Tema sicurezza informatica

La sicurezza informatica detta (information security) è l'insieme dei mezzi e delle tecnologie tesi alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici; a questi tre parametri si tende attualmente ad aggiungere l'autenticità delle informazioni.

É in linguaggio tecnico chiamato cybersecurity termine che ne rappresenta una sottoclasse essendo quell'ambito della sicurezza informatica che dipende solo dalla tecnologia. Con esso si enfatizzano spesso qualità di resilienza, robustezza e reattività che una tecnologia deve possedere per fronteggiare attacchi mirati a comprometterne il suo corretto funzionamento e le sue performance (attacchi cyber).

Nella sicurezza informatica sono coinvolti elementi tecnici, organizzativi, giuridici e umani. Per valutare la sicurezza è solitamente necessario individuare le minacce, le vulnerabilità e i rischi associati agli asset informatici, al fine di proteggerli da possibili attacchi (interni o esterni) che potrebbero provocare danni diretti o indiretti di impatto superiore a una determinata soglia di tollerabilità (es. economico, politico-sociale, di reputazione) a un'organizzazione.

Aspetti generali

La sicurezza informatica è un problema molto sentito in ambito tecnico-informatico per via della crescente informatizzazione della società e dei servizi (pubblici e privati) in termini di apparati e sistemi informatici e della parallela diffusione e specializzazione degli attaccanti o cracker.

L'interesse per la sicurezza dei sistemi informatici è dunque cresciuto negli ultimi anni, proporzionalmente alla loro diffusione e al ruolo da essi svolto nella collettività.

Sicurezza domestica e nelle aziende

dal momento che l'informazione è un bene aziendale, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento. Per questo esistono, a carico delle imprese, precisi obblighi in materia di privacy, tra cui quello di redigere annualmente uno specifico documento programmatico sulla sicurezza. La materia privacy è però estremamente limitativa trattando unicamente il tema della protezione dei dati personali, escludendo tutto il resto; la legge sulla privacy infatti non impone alcuna protezione per informazioni prive di dati personali. Spesso si fa confusione tra tutela dei dati personali e sicurezza delle informazioni tout court (informazioni riservate e confidenziali ma che nulla hanno che vedere con dati personali).

Esiste a livello internazionale la norma ISO 27001 finalizzata alla standardizzazione delle modalità adatte a proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità. Lo standard indica i requisiti di un adeguato sistema di gestione della sicurezza delle informazioni (SGSI; in inglese Information security management system o ISMS) finalizzato a una corretta gestione dei dati dell'azienda. Una fase indispensabile di ogni pianificazione della sicurezza è la valutazione del rischio e la gestione del rischio. Le organizzazioni possono far certificare ISO 27001 il proprio SGSI.