Politica di sicurezza

Politica di sicurezza

Definisce un insieme di regole che precisano in quale modo i dati e le risorse devono essere gestite, protette e distribuite all'interno del sistema.

Prevede:

- Un sistema d'identificazione degli utenti
- Una politica degli accessi
- Meccanismi logici e meccanici di protezione dell'integrità dei dati
- Misure normative ed organizzative adeguate

Esistono due filosofie che vengono adottate per lo sviluppo della politica di sicurezza:

1. "ciò che non è espressamente permesso è proibito"
2. "ciò che non è espressamente proibito è permesso"

Politica di sicurezza

- E’ importante che vengano anche definite le azioni che devono essere compiute nell'eventualità che la sicurezza della organizzazione sia compromessa.
- Ogni volta che questa viene violata, deve essere modificata per rimuovere le cause alla base della violazione
- Bisogna inoltre sviluppare procedure e piani che salvaguardino le proprie risorse da perdite e danneggiamenti; tuttavia il loro costo deve essere proporzionato ai beni da proteggere e alle probabilità di subire attacchi.

Analisi dei Rischi

L’analisi dei rischi consiste nel determinare:

- le risorse che è necessario proteggere
- le tipologie di rischi a cui sono potenzialmente esposte
- definizione di strategie atte a garantirne la protezione in relazione all’entità dei danni che deriverebbero da una loro compromissione\indisponibilità

Esempio

Uso delle risorse e disponibilità

- Bisogna effettuare una classificazione degli utenti, sia interni che esterni al sistema, che necessitano di accedere alle risorse.
- Si devono fornire delle linee di comportamento che definiscono l'uso corretto delle risorse.
- Devono essere definiti i "privilegi" dei vari utenti e le loro responsabilità quando utilizzano le risorse ed i servizi di rete.

Violazione sicurezza

- Ogni volta che viene violata la politica di sicurezza il sistema si trova esposto a minacce.
- Si deve classificare se tale violazione si è verificata a causa della negligenza di un utente, di un incidente, di un errore, della non conoscenza o non curanza della politica corrente.
- In ciascuna di queste circostanze, la politica di sicurezza, dovrebbe fornire delle direttive circa le azioni immediate da adottare.

Disaster Recovery Plan

Piano di ripristino a seguito di eventi catastrofici

- Procedure per il ripristino dell'attività delle macchine
- Procedure per il recupero di dati persi
- Procedure di continuità operativa