ATTIVITÀ SVOLTE DA:

IT SECURITY
SICUREZZA INFORMATICA

**IMPLEMENTAZIONE E GESTIONE DELLA SICUREZZA INFORMATICA**

**SICUREZZA PERIMETRALE**

**PROGETTAZIONE E REALIZZAZIONE DI RETI LOCALI E GEOGRAFICHE**

**CONTRATTI DI MANUTENZIONE E ASSISTENZA TECNICA HARDWARE E SOFTWARE**

**ANALISI, PROGETTAZIONE E REALIZZAZIONE DI SISTEMI INFORMATICI, SERVIZI E ARCHITETTURE DI RETE**

**PROGETTAZIONE E REALIZZAZIONE DI SISTEMI DI VIDEOSORVEGLIANZA SU IP**

**PRODUZIONE E VENDITA DI PERSONAL COMPUTERS E ACCESSORI**


**IT SECURITY**

Via San Jachiddu, 90 (Pal. 16 scala H)
**98152 - MESSINA**

Tel./Fax 090 5731585
Cell. 347 8103539

**www.itsecur.it**
e-mail: giuseppe.ferrito@itsecur.it


IT SECURITY
SICUREZZA INFORMATICA

**Siete certi che il vostro sistema informatico sia sicuro? L'unica vostra certezza è l'incertezza!**

SECURITY
SICUREZZA INFORMATICA

Microsoft
Authorised Education Reseller 2004

IBM Business Partner

NOD32

FORTINET

D-Link

KERIO

INTELLINET

Business Service Provider
TELECOM

CLUSIT

## Cosa è la sicurezza informatica?

Per definizione banale e restrittiva la sicurezza informatica si occupa di rendere vani i tentativi di attacco passivo e attacco attivo che possono essere perpetrati ai danni di un'azienda o di un privato.

La prevenzione dagli attacchi passivi copre gli aspetti che riguardano la creazione di un ambiente di rete sicuro tale da poter garantire la circolazione dei dati senza che questi possano essere in qualche modo intercettati, manipolati, interrotti o letti.

La prevenzione dagli attacchi attivi copre gli aspetti che riguardano le contromisure da apportare per evitare che ipotetici intrusori o virus/worm possano appropriarsi delle password di accesso o sfruttare le vulnerabilità di un sistema, tali da poter consentire la consultazione fraudolenta dei dati desiderati.

La semplice applicazione di una password è quindi da considerarsi una misura di sicurezza flebile: se il sistema è afflitto da una o più vulnerabilità l'intrusore avrà comunque modo di superarla.

## Ma cosa è una vulnerabilità?

Una vulnerabilità è un problema di programmazione "involontario" che affligge un software (sia esso un sistema operativo, un programma per la gestione della posta, un programma per la navigazione nelle pagine internet, etc.) e consente ad un ipotetico intrusore di sfruttarne la potenzialità a piacimento in modo da accedere ai dati desiderati. Nessun software è immune da vulnerabilità: per questo una volta acquisito ha bisogno di essere controllato, gestito e mantenuto nel tempo. Gli stessi software o apparati che facilitano l'implementazione della sicurezza informatica hanno bisogno di essere mantenuti e aggiornati nel tempo. Una vulnerabilità è come una porta lasciata aperta per sbaglio che conduce alla cassaforte principale di una banca; il ladro non avrà bisogno di provare a scassinare altre porte se avrà la bravura di scoprire il percorso meno accidentato.

## Qual è il modo migliore per fare sicurezza?

Il punto è certamente l'outsourcing: se si è una piccola o media azienda è sempre meglio affidarsi a chi fa della sicurezza informatica il proprio lavoro e non tentare di risolvere il problema internamente.

Per le grosse aziende può certamente far comodo implementare la sicurezza in outsourcing in aree ben prefissate o affidarsi ad esperti del settore per testare il grado di affidabilità delle strutture o degli apparati configurati da terzi.

## Come essere certi di affidare il lavoro in outsourcing ad aziende competenti?

Anzitutto bisogna diffidare da chi dichiara di fornire soluzioni standard per ogni evenienza. In realtà ogni rete (per quanto simile strutturalmente) presenta differenze e problematiche eterogenee, a partire per esempio dal tipo di dato (e quindi dal traffico) che circola.

Le soluzioni vincenti e soprattutto funzionanti sono quelle che si adattano alla rete dopo averne analizzato le caratteristiche hardware e software. **Chi effettua un'analisi preventiva della struttura del network sarà certamente un professionista del settore.**

Non esistono quindi soluzioni standardizzate, semmai customizzabili (cioè personalizzate all'esigenza).

Bisogna anche evitare chi vuole applicare l'antica tecnica del "piazza e fuggi". Diffidare da chi vuole vendere un prodotto senza poi parlare dei relativi costi di manutenzione ed aggiornamento. Impensabile, per esempio, che un firewall venga venduto e non abbia bisogno di essere mantenuto ed aggiornato a nuove tecniche di disturbo per sempre o per tempi relativamente lunghi.

Ciò vale per qualsiasi altro apparato o servizio che si intende acquistare.

La rapidità di circolazione delle informazioni, la facilità del loro accesso e utilizzo, la sicurezza del contenuto sono fattori indispensabili per il buon funzionamento di una attività.

I rischi legati all'insicurezza dei sistemi informatici possono comprometterne i risultati.

Con l'avvento della New Economy, questi fattori diventano vitali per la sopravvivenza delle aziende.

I responsabili devono prendere decisioni e accorgimenti per prevenirne le cause e limitarne gli effetti.

La consapevolezza, la formazione, il continuo aggiornamento professionale e lo scambio di informazioni sono gli strumenti più efficaci per far fronte al problema.

## Finalità dei controlli di sicurezza

Nella società della comunicazione il valore e la riservatezza delle informazioni riveste un ruolo sempre più importante. Di conseguenza la sicurezza dei dati, in tutte le sue forme, è un aspetto fondamentale per la gestione e l'utilizzo di un Sistema Informativo.

Il controllo del livello di sicurezza di un Sistema richiede competenze tecniche specifiche e capacità specialistiche tali da rendere massimo il livello delle verifiche da effettuare sul Sistema. Inoltre è necessario un costante aggiornamento sulle possibili tipologie di crimini informatici e sulle tecniche di protezione.

La sicurezza di un Sistema deve essere assicurata per evitare:

- Il blocco delle attività del Sistema o il degrado delle prestazioni dovuto ad un utilizzo non autorizzato.
- Il furto, la modifica o la distruzione di informazioni.
- Il furto, la modifica o la distruzione di programmi.

La modifica dei programmi può essere effettuata per "sproteggere" ulteriormente il Sistema ospite.

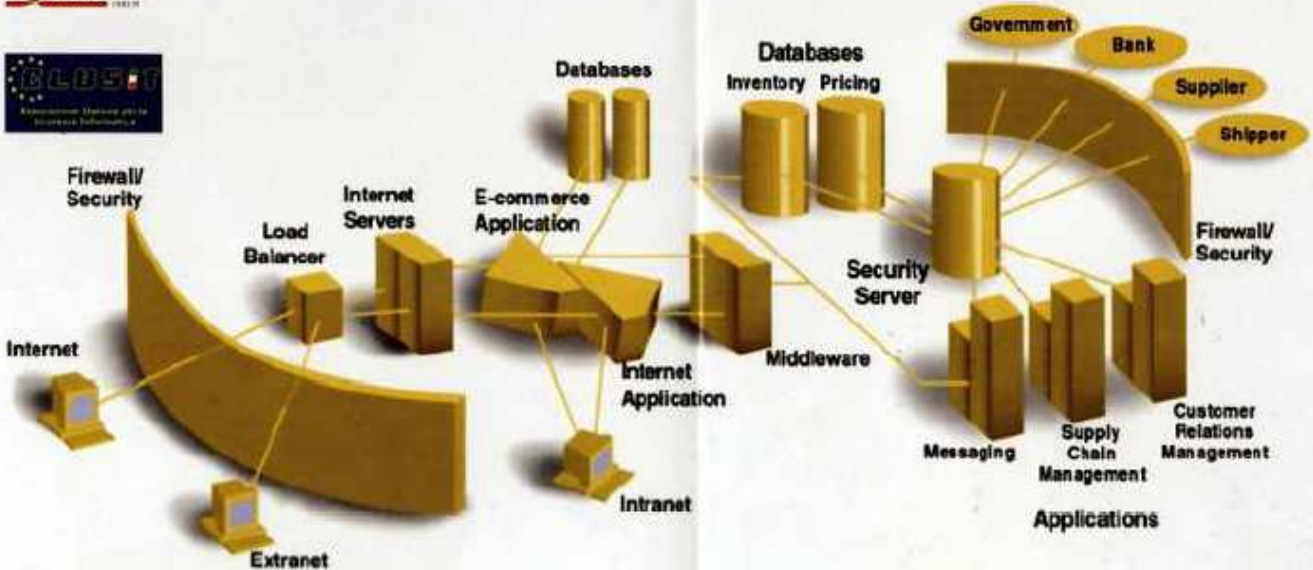
La sicurezza di un Sistema viene assicurata mediante un insieme coordinato di azioni:

- Definizione delle procedure di sicurezza e degli accessi del personale.
- Utilizzo di strumenti di sicurezza software.
- Garanzia della sicurezza fisica.
- Garanzia delle sicurezza sulle linee di comunicazione.

Un Sistema non può venire definito sicuro in termini assoluti.

Esiste sempre, almeno teoricamente con probabilità non nulla, un modalità di accesso al Sistema.

Un sistema sicuro è un sistema spento: anche questa battuta presenta un rischio ... forse qualcuno può riaccenderlo!




Stringraia Marco Orlisi