- Come e quando l'organizzazione deve cooperare con altre per cercare di risalire all'intruso
- Se l'intrusione deve essere fermata immediatamente dopo il rilevamento o l'intruso deve poter continuare la sua attività, per poterla registrare e utilizzare come prova

Come rilevare un incidente

Per stabilire se un determinato comportamento sospetto é indicativo di un incidente, bisogna analizzarlo alla luce delle seguenti considerazioni:

- discrepanze nell'uso degli account;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

Ovviamente, per rilevare anomalie bisogna avere un'idea precisa di che cosa possa essere considerato "normale". L'utilizzo di strumenti automatici per la rilevazione dell'andamento del traffico può senz'altro aiutare. Inoltre, invece di illudersi sulla possibilità di rilevare e bloccare tutte le intrusioni sul nascere, é preferibile concentrarsi su procedure che consentono di limitare l'impatto delle violazioni. Data l'enorme diversità degli attacchi, l'impiego di strumenti automatici é fondamentale. I sistemi di rilevamento automatico delle intrusioni si basano su di una combinazione di analisi statistiche e verifica della rispondenza alle regole.

Squadra di pronto intervento (CERT-AM)

Deve essere costituita una squadra di intervento per gli incidenti, in modo da poterli limitare e prevenire in maniera efficace ed economica.

La maggior parte dei programmi per la sicurezza informatica non sono efficaci quando si tratta di gestire nuove classi di minacce poco diffuse. Le risposte tradizionali, cioè l'analisi del rischio, la pianificazione delle emergenze e della revisione della sicurezza dei computer, non sono in genere sufficienti per controllare incidenti e per prevenire gravi danni relativamente a minacce poco probabili o poco note, quindi si devono attivare procedure organizzative reattive anziché misure tecnologiche protettive che potrebbero risultare troppo onerose.