Sicurezza informatica

In un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento, la salvaguardia dei sistemi informatici dalla violazioni dei dati e’ diventata una necessità inderogabile. Esistono, a carico delle imprese, precisi obblighi in materia di privacy ed è stato approvato in ambito comunitario il nuovo Standard ISO 27001:2005 che ha proprio l'obiettivo di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (ISMS) finalizzato ad una corretta gestione dei dati sensibili dell’azienda.

Si distinguono i concetti di sicurezza passiva e di sicurezza attiva.

Sicurezza passiva

Per sicurezza passiva normalmente si intendono le tecniche e gli strumenti di tipo difensivo, ossia quel complesso di soluzioni il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata. Il concetto di sicurezza passiva pertanto è molto generale: ad esempio, per l'accesso a locali protetti, l'utilizzo di porte di accesso blindate, congiuntamente all'impiego di sistemi di identificazione personale, sono da considerarsi componenti di sicurezza passiva.

Sicurezza attiva

Per sicurezza attiva si intendono, invece, le tecniche e gli strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi (confidenzialità), sia dalla possibilità che un utente non autorizzato possa modificarli (integrità).

E' evidente che la sicurezza passiva e quella attiva sono tra loro complementari ed entrambe indispensabili per raggiungere il desiderato livello di sicurezza di un sistema.

Spesso l'obiettivo dell'attaccante non è rappresentato dai sistemi informatici in sé, quanto piuttosto dai dati in essi contenuti, quindi la sicurezza informatica deve preoccuparsi di impedire l'accesso ad utenti non autorizzati, ma anche a soggetti con autorizzazione limitata a certe operazioni, per evitare che i dati appartenenti al sistema informatico vengano copiati, modificati o cancellati.

Le violazioni possono essere molteplici: vi possono essere tentativi non autorizzati di accesso a zone riservate, furto di identità digitale o di file riservati, utilizzo di risorse che l'utente non dovrebbe potere utilizzare ecc. La sicurezza informatica si occupa anche di prevenire eventuali Denial of service (DoS). I DoS sono attacchi sferrati al sistema con l'obiettivo di rendere non utilizzabili alcune risorse in modo da danneggiare gli utilizzatori del sistema. Per prevenire le violazioni si utilizzano strumenti hardware e software.

Tra i primi occupano una posizione preminente i cosiddetti firewall: la loro funzionalità principale in sostanza è quella di creare un filtro sulle connessioni entranti ed uscenti, applicando regole che contribuiscono alla sicurezza della rete informatica.

Tra i secondi ci limitiamo a segnalare i programmi antivirus, che tutti conosciamo e che vanno tenuti costantemente aggiornati, ed i firewall software che effettuano un controllo dei programmi che tentano di accedere ad internet dal computer nel quale il firewall è installato, consentendo all'utente di impostare delle regole che possano concedere o negare l'accesso ad internet da parte dei programmi stessi.