Introduzione alla sicurezza dei sistemi informatici
Sicurezza

Chi si occupa di **sicurezza informatica** ha, come obiettivo principale, quello di offrire un adeguato grado di protezione dei dati, riducendo i fattori di rischio. In particolare, proteggere i dati significa garantirne:

- la **riservatezza** o **confidenzialità**, ovvero la protezione da letture non autorizzate dei dati memorizzati, elaborati e trasmessi nel sistema, che ha lo scopo di impedire l'utilizzo illegittimo di informazioni riservate.
- L'**integrità**, ovvero la protezione da modifiche non autorizzate dei dati memorizzati, elaborati e trasmessi nel sistema, che ha lo scopo di impedire la manipolazione illegittima delle informazioni. In particolare, garantire l'integrità di un messaggio transitato sulla rete significa assicurare che il messaggio ricevuto sia esattamente quello spedito dal mittente.
- La **disponibilità**, ovvero la capacità di garantire l'accesso ai dati o alle risorse del sistema.
- L' **autenticazione** , ovvero la possibilità di identificare in modo certo e univoco chi invia, manipola e riceve i dati. L'autenticazione è una forma di prova di identità che individua univocamente gli utenti del sistema. L'autenticazione fornisce supporto al non ripudio, che consiste nel dare garanzia che chi trasmette e chi riceve non possano negare di aver inviato e ricevuto il messaggio. Il non ripudio costituisce una prova formale, utilizzabile anche a termine di legge, per dimostrare che una certa persona ha sottoscritto un documento.

Vulnerabilità

La sicurezza delle informazioni è di importanza cruciale in qualunque contesto sociale e lavorativo, anche, ma non solo, in relazione alle leggi relative alla **privacy** e alla protezione dei dati. I problemi sono fondamentalmente dovuti a un insieme di fattori che coinvolgono sia aspetti prettamente tecnici e tecnologici che aspetti organizzativi e di comportamento.

In generale i rischi in termini di sicurezza informatica sono da imputarsi alla vulnerabilità, ovvero alla presenza di lacune o insufficienze nel sistema complessivo del trattamento dei dati. La vulnerabilità può essere addebitata:

- al ***software*** (sia il sistema operativo, sia le applicazioni), che ha raggiunto ormai livelli di enorme complessità e di conseguenza contiene sempre più frequentemente errori (accidentali e non). Sfruttando gli errori diviene possibile attivare funzionalità che rendono un *software*, apparentemente innocuo, un pericolo alla sicurezza dei dati.
- Ai **protocolli di rete**. I *computer* in rete interagiscono con gli altri sistemi connessi attraverso protocolli di comunicazione che possono presentare vulnerabilità. In questo caso un sistema intruso si può inserire in una comunicazione con scopo di convincere un sistema vittima a credere che il sistema intruso possa utilizzare legittimamente i suoi servizi.
- Al **comportamento degli utenti**, che non sempre rispettano norme di sicurezza anche di tipo elementare. In realtà la protezione dei dati dipende prevalentemente dagli utenti che utilizzano i sistemi, poiché nessuno strumento tecnologico può sostituirsi al senso di responsabilità e al rispetto delle norme.

La connessione in sé non è invece una causa, ma piuttosto un mezzo, attraverso il quale avvengono i più frequenti e intrusivi attacchi alla sicurezza dei dati.

Metodologie

Gli amministratori e i responsabili dei sistemi informatici possono provvedere al mantenimento della sicurezza delle informazioni e delle risorse attuando metodologie di tipo proattivo e di tipo reattivo.

Le metodologie proattive consistono in attività di prevenzione che mirano a ridurre al minimo le vulnerabilità del sistema sia dal punto di vista organizzativo che da quello tecnologico. Una semplice strategia proattiva consiste, per esempio, nell'installare sistemi *software* **antivirus** per la rilevazione dei **virus** e nel mantenerli periodicamente aggiornati.

Le metodologie reattive vengono invece attuate ad attacco avvenuto per:

- valutare i danni e le violazioni delle norme;
- identificare i colpevoli;
- segnalare correttamente l'attacco ai responsabili legali della struttura;
- ripristinare i dati e il corretto funzionamento del sistema nel più breve tempo possibile.

Una semplice attività di reazione consiste per esempio nella rimozione dei virus, mediante il *software* antivirus che li ha rilevati.

In generale occorre prevedere la possibilità di essere vittima sia di attacchi esterni che interni, ovvero attacchi condotti da persone che operano all'interno della struttura scolastica e che hanno quindi il vantaggio di essere utenti registrati con diritti di accesso alle risorse. Questa seconda eventualità è realistica solo in scuole i cui studenti abbiano una formazione medio/alta su tematiche correlate alle tematiche TIC, quali ad esempio gli Istituti Tecnici Industriali.

Prevenzione: aspetti organizzativi

Dal punto di vista organizzativo, i responsabili dei sistemi informatici devono avere cura di utilizzare essi stessi politiche di amministrazione atte a prevenire attacchi alla sicurezza. Queste politiche si concretizzano tipicamente:

- in fase di acquisizione di nuove risorse, avendo cura di:
  - optare per sistemi operativi, applicazioni e servizi che offrano supporti al controllo degli accessi e all'implementazione di politiche di accesso articolate.
  - Utilizzare esclusivamente *software* per il quale si dispone di licenza d'uso.
  - Definire regolamenti e politiche di accesso che specifichino le responsabilità e le prerogative degli utenti.
  - Definire e implementare politiche di *backup* dei dati
  - Utilizzare *software* per la rilevazione e rimozione dei **virus** (**antivirus**).
  - Utilizzare sistemi (*hardware* e/o *software*) che consentano il monitoraggio della rete e limitino gli accessi alla rete locale.
- Periodicamente, avendo cura di:
  - aggiornare il *software* scaricando gli opportuni *package*.
  - Aggiornare in particolare gli **antivirus**.
  - Monitorare la rete e i sistemi, alla ricerca di segnali che siano indice di attività potenzialmente pericolose.

Indispensabile è definire a priori quali sono le politiche di accesso alle risorse da parte degli utenti, ovvero chi può accedere a cosa e con che tipo di diritti. Queste politiche devono poi essere implementate utilizzando sistemi operativi e applicazioni che prevedano la gestione di più utenti e meccaniche d'accesso avanzate. Sistemi operativi e applicazioni ad uso personale, che non prevedano politiche di accesso ai *file* e alle risorse, ma consentono a tutti gli utenti l'accesso a tutte le risorse (quali ad esempio *Microsoft Windows98*), rendono impossibile la realizzazione di politiche di sicurezza significative.

Password

Il metodo più semplice per l'accesso illecito a un sistema è quello di impossessarsi indebitamente

della **password** di un utente autorizzato e, spacciandosi per esso, di compromettere riservatezza, integrità, autenticazione e a volte disponibilità dei dati. A ogni utente sono tipicamente assegnate una o più *password*, tra le quali:

- la *password* di accesso al *computer* o al dominio locale, che impedisce l'utilizzo improprio delle risorse interne (*hardware*, *software* e dati).
- La *password* di accesso alla posta elettronica e ai servizi Internet, che identifica l'utente nell'uso delle risorse esterne.

Nella maggior parte dei casi è lo stesso utente che, utilizzando *password* banali o trascrivendole su promemoria, crea le condizioni perché la credenziale sia scoperta da altri.

Per evitare che questo tipo di problema si verifichi è opportuno:

- fornire agli utenti un insieme di regole di comportamento (da sottoscrivere ad esempio al momento della creazione degli *account*), che li responsabilizzino.
- Suggerire agli utenti di utilizzare *password* che siano contemporaneamente semplici da ricordare e non banali.
- Prevedere meccanismi automatici che costringano gli utenti a cambiare periodicamente la *password*.

Regole di comportamento

Definendo il regolamento d'uso delle risorse e in particolare degli *account*, è opportuno suggerire all'utente come comportarsi nella gestione della **password**. Di seguito sono elencati un insieme di semplici suggerimenti che possono costituire una porzione del regolamento:

1. Utilizzare *password* di almeno 6 caratteri e di tipo non banale, ovvero contenenti maiuscole, minuscole e segni di interpunzione. Evitare nomi propri, date o altri riferimenti personali facilmente associabili alla propria persona (come il numero di telefono). Non usare parole che possano essere contenute in un dizionario (in qualsiasi lingua).
2. La *password* è strettamente personale, per cui è opportuno non comunicare a nessuno la *password* e prestare attenzione nel momento dell'immissione per evitare che possa essere compresa da terzi. In caso di dubbio modificare, appena possibile, la *password*.
3. Non trascrivere mai la *password* su promemoria, agende, telefonini o altri supporti. La *password* deve essere ricordata a memoria.

Contestualmente l'utente va responsabilizzato facendogli comprendere che la *password* è il meccanismo di base dell'autenticazione e che terze parti in possesso della sua *password* possono produrre danni ai dati e al sistema in vece sua, sia intenzionalmente che non intenzionalmente.

Altre regole di comportamento da suggerire agli utenti riguardano in generale le loro responsabilità riguardo:

- all'uso corretto delle risorse interne;
- all'uso corretto di Internet e dei suoi servizi (posta elettronica, *chat*, *news*, *Web*, eccetera);
- alla riservatezza delle informazioni.

Infine possono essere suggeriti comportamenti prudenti che evitino la diffusione dei **virus**, come evitare di aprire o visualizzare **attach** ai messaggi di posta provenienti da indirizzi sconosciuti o di utilizzare dischetti senza prima verificarli con un antivirus o scaricare *file* da siti sospetti.

Come scegliere una password

La **password** deve essere di almeno 6 caratteri e deve contenere lettere maiuscole e minuscole, numeri e/o segni di interpunzione. Deve cioè assomigliare a una sequenza di caratteri scelta a caso tra quelli presenti sulla tastiera. *Password* di almeno 8 caratteri sono fortemente consigliate.

Sequenze di caratteri così strutturate sono però difficili da memorizzare per cui vengono suggeriti meccanismi di costruzione della *password*, che consentano di ottenere parole d'ordine non elementari a partire da informazioni mnemoniche. Il metodo più utilizzato per la generazione di *password* con le caratteristiche suddette è quello di scegliere una frase semplice da ricordare e, partendo da questa, costruire una sequenza di caratteri, tipicamente basata sulle iniziali delle parole. Per esempio partendo da Biancaneve e i sette nani si può facilmente ricordare la *password* B-n&i7na.

Di seguito è riportata una tabella con altri semplici casi:

frase	***password***
Alì Babà e i 40 ladroni	@B&i40La
44 gatti in fila per 6 col resto di 2	44Gifx6r2
Art 1. L'Italia è una repubblica fondata sul lavoro	a1:L'IÈ1R

Prevenzione: aspetti tecnici

In generale è obiettivo dell'amministratore e del responsabile dei sistemi evitare qualunque minaccia ovvero qualunque evento o entità che possa danneggiare il sistema compromettendo i dati o i servizi critici. Esistono numerose categorie di minacce che vanno dagli eventi catastrofici naturali e non (incendi, terremoti, alluvioni), agli incidenti che coinvolgono le infrastrutture, casuali o intenzionali (taglio di cavi, sospensione dell'erogazione di corrente), ai veri e propri attacchi alla sicurezza del sistema.

Un **attacco** è un tentativo di accesso o d'uso non autorizzato dei dati e dei sistemi, che mira a compromettere riservatezza, integrità, disponibilità, autenticazione e/o non ripudio. L'attacco non è di per sé necessariamente fruttuoso, ma può fallire grazie alle politiche di sicurezza proattiva che sono state realizzate. Se l'attacco ha successo, si è di fronte a un incidente che ha inciso sulla sicurezza informatica della struttura.

Si distinguono due tipologie di attacchi:

- **attacchi passivi**, che hanno l'obiettivo di compromettere la riservatezza e l'autenticazione, entrando in possesso di informazioni private.
- **Attacchi attivi**, che hanno l'obiettivo di compromettere l'integrità e la disponibilità, ovvero mirano ad alterare le informazioni e/o danneggiare i sistemi.

Molto spesso gli attacchi passivi sono effettuati per ottenere le informazioni necessarie a iniziare un attacco attivo.

Alcuni attacchi

Le tipologie di attacco alla sicurezza di sistemi sono fortemente variegate e vengono continuamente prodotti nuovi attacchi che sfruttano le diverse vulnerabilità.

In questo contesto introdurremo diversi attacchi, senza l'ambizione di fare un elenco esaustivo, ma con l'obiettivo di introdurre alcuni tra i meccanismi più diffusi e più pericolosi, ovvero:

- **abuso dell'identità elettronica**,

- **exploit**,
- **malicious software**,
- **sniffing**,
- **spoofing**,
- **Denial of service**.

Abuso dell'identità elettronica

L'identità elettronica degli utenti può essere sostituita in modo malizioso intercettando le credenziali di autenticazione (ad esempio la *password*) sia al di fuori del sistema (attraverso confidenze o promemoria), sia sfruttando vulnerabilità dei sistemi interni (ad esempio con un **cavallo di Troia**), sia mentre queste credenziali transitano sulla rete.

In questo caso, utilizzando le credenziali dell'utente ottenute maliziosamente è possibile sostituirsi ad esso. I problemi più gravi si hanno:

- quando l'abuso produce gravi violazioni alle norme vigenti.
- Quando l'abuso avviene in un contesto commerciale e dà origine a obblighi per la persona la cui identità è stata utilizzata impropriamente.
- Quando viene abusata l'identità dell'amministratore del sistema e, dunque, si è resa possibile la compromissione completa della sicurezza dei dati e delle risorse.

In particolare in questo caso sono colpiti:

- l'autenticazione, poiché qualunque azione compiuta dall'utente sostituito è stata in realtà compiuta da altri.
- Il non ripudio, poiché l'utente abusato può negare di aver partecipato ad una comunicazione e/o di avere sottoscritto un accordo.
- La riservatezza e l'integrità dei dati che sono rispettivamente visibili e scrivibili dall'utente la cui identità è stata utilizzata impropriamente.

Molte volte l'abuso dell'identità elettronica è il primo passo di attacchi più complessi e distruttivi ed è utilizzato proprio per rendere difficile l'identificazione di chi ha compiuto azioni dannose e criminali.

Exploit

Le vulnerabilità dei programmi sono tipicamente generate da un errore nella progettazione o nell'implementazione del *software*. Si indica tipicamente con **exploit** l'esecuzione delle azioni necessarie ad approfittare di una vulnerabilità del sistema per sferrare un attacco. La vulnerabilità in se può essere sfruttata solo mettendo in opera un procedimento apposito, il più delle volte complesso, volto a sfruttarla per danneggiare la sicurezza del sistema.

Possono essere vulnerabili sia i sistemi ad uso personale sia i *server*, ma gli *exploit* avvengono più frequentemente sui *server* che, essendo sempre accesi e connessi, sono maggiormente esposti. Le vulnerabilità del *software* possono dipendere a volte da errate configurazioni ed installazioni, fatte dall'amministratore o dagli stessi utenti, che rendono un sistema robusto facilmente accedibile dall'esterno. Ad esempio concedere l'uso di programmi che operano in modalità superutente, aumenta notevolmente il grado di vulnerabilità del sistema operativo.

Esistono appositi *tool* che consentono di scoprire le vulnerabilità presenti in un certo sistema, attraverso un insieme di operazioni di *vulnerability assessment*. La migliore difesa verso la vulnerabilità del *software* resta comunque il frequente aggiornamento e l'installazione di tutti i moduli di correzione offerti dal produttore (*patch*).

Software doloso (malicious software o malware)

Il *software* doloso (**malicious software**, contratto a volte nel neologismo ***malware***) è un *software* o una porzione di *software* che produce effetti dannosi o non desiderati. Questo tipo di programmi è dunque da considerarsi nocivo, ovvero potenzialmente lesivo della sicurezza del sistema.

Esistono diverse tipologie di *software* doloso tra cui i più noti e diffusi sono **virus**, ***worm*** e **cavalli di Troia**:

- **Cavalli di Troia**: sono programmi apparentemente innocui che una volta eseguiti, effettuano operazioni diverse da quelle per le quali l'utente li aveva utilizzati e tipicamente dannose. Un esempio di cavallo di troia molto semplice è la creazione di una finestra di *login* identica a quella del sistema ma finta, che invia *password* e altre informazioni riservate all'autore del *software* doloso. Spesso quando un sistema viene compromesso l'intruso inserisce cavalli di troia con lo scopo di mascherare l'attacco, procurarsi informazioni aggiuntive e creare un accesso (***backdoor***) da sfruttare successivamente.
- **Virus**: sono porzioni di codice che realizzano tipicamente due attività:
  - quello di replicarsi e inserire se stessi in *file* eseguibili preesistenti sul sistema. Questa attività mira alla diffusione del virus.
  - Quello di compromettere l'integrità delle informazioni e la disponibilità delle risorse. Questa fase attiva del virus viene avviata a scoppio ritardato in modo da consentire una prima fase di diffusione dell'infezione e tipicamente comprende l'aggressione ai dati e ai programmi contenuti nella memoria di massa del sistema.

  Su questo argomento è disponibile un ulteriore **approfondimento**.
- **Worm**: sono programmi che utilizzano i servizi di rete per propagarsi da un sistema all'altro. Agiscono creando copie di se stessi sugli *host* ospiti e mettendosi in esecuzione. Sono dunque auto-replicanti e autosufficienti poiché in grado di funzionare senza bisogno di un programma ospite.

Sniffing

Lo **sniffing** è un attacco di tipo passivo che mira a compromettere riservatezza e autenticazione effettuando intercettazioni delle comunicazioni. Quando i dati viaggiano non criptati su una rete a mezzo condiviso (come sono tipicamente le LAN) è possibile da un qualsiasi punto della rete intercettare i pacchetti in transito destinati ad altri *host*. È particolarmente critica la fase in cui il *client* invia, in chiaro, a un *server* le informazioni relative all'autenticazione dell'utente. Per questo motivo è opportuno utilizzare servizi che prevedano la trasmissione **cifrata** delle *password*.

L'intercettazione dei dati è fatta attraverso appositi strumenti detti ***sniffer***, che raccolgono le informazioni in transito ed effettuano su di esse diverse operazioni:

- conversione dei pacchetti in una forma leggibile e filtraggio in base a criteri definibili dall'utente. Il filtraggio è tipicamente applicato alle *password* e agli *account*.
- Monitoraggio della rete, sia in termini di performance, che di traffico e di errori, anche attraverso la manutenzione di appositi *log*.

Spoofing

Vengono indicati con il termine **spoofing** diversi tipi di attacchi che hanno come meccanica comune quella della sostituzione. In particolare:

- se ci si sostituisce a un utente senza averne diritto, ovvero se si utilizza una qualche forma di abuso dell'identità elettronica, si sta facendo ***user account spoofing***.
- Se si prende il controllo di un canale di comunicazione e su questo si modifica il contenuto dei pacchetti, si sta facendo ***data spoofing***.
- Se si manipola l'indirizzo IP da cui parte una certa connessione in modo da far credere di essere un sistema sorgente differente, si sta facendo ***IP spoofing*** (o ***IP address spoofing***).

Tra questi tipi di attacchi, l'*IP spoofing* è il più noto e diffuso, e ha come obiettivo quello di aggirare i principali controlli attivi effettuati per garantire la sicurezza, che sono appunto basati sul monitoraggio dei numeri IP. Il sistema che effettua l'attacco si spaccia per un diverso IP mentre il sistema che subisce l'attacco invia le risposte all'*host* effettivamente corrispondente all'IP utilizzato per lo *spoofing*.

Lo *spoofing* di indirizzo può essere fatto dall'interno o dall'esterno della sottorete. Lo *spoofing* esterno è più complesso da realizzare perché l'*host* attaccato e quello attaccante non utilizzano mezzi condivisi.

Negazione di servizio (Denial of service)

Gli attacchi di tipo **Denial of service** hanno come principale bersaglio la disponibilità delle risorse, in particolare dei sistemi e dei servizi. Lo scopo di chi tenta l'attacco non è quindi quello di ottenere informazioni o di modificarle, quanto quello di impedire ad altri l'accesso alle informazione, anche quando autorizzati, ovvero di negare loro il servizio.

Il risultato di un attacco di questo tipo è dunque l'interruzione di un servizio che risulta indisponibile agli utenti legittimi. Alcune volte questo effetto è ottenuto rendendo le risorse troppo impegnate, in modo da provocare risposte negative a richieste di servizio legittime. Altre volte invece il sistema viene mandato in *crash* e necessita dell'intervento dell'amministratore per riprendere il corretto funzionamento e l'erogazione dei servizi.

Spesso l'attacco ha come obiettivo quello di tenere la vittima occupata, mentre sta avvenendo qualche altra aggressione più critica al sistema. L'autore dell'attacco tipicamente maschera il proprio indirizzo in modo da rendere impossibile o quantomeno molto difficoltoso rintracciarlo. *Denial of service* famosi hanno avuto come bersaglio siti di grandi dimensioni, come ad esempio *Yahoo*.

Due forme molto semplici e diffuse di *Denial of service* sono:

- il ***mail bombing***, che è realizzato inviando a un utente una quantità di posta sufficiente a riempire lo spazio disponibile e dunque bloccare il suo servizio di ricezione.
- La ***bandwidth consumption***, che consiste nel generare una quantità elevatissima di traffico verso una certa destinazione, occupando tutta la larghezza di banda disponibile ed impedendo così ad altri di usufruire dei servizi messi a disposizione da quel nodo.

Alcune contromisure

Di fronte alle innumerevoli tipologie di **attacco** risulta fondamentale operare per ridurre al minimo le vulnerabilità. Oltre alla manutenzione del *software* e alle altre linee guida per la prevenzione dei problemi, è utile e a volte indispensabile dotarsi di tecnologie *hardware* e *software* dedicate alla tutela della sicurezza e alla prevenzione degli attacchi.

Tra queste, ne citiamo alcune particolarmente utili e significative:

- la **crittografia**, che consente di far transitare sulla rete messaggi cifrati nascondendone il contenuto e inoltre offre supporto di base alla certificazione e alla della firma digitale.
- I *software* **antivirus**, che consentono di rilevare e rimuovere i **virus**.
- I **firewall**, ovvero sistemi di filtraggio delle informazioni utilizzati per creare una barriera difensiva perimetrale, ovvero per rendere più difficili gli attacchi ai sistemi di una LAN prevenendo gli accessi non autorizzati.

Crittografia

Il successo di alcuni attacchi può essere inibito mediante la trasmissione di messaggi crittografati, ovvero codificati in modo da non poter essere compresi.

Il modello crittografico funziona nel modo seguente: i messaggi da codificare, detti **in chiaro**, sono cifrati mediante una funzione la cui computazione dipende da un parametro detto **chiave**. Il messaggio viene quindi trasmesso in forma crittografata e può essere riportato alla forma in chiaro soltanto da chi possiede la chiave atta alla decifratura. Eventuali intrusi che riuscissero a intercettare la comunicazione, ma non fossero in possesso della chiave di decifratura, non riuscirebbero a ricostruire il messaggio originale.

In tempi passati, quando la **crittografia** veniva utilizzata prevalentemente per uso militare e con mezzi trasmissivi tradizionali, la segretezza del meccanismo veniva riposta in due fattori:

- il metodo con cui avveniva la crittografazione e dunque la decrittografazione, ovvero le funzioni di codifica e di decodifica.
- Le chiavi di crittografazione e decrittografazione ovvero i parametri da passare rispettivamente alle funzioni di codifica e di decodifica.

Sulla rete utilizzare un algoritmo privato di crittografazione può significare limitare il numero dei potenziali destinatari dei messaggi, per cui tipicamente la segretezza è riposta esclusivamente nella chiave. I meccanismi di crittografia sono alla base delle diverse forme di certificazione a disposizione su Internet e del funzionamento della firma digitale.

Su questo argomento è disponibile un ulteriore **approfondimento**.

Antivirus

L'unico sistema efficace per prevenire danni derivanti dalla diffusione di **virus** è l'utilizzo di appositi *software* **antivirus** il cui obiettivo è identificare il virus e rimuoverlo prima che entri in azione. Per rilevare la presenza di un virus i *software* antivirus cercano all'interno della memoria (centrale e di massa) particolari sequenze di *byte* che costituiscono l'impronta identificativa del virus. La continua produzione di nuovi virus rende quindi indispensabile un aggiornamento continuativo del *software* antivirus per garantirne l'efficacia nel tempo. Alcune volte i *software* antivirus sono in grado di rilevare anche virus di cui non conoscono la sequenza di *byte* identificativa, riscontrando su base probabilistica comportamenti anomali o sospetti.

Le verifiche del *software* antivirus vengono tipicamente fatte in via automatica:

- all'avvio del sistema, verificando almeno il *Master Boot Record* e i *file* di sistema.
- Periodicamente, scandendo la memoria centrale.
- Ogniqualvolta si effettua una operazione rischiosa (come l'apertura di un **attach** di posta elettronica, l'inserimento di un dischetto nel *drive*, il *download* di un *file*), verificando i *file* potenzialmente pericolosi.

Le attività dei *software* antivirus rallentano le prestazioni del sistema, richiedendo continue scansioni

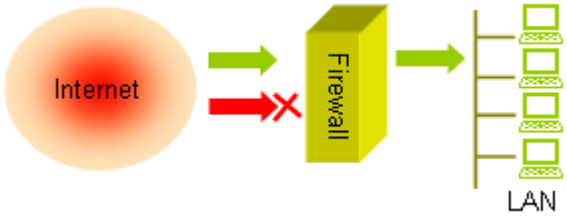
della memoria e del disco. Per esempio è possibile effettuare scansioni periodiche non automatiche di tutto il *filesystem* da attivare in momenti in cui il sistema non è utilizzato. Per questo motivo alcune attività di verifica vengono attivate su richiesta.

Su virus e antivirus è disponibile un ulteriore **approfondimento**.

Firewall

Un **firewall** è un sistema connesso alla rete con lo scopo di filtrare i pacchetti in transito. Tipicamente viene posto a bordo della rete con lo scopo di creare una barriera difensiva che aumenti il grado di sicurezza perimetrale, ovvero renda più difficile gli attacchi dall'esterno all'interno del sistema.

Un *firewall* può essere realizzato sia come infrastruttura *hardware* dedicata che utilizzando un *computer* e un opportuno insieme di *software*. Deve essere posto sul bordo (logico) della LAN se si desidera far passare per il *firewall* tutti i pacchetti in entrata e in uscita dalla rete locale. Il *firewall* controlla il flusso dei pacchetti, ovvero decide se consentire o negare l'accesso, implementando delle specifiche politiche di filtraggio del traffico.



Utilizzare un *firewall* significa dunque decidere e implementare delle politiche di sicurezza (*security policy*) che definiscono i criteri di protezione, ad esempio decidendo che è ammesso solo il traffico generato da alcuni servizi (la posta o il *Web*) e non traffico derivante da servizi non standard (che potrebbero rendere possibile o nascondere un attacco).

Si possono distinguere diverse tipologie di *firewall* che utilizzano meccanismi di verifica con differenti livelli di sofisticazione. In particolare i *firewall* più semplici filtrano i pacchetti esaminando le informazioni contenute nell'intestazione e, confrontandole con le *security policy*, decidono se autorizzare o no il transito. Offrono invece una protezione più completa i *firewall* che esaminano anche il contenuto dei pacchetti in transito, con lo scopo di assicurasi che il sistema di destinazione dei messaggi sia realmente in attesa, ad esempio che lo scaricamento di una *mail* sia stato richiesto dal *client*.

Conclusioni

Questa breve trattazione dei problemi correlati alla sicurezza informatica e delle principali metodiche di prevenzione ha avuto lo scopo di introdurre una tematica complessa ed in continua evoluzione. In particolare si è voluto dare enfasi al fatto che un buon sistema organizzativo e un insieme di regole formalizzato, costituiscono un elemento indispensabile nell'attuazione di politiche di prevenzione dei problemi di sicurezza.

Ad esso va affiancato un opportuno insieme di tecnologie *hardware* e *software* che consentono all'amministratore e al responsabile dei sistemi di prevenire le forme più frequenti di attacco e di recuperare in caso in cui questo abbia successo, ripristinando rapidamente le funzionalità dei sistemi.

Sono disponibili approfondimenti relativi alle seguenti tematiche correlate:

- **i virus**,
- **la crittografia**,
- **la privacy**.

I **riferimenti bibliografici** *on line* consentono di svolgere autonomamente ulteriori attività di approfondimento.