Le workstation che possiedono applicazioni anti virus devono controllare tutti i dati che vengono immessi sul sistema.

I programmi non devono essere aperti senza essere prima sottoposti ad un'analisi. Tutti i file trasmessi attraverso la rete (comprese le e-mail) devono essere analizzati al momento della ricezione. L'analisi delle informazioni in transito tra interno ed esterno deve avvenire al perimetro della rete effettuando l'analisi attraverso i sistemi di accesso (firewall o server posta). Tale approccio permette il controllo e la gestione dei sistemi anti virus in modo centralizzato e rende più efficiente:

- L'uso delle risorse di elaborazione dei sistemi (l'analisi avviene una sola volta).
- L'amministrazione.
- L'aggiornamento dei sistemi anti virus.

Funzioni dei programmi antivirus

Un programma che si proponga di instaurare un livello sufficiente di sicurezza e protezione da virus informatici deve essere dotato di precise funzioni.

Il sistema di difesa dovrà avere:

- Il modo di funzionamento non intrusivo nei confronti del sistema, con impatto minimo e possibilità di ottimizzazione dell'occupazione di memoria.
- La presenza di funzioni di individuazione virus di bootstrap e di file.
- La possibilità di individuare i virus residenti in memoria è un requisito fondamentale del prodotto antivirus: in caso contrario, il prodotto stesso può divenire veicolo di propagazione.
- La possibilità di scoprire virus auto-mutanti (polimorfi).
- La possibilità di individuare infezioni relative al settore Master Boot Record.
- La possibilità di individuazione dei virus in file compressi. Il virus può essere localizzato all'interno del file compresso, o all'esterno del file ma compresso con esso.
- La possibilità di dirottare l'output su file o stampante: ciò risulta particolarmente utile in caso di numero elevato di file infettati, o rimozioni incomplete.