati (e quindi ore ed ore di lavoro). Ma, in realtà, che cosa rischiamo davvero ?

2.4 Virus & C.

Il rischio più grosso è quello di perdere definitivamente ed in modo irreversibile una parte (od anche tutti) i dati presenti sul nostro Hard Disk. Nella peggiore delle ipotesi il PC rifiuterà di avviarsi ed anche il ricorso ad un esperto sarà inutile. Nella migliore, noteremo solo sporadici malfunzionamenti, rallentamenti, blocchi improvvisi e saltuarie perdite di documenti. Potremmo infine non accorgerci di nulla, ma comunque il nostro PC sarebbe utilizzato da altri a nostra insaputa durante i collegamenti Internet, per gli scopi più impensati.

Descrivere in dettaglio le tecniche utilizzate dai creatori di virus (o meglio "*malware*" come si dice oggi) non è lo scopo di queste note. Chiediamoci però almeno in linee generali come un "malware" può entrare nel nostro PC. La storia insegna che anche quando le mura sono alte e ben protette, e le porte chiuse si può conquistare una città (il nome Ulisse vi dice niente ?). Quindi bisogna conoscere l'attaccante e non abbassare la guardia.

Lo scopo principale di un "malware" è installarsi a vostra insaputa sul disco rigido del PC, per eseguire i compiti per cui è stato scritto; ma come entra ?

- La strada più semplice è quella della posta elettronica; un vostro conoscente (o anche uno sconosciuto) vi manda un messaggio del tipo "ti allego questa immagine (o documento, o file... fate voi), aprila e dammi un parere"; voi aprite l'allegato... ed il guaio è fatto. Questo tipo di infezione si chiama "trojan horse".....
- state tranquillamente navigando su Internet, quando si apre una finestra che vi invita a premere il tasto "OK" per, ad esempio, accedere ad un'area riservata del sito; se confermate, tramite un controllo che si chiama ActiveX, sul vs. PC viene trasferito e lanciato un programma esterno... sarà "malware" ?
- State sempre navigando tranquillamente su internet, su siti "istituzionali", e quindi pensate di dormire sonni tranquilli, ma il cattivo di turno sfrutta una falla nella sicurezza di Windows e vi infetta comunque. Questo è il caso del virus Blaster che nell'estate del 2003 è entrato nei computer di mezzo mondo; fortuna che si limitava a spegnere il PC
- infine il vostro amico vi dice: "carica questo simpatico programmino gratuito, vedrai che divertimento..."; purtroppo il programmino gratuito è divertente, ma si porta con se un bel po' di "zavorra"....

Ovviamente le modalità di infezione e le loro varianti sono moltissime, ed elencarle tutte impiegherebbe diverse pagine. Ci basti sapere che molte volte è il nostro comportamento disattento ad aprire le porte a questi programmi. Sarà quindi utile sapere che tipologie di "infezioni" possiamo contrarre.

- Il **virus classico** è un programma che porta con se conseguenze in qualche modo distruttive per il PC che lo ospita. Di solito una volta attivato attacca qualche tipo di file (ad esempio solo i documenti) oppure parti cruciali del sistema operativo (le DLL, oppure la cartella di Windows). I danni sono comunque rilevanti, ed inoltre il virus tende a replicarsi su altre macchine collegate in rete
- un **virus benigno** invece si limita a comportamenti fastidiosi, ma non troppo distruttivi. Tipico è il caso del già citato Blaster e delle sue varianti

- un **virus di macro**, ormai relativamente poco diffuso, è un programma che sfrutta la capacità di alcune applicazioni Office di eseguire le macro (Microsoft Word in primis). Si presenta insieme ad un semplice documento .doc, e può diventare estremamente pericoloso
- una "**backdoor**" è un software che non si manifesta esplicitamente, ma prende il controllo del vostro PC per gli scopi più diversi : furto di informazioni, trasferimento non autorizzato di dati, controllo remoto delle vostre risorse, attacchi Dos (Denial of Service) ad altri computer di Internet. Tristemente famoso è "Back Orifice" (un nome che è tutto un programma...)
- un "**dialer**" non è propriamente un virus, perché si limita a cambiare i parametri della vs connessione ad internet, per chiamare con il modem numeri a pagamento. Risultato: bollette stratosferiche. Funziona solo se vi collegate ad internet con un modem analogico, quindi se usate un router o l'ADSL siete al sicuro. Un effetto collaterale dei Dialer di solito è quello di cambiare la pagina di apertura del Browser ed indirizzarla di solito su siti porno.
- uno "**spyware**" è un piccolo programma, di solito contenuto in altri SW di utilizzo normale (ad es. KAZAA, oppure GO!ZILLA) che raccoglie informazioni sul modo in cui usate il PC e le trasmette periodicamente ad una o più Aziende a scopo di analisi pubblicitaria. Alcuni sono legali (ad es. Alexa) e compresi nelle licenze d'uso anche di programmi commerciali. Altri sono meno legali, ed oltre alle vostre abitudini di navigazione trasmettono anche le password di accesso ai siti web ed i numeri della vostra carta di credito

2.5 ...e Allora ??

Allora cominciamo con un po' di sana teoria, che aiuta a comprendere i termini del problema. La Sicurezza (non solo informatica) si basa su due soli concetti : **l'Autenticazione** ed i **Diritti**. Quando ci troviamo ad esempio di fronte ad un Bancomat, inseriamo prima la carta e poi il PIN; questa è la fase di Autenticazione: il sistema in base ai parametri forniti ci riconosce oppure ci rifiuta (perché magari abbiamo sbagliato il PIN). Una volta che siamo stati "autenticati", il sistema ci assegna i "diritti" : ad esempio possiamo consultare il nostro Estratto Conto, oppure fare un prelievo, ma certo non esaminare la situazione contabile di un altro cliente. Inoltre i nostri "diritti" possono variare nel tempo: perciò non possiamo più prelevare se abbiamo superato già il nostro limite mensile. Allo stesso modo, il cassiere della banca, sul suo terminale, all'inizio del lavoro comunque viene "autenticato", ma avrà molti più diritti di noi, perché sarà abilitato ad eseguire le operazioni che la sua posizione comporta. Probabilmente il Direttore della filiale avrà maggiori diritti del cassiere, e così via fino all' "amministratore" del sistema che gode ovviamente di diritti illimitati. Inoltre un sistema sicuro registra nel tempo anche CHI ha eseguito una certa operazione, in modo da controllare con esattezza le responsabilità.

Tutti i sistemi informatici attuali si fondano su questi principi, per cui sul vostro PC di solito l'amministratore siete voi, quindi avete diritti illimitati, perciò un programma eseguito da voi può provocare tutti i danni che vuole. Ecco allora la prima legge della sicurezza:

"Ogni utente deve possedere il minimo dei diritti necessari al corretto espletamento delle sue funzioni".

Questo significa che meno diritti si possiedono, meno danni si possono arrecare al sistema, e questo è particolarmente vero in ambienti di Rete su PC Aziendali o comunque di proprietà altrui. Se infatti si reca un danno ai propri dati... pazienza, ma se in gioco c'è la sicurezza di Archivi dell'Azienda o l'Ente per cui lavorate il discorso cambia di molto.

2.6 Autenticazione e Diritti

Dunque i sistemi informatici attuali si basano sui principi dell'autenticazione e dei diritti, e di solito partono già con alcuni "gruppi" o "categorie" di utenti standard, a cui possono essere associati gli utilizzatori reali. Questi gruppi sono :

- **Amministratori**; **Administrator** in Windows, **root** in linux/unix. Un utente che appartiene a questo gruppo ha di solito diritti illimitati, quindi può gestire il sistema, ed anche assegnare diritti agli altri utenti
- **User** oppure **Power User**; un utente in questo gruppo **non può** gestire alcuni aspetti (quelli importanti per il corretto funzionamento del sistema) e di solito **non può** cambiare i diritti propri o degli altri utenti (il discorso è particolare per gli ambienti Windows, ci torneremo in seguito)
- **guest**, cioè ospite; di solito questo utente è abilitato solo a "leggere" alcune informazioni, ma non può cambiare nulla del sistema

Se il PC *non è collegato in rete*, l'autenticazione è locale, quindi è il PC stesso che controlla le credenziali; se si usa una Rete Aziendale, l'autenticazione può essere locale o *centralizzata*; in questo secondo caso è un Computer Server esterno che controlla le credenziali, e quindi il controllo è delegato ad un utente che ricopre il ruolo di amministratore di rete.

Risulta dunque chiaro che quindi la prima regola della sicurezza, riscritta, sarebbe :

"autenticarsi come amministratore solo quando è necessario eseguire compiti di gestione del sistema, ed entrare come "user" in tutti gli altri casi"

Questa regola è seguita alla lettera nei sistemi LINUX, dove si diventa "root" solo in alcuni (rari) casi. Ma nei sistemi Windows ....

2.7 La Password

Nella maggioranza dei casi la fase di autenticazione si supera indicando due informazioni: il *nome utente* (in inglese *login id*) e la *password* (in italiano *parola chiave*). Il *nome utente* può

essere scelto da voi oppure scelto dall'amministratore del sistema, e di solito una volta assegnato non è più modificabile. La *password*, anche se assegnata dall'amministratore, è SEMPRE modificabile dall'utente. Quindi la scelta di una buona password è essenziale.

Alcuni sistemi implementano delle regole, per cui la password, per essere valida, deve ad es. essere più lunga di 6 caratteri, avere all'interno lettere maiuscole e minuscole etc. In altri casi la scelta spetta a voi ed è completamente libera. Inoltre una password può avere una *scadenza*, cioè essere valida solo per periodi limitati di tempo. La domanda allora è: come si sceglie una password ?

Chi usa Internet sa che molti Siti Web per l'accesso ad alcune informazioni o servizi richiedono una autenticazione. Ora, se state navigando sul sito delle ricette della nonna, una ottima password può essere anche "pippo"; se state accedendo alla Banca on Line e volete evitare di trovarvi col Conto Corrente a zero, meglio pensarci su.

Non esiste una regola per la scelta di una password, e molto dipende dalle informazioni da proteggere e dal tipo di attacco che possono subire. In particolare, recuperare una password sconosciuta è possibile attraverso:

- ✔ **il semplice tentativo**; siccome le password che si scelgono sono quasi sempre le stesse, chi vi conosce proverà in sequenza: il vostro nome (o soprannome) e quello dei familiari, compreso il cane; la data di nascita, di matrimonio etc.; la targa della macchina e così via. Sareste sorpresi di come questi tentativi abbiano successo in molti casi ....
- ✔ **l'attacco a forza bruta**; esistono programmi che cercano di indovinare la password basandosi su "dizionari" di milioni di termini, comprendenti tutte le parole di senso comune; altri programmi invece si basano su semplici combinazioni di lettere, sono più lenti, ma avendo tempo...
- ✔ **le vulnerabilità dei singoli programmi**; Microsoft Office, ad esempio, fino alla versione 2000 usava un metodo banale per proteggere i documenti e bastava un semplice programmino per avere accesso alle password di protezione
- ✔ **la richiesta diretta**; a volte basta chiedere, magari spacciandosi per chi non si è. Non avete idea di come sia semplice ottenere una password solo chiedendola all'interessato, a voce ma anche per posta elettronica.

Potremmo continuare, ma rischiamo di annoiarvi. Allora meglio qualche regola pratica:

- ✔ **non usate password troppo corte**; gli attacchi a forza bruta hanno successo immediato sulle password brevi; usate una parola di almeno otto caratteri
- ✔ **evitate tutte le parole di senso comune**; i "vocabolari" disponibili per gli attacchi sono molto aggiornati....
- ✔ **mischiate numeri, simboli e lettere maiuscole e minuscole**;
- ✔ **cambiate abbastanza spesso la password**, diciamo una volta ogni sei mesi, e soprattutto non comunicatela a nessuno (compreso amici e colleghi); ovviamente c'è chi la attacca col post-it sul monitor, ma voi non lo fareste mai, vero ?

Seguendo queste semplici regole avrete una password quasi perfetta, con un solo piccolo difetto: *sarà difficile da ricordare....*

2.8 Cambiare la password in Windows

Nei sistemi Windows (2000 o XP), se il computer è collegato ad un Dominio, dopo esserti autenticato (quindi dopo aver avuto accesso al Desktop) è sufficiente premere contemporaneamente i tasti *Ctrl Alt* e *Canc*; nella finestra del Task Manager scegliere "Cambio Password", immetti la vecchia e la nuova e premi OK.

In Windows XP, se il computer NON è collegato ad un Dominio, basta scegliere dal Menu Start la voce *Pannello di Controllo* e quindi *Account Utente*, selezionale il proprio Account e eseguire "*Cambia Password*".

2.9 I sistemi Windows

Windows nel passato non è mai stato un sistema operativo orientato alla sicurezza; solo dalla diffusione di Windows NT il problema è stato affrontato in modo serio, e **sui sistemi Desktop si dovrebbero usare solo Windows 2000 oppure XP**. *Questo significa che se siete utenti di Windows 95, 98 o ME l'unico consiglio sensato è: se vi interessa la sicurezza cambiate sistema operativo.*

Nonostante tutto, Microsoft lascia all'utente ampia libertà di configurazione, anzi nelle installazioni standard di Windows 2000 e XP è frequente vedere accessi al sistema senza autenticazione direttamente come Amministratori. In parole povere chiunque si sieda davanti al vostro PC, con la semplice pressione del tasto di accensione ha a disposizione tutti i vostri dati. Allora ecco i primi consigli:

- assegnate una Password a tutti gli Utenti del PC, in primo luogo a quelli del Gruppo Amministratori
- create almeno due account di accesso al PC: uno amministrativo ed uno del gruppo User per il lavoro di tutti i giorni
- autenticatevi come amministratori SOLO quando è effettivamente necessario : per installare nuovi Software o per cambiare la configurazione del sistema. Ricordate che meno diritti avete meno danni potete procurare

Sembra facile, ma il mondo Windows è strano: potreste incontrare ad esempio delle applicazioni che se non avete diritti amministrativi non partono nemmeno; in questi casi il consiglio è: cambiate applicazioni.

Ora che almeno l'accesso al vostro PC è autenticato, passiamo agli altri passi da compiere nella lunga strada della tranquillità :

1. Scelta delle Applicazioni
2. Tenere aggiornato il Sistema
3. Backup dei dati
4. Assegnazione dei Diritti Utente
5. Programmi Antivirus
6. Firewall : chiudi la porta al nemico

2.10 Scelta delle Applicazioni

La nostra analisi riguarda la sicurezza, quindi non parleremo di gusti personali. Sappiamo bene che ognuno di noi predilige determinate applicazioni, per i motivi più diversi, a volte solo per abitudine. Alcuni di questi programmi però possono essere fonte di guai seri, quindi anche le abitudini, quando sono cattive, vanno cambiate. Cominciamo...

Del **Sistema Operativo** abbiamo già parlato: se proprio dovete usare una versione di Windows, scegliete Windows 2000 oppure XP. TUTTI i sistemi operativi precedenti di Microsoft non hanno i requisiti minimi per essere utilizzati in ambienti di produzione seri. Una buona alternativa è LINUX, soprattutto per soluzioni Server, ma bisogna essere abbastanza esperti per poter sfruttare al meglio questo sistema robusto ed affidabile (oltre che gratuito). Per il seguito assumeremo comunque come ambiente di riferimento Windows.

Il **Browser** (in pratica il programma che ci permette di accedere ai siti internet) sembra una applicazione banale. Tutti i Windows (dal 95 in poi) comprendono Internet Explorer, quindi la scelta di milioni di utenti è appunto questa. *In fondo perché cercare un altro programma quando si dispone di uno strumento facile, veloce e gratuito ??*

Semplicemente perché Explorer, ed anche la tecnologia ActiveX che Microsoft usa, si sono rivelati incredibilmente deboli dal punto di vista della sicurezza. La versione 6.0 (ultima disponibile nel momento in cui scriviamo) viene aggiornata in pratica ogni quindici giorni. Inoltre è un Browser lento, che apre senza fiatare tutte le schifezze che gli si danno in pasto (compreso decine di finestre Pop Up non richieste). Esistono validissime alternative come Mozilla o Firefox (www.mozillaitalia.org), oppure Opera che sono molto più efficienti e sicure. Però Explorer è il leader del mercato e potreste incontrare siti fatti da incompetenti, che non rispettano lo standard HTML, e che si vedono bene solo col Browser Microsoft. Sono sempre di meno, ma evitateli come la peste. *Se proprio volete usare Explorer, disabilitate almeno i controlli ActiveX nelle opzioni Internet.*

Per chi usa la **posta elettronica**, la scelta più semplice è *Outlook Express*; è un programma efficiente, che in passato ha avuto i suoi problemi ma che ora è abbastanza sicuro. Se non avete esigenza sofisticate usatelo pure, avendo cura di disabilitare l'anteprima automatica dei messaggi. *Attenzione agli allegati, ed ai messaggi "strani": la strada che seguono molti virus è quella degli allegati che sembrano innocui, magari semplici immagini, ma in effetti trasportano*

infezioni dannose. Se volete cambiare, provate il client di posta di Mozilla (potente e flessibile) oppure tutta una serie di classici come Eudora Mail.

Di solito in ambito lavorativo si utilizza una suite di **programmi Office** (Elaborazione Testi, Foglio Elettronico etc.). Anche in questo caso il prodotto più diffuso è Microsoft Office, ed anche in questo caso la possibilità per questi applicativi di eseguire dei programmi in automatico (le macro) pone seri rischi di sicurezza. Molti virus sono infatti "Virus di Macro", nascosti dentro documenti di Word o di Excel, che una volta aperti infettano il sistema. Fino alla versione 97 di Office, il programma non avvertiva neppure dell'esecuzione di una Macro. Dalla versione 2000 in poi si può scegliere di eseguire o rifiutare le macro dei documenti, e potreste trovare più semplice disattivarle del tutto con l'apposita opzione di configurazione.

Anche in questo caso esistono alternative più efficienti e sicure. La versione attuale di OpenOffice (1.4) è stabile, veloce, potente e pure gratuita. Si trova e si scarica in www.openoffice.org .

Infine **attenzione a cosa si scarica da Internet**: molte applicazioni gratuite contengono in realtà al loro interno spyware (violazione della privacy) e backdoor (controllo remoto del vs. PC). La regola generale è di evitare di installare programmi sconosciuti su PC utilizzati per lavorare.

2.11 Tenere aggiornato il sistema

La comparsa giornaliera di nuove vulnerabilità costringe l'utente attento alla sicurezza ad aggiornare di continuo il sistema. *Questo circolo vizioso sta diventando insostenibile*. Facciamo un semplice esempio. Se comprate oggi un nuovo PC, probabilmente troverete preinstallato Windows XP nella versione Service Pack 1. Ebbene, per portare il sistema al livello di sicurezza più recente dovreste scaricare dal sito di Microsoft una sessantina di Patch, per almeno 50 MegaByte di software. Se questo può sembrare appena accettabile per chi ha una connessione veloce (almeno ADSL), è sicuramente impossibile per la maggioranza degli utenti dotati si semplice Modem analogico. Infatti, se tutto va bene, servirebbero una decina di ore di collegamento.

Inoltre l'opzione di aggiornamento automatico in XP avrebbe lo scopo di semplificare questi passaggi all'utente finale: ma una buona metà delle patch disponibili non è utile per la maggioranza dei sistemi, e molte in passato hanno creato più problemi di quelli che hanno risolto. Quindi scaricare tutto può essere controproducente. Un altro esempio : alla comparsa del virus Blaster, Microsoft ha rilasciato una patch che avrebbe dovuto risolvere il problema. Dopo un paio di mesi si è scoperto che quella "pezza" non copriva tutti i buchi, quindi eccone un'altra che ora pare sia definitiva....

Ultimo esempio : Microsoft Windows Server 2003 è stato rilasciato ad Ottobre 2003; dopo quindici giorni sono già disponibili una decina di aggiornamenti; per non parlare di Office 2003... Devo continuare ??

Per la sicurezza è essenziale la stabilità del Sistema Operativo, e finora Bill Gates ha badato più ai soldi che ai suoi clienti. Seguire la strada degli aggiornamenti continui è assurdo, quindi meglio affidarsi ad un buon consulente (ma costa), oppure seguire i semplici consigli che stiamo cercando di dare.

2.12 Backup dei Dati

Backup in inglese è sinonimo di "Copia di Sicurezza". Il concetto è molto semplice: periodicamente è opportuno trasferire i propri dati su supporti diversi dall'Hard Disk del PC, in modo che in caso di problemi possiamo recuperare il lavoro svolto. In genere si utilizza un masterizzatore ed un CD scrivibile, visti i costi decisamente popolari di questa soluzione. In alternativa potete scegliere Nastri Magnetici, Dischi ZIP, Memorie su USB ed altre decine di metodi che sarebbe lungo e noioso elencare.

Quindi ora dobbiamo solo definire la voce "periodicamente", e individuare nel caos del nostro disco rigido quali sono i dati veramente importanti. Facile, no ?

Stabilire una regola generale per la periodicità del Backup è difficile, perché dipende da una miriade di fattori. In primis dal tipo di uso che si fa del Computer, e poi dalla quantità e dalla qualità dei dati memorizzati. Diciamo che una buona indicazione è ogni due settimane, ma ci sono anche casi in cui è indispensabile eseguire backup giornalieri (contabilità aziendali con un elevato numero di transazioni, ad esempio).

Risulta invece impossibile indicare in modo generico QUALI dati copiare. Infatti le domande da porsi sono :

- quali applicazioni uso più frequentemente ?
- Dove queste applicazioni salvano i dati ?
- Esistono cartelle del disco rigido che è opportuno salvare ?

Alla prima domanda dovrebbe essere abbastanza facile rispondere: sicuramente un programma di Word Processing, un Foglio Elettronico, Internet e la Posta; poi, che so, uno di Ritocco Fotografico, lo Scanner...; infine le applicazioni che usate per lavoro, la contabilità, la fatturazione, etc.

Alcuni Software chiedono dove salvare i documenti, quindi è una nostra responsabilità scegliere le cartelle in modo che siano facilmente accessibili; Windows da un po' di versioni prevede una cartella chiamata appunto "*Documenti*" ed è una buona idea usarla sempre, anche per motivi di privacy, come vedremo in seguito. **Evitate assolutamente di salvare documenti sul Desktop**: è una cartella di difficile "reperibilità", di solito non viene archiviata dai programmi di Backup. Questo consiglio però pare non essere molto seguito: si vedono desktop più affollati di Piazza di Spagna a mezzogiorno, con ricerche affannose del tipo "ma questo documento era proprio qui, me lo ricordo bene ... ".

Purtroppo però non sempre le cose sono così facili : sapete per caso dove il vostro programma di posta preferito (ad esempio Outlook Express) archivia i messaggi ? E la rubrica dei contatti ? Ed il vostro programma di contabilità, dove mette i preziosissimi archivi frutto di tante giornate di lavoro ?

Dovreste chiedervelo, se volete eseguire un Backup che serve a qualcosa...

2.13 Assegnazione dei Diritti Utente

Della fase di autenticazione e dei vari profili di utenti abbiamo già parlato. Abbiamo anche detto che è buona norma accedere al PC con il minimo dei diritti necessario all'utilizzo di tutti i giorni, ed abbiamo suggerito l'uso di più profili utente in modo da minimizzare i rischi.

Sia Windows (2000 ed XP) che Linux dispongono di strumenti assai sofisticati per l'assegnazione dei diritti degli utenti. Si può restringere l'accesso ad alcune cartelle, impedire la navigazione su siti pericolosi, precludere l'uso di specifiche funzionalità etc. Non è nostra intenzione scendere nei dettagli delle procedure, ci limiteremo quindi ad evidenziare alcune cose che è utile conoscere.

Windows fa differenza tra utenti che accedono in *locale* ed utenti che accedono attraverso la *Rete* alle risorse del PC. Nel primo caso *tutti gli Utenti autorizzati all'accesso locale hanno piena disponibilità della maggioranza delle cartelle del disco C:*. Questo significa che se siete abituati a salvare i vostri documenti ad esempio nella cartella *c:\lavoro*, normalmente tutti possono infilarci il naso. **Ma se salvate nella vostra cartella Documenti, SOLO VOI avete accesso ai files**. Questo perché Windows salva il "profilo" di ogni utente in c:\Documents and Settings, ed ogni cartella è protetta dall'accesso altrui, a meno che l'Amministratore non decida il contrario.

Nel secondo caso, l'Amministratore decide quali risorse condividere in Rete, ed i diritti di utilizzo delle stesse. Mettere in comune delle risorse richiede un po' di attenzione: se per una stampante non ci sono problemi, le cartelle condivise possono essere fonte di guai. In particolare bisognerebbe evitare di assegnare diritti di accesso al Gruppo "Everyone" (cioè tutti), elencando uno per uno gli utenti abilitati. Il consiglio è : ***condividete il meno possibile***.

2.14 Antivirus

Lo scopo di un antivirus è quello di fare da "sentinella" al vostro PC per evitare che un programma "cattivo" possa causare danni. Esistono molti prodotti sul mercato, e pare che sia uno dei settori in cui la crisi si sente di meno. Queste applicazioni vengono caricate in memoria all'avvio del sistema, e controllano di continuo l'attività del PC alla ricerca delle "firme" (cioè degli elementi caratteristici) dei Virus noti. Una volta individuata all'interno di un File o di una Applicazione la "firma" del Virus, il programma blocca l'esecuzione del Codice e vi chiede se porre in "quarantena" il colpevole oppure cancellarlo del tutto. In alcuni casi è anche possibile

"pulire" il File dal Virus in modo da poterlo riutilizzare. Il principio di funzionamento è semplice, ma comporta alcuni svantaggi:

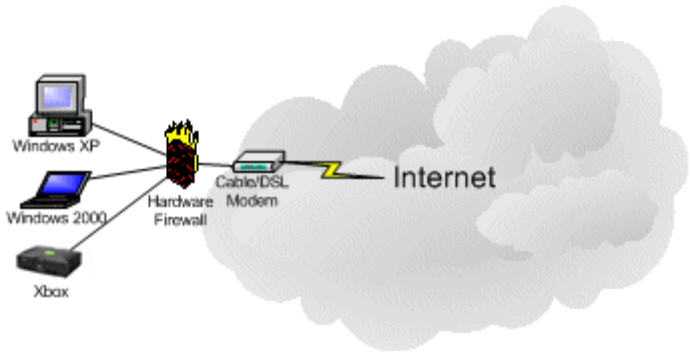
- l'antivirus è sempre presente in memoria, e deve controllare ogni operazione di lettura o scrittura eseguita sul PC; quindi rallenta in modo più o meno marcato l'esecuzione delle applicazioni
- la maggior parte dei motori di scansione si basa sul riconoscimento di "tracce" del virus che vengono confrontate con un Archivio di Firme; se il "malware" è recente, oppure le firme non sono aggiornate il virus passa senza problemi
- l'Antivirus è inefficace su alcuni attacchi che sfruttano vulnerabilità particolari di Windows: è il caso del già citato Blaster, ma di recente se ne sono presentati molti altri.

Quindi i consigli che possiamo dare sono:

- cercate un Antivirus "leggero" che sia poco "presente" nelle elaborazioni normali del PC, e che quindi rallenti poco la macchina; uno dei più "pesanti" è il Norton che nelle ultime versioni offre anche livelli di protezione sostanzialmente inutili
- tenete aggiornato l'archivio delle firme: c'è chi scarica gli aggiornamenti ogni giorno, ma un comportamento "normale" è almeno una volta alla settimana. Ricordate che un Antivirus non aggiornato equivale a nessun Antivirus
- ricordate che le due regole precedenti non vi mettono al riparo da disastri: molto dipende anche dal vostro comportamento, e una condotta "libertina" e poco attenta porta a gravi conseguenze (parliamo ovviamente di computer)
- accanto all'antivirus, potete usare un buon FireWall, come vedremo qui di seguito

2.15 FireWall

La traduzione più esatta è "porta tagliafuoco", cioè quelle paratie che spesso vediamo nei luoghi pubblici o negli alberghi che servono ad isolare alcune parti del fabbricato per evitare che un eventuale incendio si propaghi con facilità. Infatti un FireWall serve ad isolare una "Zona Informatica" dall'esterno. Ora per "Zona Informatica" possiamo intendere un insieme di Computer, ad esempio una Rete Locale, oppure anche un solo PC, il nostro, che si collega ad Internet.



Come indicato in figura, di solito un FireWall filtra il traffico da e per Internet, quindi tra una "Zona" considerata sicura cioè "**Trusted**" (la *Rete locale*) ed una considerata "insicura" quindi "**Untrusted**" (*Internet*). Esistono svariati tipi di FireWall: in generale se vogliamo proteggere una LAN che condivide l'accesso ad Internet, come in figura, potremo usare un "HardWare FireWall" cioè una apparecchiatura (un PC dedicato oppure un Router) con SW di controllo del traffico. Se più semplicemente abbiamo un solo PC che si collega con una connessione privata, la soluzione ideale è un "Personal FireWall" cioè un semplice programma da installare proprio come un Antivirus.

L'importanza di questo tipo di applicazioni è cresciuta con la diffusione di tipologie di collegamento come l'ADSL che prevedono in alcuni casi l'assegnazione di un indirizzo IP Statico, cioè fisso. Questo comporta che un cattivone conoscendo il nostro indirizzo IP (cosa abbastanza semplice) possa, sfruttando una qualche falla nella sicurezza, entrare nella nostra LAN o nel nostro PC.

Compito del FireWall è dunque quello di controllare il traffico, e per fare questo ha bisogno di "regole": dobbiamo indicare quale tipo di comunicazione è permesso e quale vietato. In più i FireWall "personali" possono anche autorizzare l'accesso ad internet solo ad alcune applicazioni. Non è questa la sede adatta ad un trattamento approfondito della configurazione di un FireWall: sappiate però che regole scritte male equivalgono a nessuna regola, quindi bisogna sapere cosa si fa. Un FireWall ben sistemato è estremamente utile nel prevenire attacchi dall'esterno, ma perfettamente inutile se l'attacco proviene dall'interno.

Esistono molti "Personal FireWalls", come *Zone Alarm*, oppure Norton o McAfee. Nessuno è particolarmente semplice da configurare, ma con un pò di attenzione si ottengono buoni risultati. Per la protezione di LAN o per la configurazione degli "HardWare Firewalls" il "fai da te" è sconsigliato: meglio rivolgersi ad un buon professionista.

2.16 Allora...

Se alla fine della lettura siete spaventati non preoccupatevi, era proprio questo lo scopo. Il concetto di "sicurezza" è ormai strettamente legato a quello di "connessione". Evitare problemi non è poi così complicato, basta solo fare attenzione a quello che si fa.

Buona fortuna ....

3. Licenza Creative Commons

Attribuzione–NonCommerciale–NonOpereDerivate 2.0 (ITALIA)

L'OPERA (COME SOTTO DEFINITA) È MESSA A DISPOSIZIONE SULLA BASE DEI TERMINI DELLA PRESENTE LICENZA "CREATIVE COMMONS PUBLIC LICENCE" ('CCPL' O 'LICENZA'). L'OPERA E' PROTETTA DAL DIRITTO D'AUTORE E/O DALLE ALTRE LEGGI APPLICABILI. OGNI UTILIZZAZIONE DELL'OPERA CHE NON SIA AUTORIZZATA AI SENSI DELLA PRESENTE LICENZA O DEL DIRITTO D'AUTORE È PROIBITA.

CON IL SEMPLICE ESERCIZIO SULL'OPERA DI UNO QUALUNQUE DEI DIRITTI QUI DI SEGUITO ELENCATI, TU ACCETTI E TI OBBLIGHI A RISPETTARE INTEGRALMENTE I TERMINI DELLA PRESENTE LICENZA AI SENSI DEL PUNTO 8.e. IL LICENZIANTE CONCEDE A TE I DIRITTI QUI DI SEGUITO ELENCATI A CONDIZIONE CHE TU ACCETTI DI RISPETTARE I TERMINI E LE CONDIZIONI DI CUI ALLA PRESENTE LICENZA.

1. Definizioni Ai fini e per gli effetti della presente licenza, si intende per

a. **"Collezione di Opere"** un'opera, come un numero di un periodico, un'antologia o un'enciclopedia, nella quale l'Opera nella sua interezza e forma originale, unitamente ad altri contributi costituenti loro stessi opere distinte ed autonome, sono raccolti in un'unità collettiva. Un'opera che costituisce Collezione di Opere non verrà considerata Opera Derivata (come sotto definita) ai fini della presente Licenza;

b. **"Opera Derivata"** un'opera basata sull'Opera ovvero sull'Opera insieme con altre opere preesistenti, come una traduzione, un arrangiamento musicale, un adattamento teatrale, narrativo, cinematografico, una registrazione di suoni, una riproduzione d'arte, un digesto, una sintesi, od ogni altra forma in cui l'Opera possa essere riproposta, trasformata o adattata. Nel caso in cui un'Opera tra quelle qui descritte costituisca già Collezione di Opere, essa non sarà considerata Opera Derivata ai fini della presente Licenza. Al fine di evitare dubbi è inteso che, quando l'Opera sia una composizione musicale o registrazione di suoni, la sincronizzazione dell'Opera in relazione con un'immagine in movimento ("synching") sarà considerata Opera Derivata ai fini di questa Licenza;

c. **"Licenziante"** l'individuo o l'ente che offre l'Opera secondo i termini e le condizioni della presente Licenza;

d. **"Autore Originario"** il soggetto che ha creato l'Opera;

e. **"Opera"** l'opera dell'ingegno suscettibile di protezione in forza delle leggi sul diritto d'autore, la cui utilizzazione è offerta nel rispetto dei termini della presente Licenza;

f. **"Tu"/"Te"** 'individuo o l'ente che esercita i diritti derivanti dalla presente Licenza e che non abbia precedentemente violato i termini della presente Licenza relativi all'Opera, o che, nonostante una precedente violazione degli stessi, abbia ricevuto espressa autorizzazione dal Licenziante all'esercizio dei diritti derivanti dalla presente Licenza.

2. Libere utilizzazioni. La presente Licenza non intende in alcun modo ridurre, limitare o restringere alcun diritto di libera utilizzazione o l'operare della regola dell'esaurimento del diritto o altre limitazioni dei diritti esclusivi sull'Opera derivanti dalla legge sul diritto d'autore o da altre leggi applicabili.

3. Concessione della Licenza. Nel rispetto dei termini e delle condizioni contenute nella presente Licenza, il Licenziante concede a Te una licenza per tutto il mondo, gratuita, non esclusiva e perpetua (per la durata del diritto d'autore applicabile) che autorizza ad esercitare i diritti sull'Opera qui di seguito elencati:

a. riproduzione dell'Opera, incorporazione dell'Opera in una o più Collezioni di Opere e riproduzione dell'Opera come incorporata nelle Collezioni di Opere;
b. distribuzione di copie dell'Opera o di supporti fonografici su cui l'Opera è registrata, comunicazione al pubblico, rappresentazione, esecuzione, recitazione o esposizione in pubblico, ivi inclusa la trasmissione audio digitale dell'Opera, e ciò anche quando l'Opera sia incorporata in Collezioni di Opere;

I diritti sopra descritti potranno essere esercitati con ogni mezzo di comunicazione e in tutti i formati. Tra i diritti di cui sopra si intende compreso il diritto di apportare all'Opera le modifiche che si rendessero tecnicamente necessarie per l'esercizio di detti diritti tramite altri mezzi di comunicazione o su altri formati, ma a parte questo non hai diritto di realizzare Opere Derivate. Tutti i diritti non espressamente concessi dal Licenziante rimangono riservati, ivi inclusi quelli di cui ai punti 4(d) e (e).

4. Restrizioni. La Licenza concessa in conformità al precedente punto 3 è espressamente assoggettata a, e limitata da, le seguenti restrizioni

a. Tu puoi distribuire, comunicare al pubblico, rappresentare, eseguire, recitare o esporre in pubblico l'Opera, anche in forma digitale, solo assicurando che i termini di cui alla presente Licenza siano rispettati e, insieme ad ogni copia dell'Opera (o supporto fonografico su cui è registrata l'Opera) che distribuisci, comunichi al pubblico o rappresenti, esegui, reciti o esponi in pubblico, anche in forma digitale, devi includere una copia della presente Licenza o il suo Uniform Resource Identifier. Non puoi proporre od imporre alcuna condizione relativa all'Opera che alteri o restringa i termini della presente Licenza o l'esercizio da parte del beneficiario dei diritti qui concessi. Non puoi concedere l'Opera in sublicenza. Devi mantenere intatte tutte le informative che si riferiscono alla presente Licenza ed all'esclusione delle garanzie. Non puoi distribuire, comunicare al pubblico, rappresentare, eseguire, recitare o esporre in pubblico l'Opera, neanche in forma digitale, usando misure tecnologiche miranti a controllare l'accesso all'Opera ovvero l'uso dell'Opera, in maniera incompatibile con i termini della presente Licenza. Quanto sopra si applica all'Opera anche quando questa faccia parte di una Collezione di Opere, anche se ciò non comporta che la Collezione di Opere di per sé ed indipendentemente dall'Opera stessa debba essere soggetta ai termini ed alle condizioni della presente Licenza. Qualora Tu crei una Collezione di Opere, su richiesta di qualsiasi Licenziante, devi rimuovere dalla Collezione di Opere stessa, ove materialmente possibile, ogni riferimento a tale Licenziante o, su richiesta di qualsiasi Autore Originario, a tale Autore Originario, come da richiesta.
b. Tu non puoi esercitare alcuno dei diritti a Te concessi al precedente punto 3 in una maniera tale che sia prevalentemente intesa o diretta al perseguimento di un vantaggio commerciale o di un compenso monetario privato. Lo scambio dell'Opera con altre opere protette dal diritto d'autore, per mezzo della condivisione di file digitali (c.d. filesharing) o altrimenti, non è considerato inteso o diretto a perseguire un vantaggio commerciale o un compenso monetario privato, a patto che non ci sia alcun pagamento di alcun compenso monetario in connessione allo scambio di opere coperte da diritto d'autore.
c. Qualora Tu distribuisca, comunichi al pubblico, rappresenti, esegua, reciti o esponga in pubblico, anche in forma digitale, l'Opera, devi mantenere intatte tutte le informative sul diritto d'autore sull'Opera. Devi riconoscere all'Autore Originale una menzione adeguata rispetto al mezzo di comunicazione o supporto che

utilizzi citando il nome (o lo pseudonimo, se del caso) dell'Autore Originale, ove fornito; il titolo dell'Opera, ove fornito; nella misura in cui sia ragionevolmente possibile, l'Uniform Resource Identifier, che il Licenziante specifichi dover essere associato con l'Opera, salvo che tale URI non faccia riferimento alla informazione di protezione di diritto d'autore o non dia informazioni sulla licenza dell'Opera. Tale menzione deve essere realizzata in qualsiasi maniera ragionevole possibile; in ogni caso, in ipotesi di Collezione di Opere, tale menzione deve quantomeno essere posta nel medesimo punto dove viene indicato il nome di altri autori di rilevanza paragonabile e con lo stesso risalto concesso alla menzione di altri autori di rilevanza paragonabile.

d. Al fine di evitare dubbi è inteso che, se l'Opera sia di tipo musicale

   i. **Compensi per la comunicazione al pubblico o la rappresentazione od esecuzione di opere incluse in repertori**. Il Licenziante si riserva il diritto esclusivo di riscuotere compensi, personalmente o per il tramite di un ente di gestione collettiva (ad es. SIAE), per la comunicazione al pubblico o la rappresentazione od esecuzione, anche in forma digitale (ad es. tramite webcast) dell'Opera, se tale utilizzazione sia prevalentemente intesa o diretta a perseguire un vantaggio commerciale o un compenso monetario privato.

   ii. **Compensi per versioni cover**. Il Licenziante si riserva il diritto esclusivo di riscuotere compensi, personalmente o per il tramite di un ente di gestione collettiva (ad es. SIAE), per ogni disco che Tu crei e distribuisci a partire dall'Opera (versione cover), nel caso in cui la Tua distribuzione di detta versione cover sia prevalentemente intesa o diretta a perseguire un vantaggio commerciale o un compenso monetario privato.

e. **Compensi per la comunicazione al pubblico dell'Opera mediante fonogrammi.** Al fine di evitare dubbi, è inteso che se l'Opera è una registrazione di suoni, il Licenziante si riserva il diritto esclusivo di riscuotere compensi, personalmente o per il tramite di un ente di gestione collettiva (ad es. IMAIE), per la comunicazione al pubblico dell'Opera, anche in forma digitale, nel caso in cui la Tua comunicazione al pubblico sia prevalentemente intesa o diretta a perseguire un vantaggio commerciale o un compenso monetario privato.

f. **Altri compensi previsti dalla legge italiana**. Al fine di evitare dubbi, è inteso che il Licenziante si riserva il diritto esclusivo di riscuotere i compensi a lui attribuiti dalla legge italiana sul diritto d'autore (ad es. per l'inserimento dell'Opera in un'antologia ad uso scolastico ex art. 70 l. 633/1941), personalmente o per tramite di un ente di gestione collettiva (ad es. SIAE, IMAIE), se l'utilizzazione dell'Opera sia prevalentemente intesa o diretta a perseguire un vantaggio commerciale o un compenso monetario privato. Al Licenziante spettano in ogni caso i compensi irrinunciabili a lui attribuiti dalla medesima legge (ad es. l'equo compenso spettante all'autore di opere musicali, cinematografiche, audiovisive o di sequenze di immagini in movimento nel caso di noleggio ai sensi dell'art. 18-bis l. 633/1941).

5. Dichiarazioni, Garanzie ed Esonero da responsabilità

SALVO CHE SIA ESPRESSAMENTE CONVENUTO ALTRIMENTI PER ISCRITTO FRA LE PARTI, IL LICENZIANTE OFFRE L'OPERA IN LICENZA "COSI' COM'E'" E NON FORNISCE ALCUNA DICHIARAZIONE O GARANZIA DI QUALSIASI TIPO CON RIGUARDO ALL'OPERA, SIA ESSA ESPRESSA OD IMPLICITA, DI FONTE LEGALE O DI ALTRO TIPO, ESSENDO QUINDI ESCLUSE, FRA LE ALTRE, LE GARANZIE RELATIVE AL TITOLO, ALLA COMMERCIABILITÀ, ALL'IDONEITÀ PER UN FINE SPECIFICO E ALLA NON VIOLAZIONE DI DIRITTI DI TERZI O ALLA MANCANZA DI DIFETTI LATENTI O DI ALTRO TIPO, ALL'ESATTEZZA OD ALLA PRESENZA DI ERRORI, SIANO ESSI ACCERTABILI O MENO. ALCUNE GIURISDIZIONI NON CONSENTONO L'ESCLUSIONE DI GARANZIE IMPLICITE E QUINDI TALE ESCLUSIONE PUÒ NON APPLICARSI A TE.

6. Limitazione di Responsabilità. SALVI I LIMITI STABILITI DALLA LEGGE APPLICABILE, IL LICENZIANTE NON SARÀ IN ALCUN CASO RESPONSABILE NEI TUOI CONFRONTI A QUALUNQUE TITOLO PER ALCUN TIPO DI DANNO, SIA ESSO SPECIALE, INCIDENTALE, CONSEQUENZIALE, PUNITIVO OD ESEMPLARE, DERIVANTE DALLA PRESENTE LICENZA O DALL'USO DELL'OPERA, ANCHE NEL CASO IN CUI IL LICENZIANTE SIA STATO EDOTTO SULLA POSSIBILITÀ DI TALI DANNI. NESSUNA CLAUSOLA DI QUESTA LICENZA ESCLUDE O LIMITA LA RESPONSABILITA' NEL CASO IN CUI QUESTA DIPENDA DA DOLO O COLPA GRAVE.

7. Risoluzione

a. La presente Licenza si intenderà risolta di diritto e i diritti con essa concessi cesseranno automaticamente, senza necessità di alcuna comunicazione in tal senso da parte del Licenziante, in caso di qualsivoglia inadempimento dei termini della presente Licenza da parte Tua, ed in particolare delle disposizioni di cui ai punti 4.a, 4.b e 4.c, essendo la presente Licenza condizionata risolutivamente al verificarsi di tali inadempimenti. In ogni caso, la risoluzione della presente Licenza non pregiudicherà i diritti acquistati da individui o enti che abbiano acquistato da Te Collezioni di Opere, ai sensi della presente Licenza, a condizione che tali individui o enti continuino a rispettare integralmente le licenze di cui sono parte. Le sezioni 1, 2, 5, 6, 7 e 8 rimangono valide in presenza di qualsiasi risoluzione della presente Licenza.
b. Sempre che vengano rispettati i termini e le condizioni di cui sopra, la presente Licenza è perpetua (e concessa per tutta la durata del diritto d'autore sull'Opera applicabile). Nonostante ciò, il Licenziante si riserva il diritto di rilasciare l'Opera sulla base dei termini di una differente licenza o di cessare la distribuzione dell'Opera in qualsiasi momento; fermo restando che, in ogni caso, tali decisioni non comporteranno recesso dalla presente Licenza (o da qualsiasi altra licenza che sia stata concessa, o che sia richiesto che venga concessa, ai termini della presente Licenza), e la presente Licenza continuerà ad avere piena efficacia, salvo che vi sia risoluzione come sopra indicato.

8. Varie

a. Ogni volta che Tu distribuisci, o rappresenti, esegui o reciti pubblicamente in forma digitale l'Opera o una Collezione di Opere, il Licenziante offre al destinatario una licenza per l'Opera nei medesimi termini e condizioni che a Te sono stati concessi dalla presente Licenza.
b. L'invalidità o l'inefficacia, secondo la legge applicabile, di una o più fra le disposizioni della presente Licenza, non comporterà l'invalidità o l'inefficacia dei restanti termini e, senza bisogno di ulteriori azioni delle parti, le disposizioni invalide od inefficaci saranno da intendersi rettificate nei limiti della misura che sia indispensabile per renderle valide ed efficaci.
c. In nessun caso i termini e le disposizioni di cui alla presente Licenza possono essere considerati rinunciati, né alcuna violazione può essere considerata consentita, salvo che tale rinuncia o consenso risultino per iscritto da una dichiarazione firmata dalla parte contro cui operi tale rinuncia o consenso.
d. La presente Licenza costituisce l'intero accordo tra le parti relativamente all'Opera qui data in licenza. Non esistono altre intese, accordi o dichiarazioni relative all'Opera che non siano quelle qui specificate. Il Licenziante non sarà vincolato ad alcuna altra disposizione addizionale che possa apparire in alcuna comunicazione da Te proveniente. La presente Licenza non può essere modificata senza il mutuo consenso scritto del Licenziante e Tuo.
e. **Clausola iCommons**. Questa Licenza trova applicazione nel caso in cui l'Opera sia utilizzata in Italia. Ove questo sia il caso, si applica anche il diritto d'autore italiano. Negli altri casi le parti si obbligano a rispettare i termini dell'attuale Licenza Creative Commons generica che corrisponde a questa Licenza Creative Commons iCommons.