- Modifiche alle configurazioni dell'applicazione;
- Accesso ai dati (inserimento, modifica, lettura, rimozione), ai file e alle risorse dell'applicazione e tipo di accesso;
- Disattivazione del meccanismo di tracciamento;
- La procedura di tracciamento sarà predisposta per l'emissione di "Alert" al verificarsi di uno o più eventi configurabili dall'amministratore del sistema.

5.4.2 Tracciamento eventi di "Alarm Detection"

Oltre ad attenersi alle prescrizioni riportate nei paragrafi precedenti, durante lo sviluppo del codice è essenziale inserire particolari funzioni di tracciamento che, operanti in determinati e specifici punti dell'applicativo, permettano la rilevazione e il logging di eventi anomali o di frode, significativi per la sicurezza dell'organizzazione.
Attraverso l'inserimento di specifiche stringhe di codice all'interno dell'applicativo, si vogliono rilevare alcuni eventi ritenuti sensibili ai fini del mantenimento della riservatezza, integrità e disponibilità del dato applicativo.
In seguito, le segnalazioni prodotte e inserite in appositi file di Log, discriminate per mezzo di TAG (DetCode) opportuni, possono essere elaborate da un sistema di correlazione e utilizzate come fonte per attività di Audit (Ex/Post) degli eventi di sicurezza.

Questa nuova strategia di rilevazione, risulta strettamente necessaria per superare i limiti tecnologici intrinseci delle tecnologie Anti-Intrusione commerciali. In particolare, tali tecnologie non permettono:

- l'analisi di flussi applicativi di applicazioni dell'ente di tipo "Make" (le soluzioni di mercato sono progettate per l'esclusivo utilizzo su applicazioni di tipo commerciale);
- l'analisi di flussi applicativi che fanno uso di meccanismi di cifratura delle informazioni;
- la rilevazione di vulnerabilità software determinate da errori in input commessi dall'utente;
- la rilevazione di vulnerabilità software determinate dall'assenza di controlli applicativi durante le operazioni di allocazione di blocchi di memoria nelle aree di memoria volatile.

5.4.3 Scopo e campo di applicazione per eventi di "Alarm Detection"

Il software sviluppato e personalizzato per l'organizzazione è realizzato seguendo le indicazioni e le necessità espresse dall'organizzazione medesima, nel rispetto dei vincoli di sicurezza imposti nel Piano di Sicurezza (in seguito PdS).
Nella fase di produzione e/o aggiornamento del Piano di Sicurezza di una specifica applicazione, insieme all'esame del funzionamento, all'analisi delle informazioni da esso trattate e all'analisi dei flussi applicativi pertinenti (input, output, accesso a DB, autenticazione, ecc.), si procederà all'individuazione delle raccomandazioni degli eventi di Alarm Detection che permetteranno, alle competenti linee di Sviluppo, di identificare e implementare gli opportuni meccanismi di generazione delle informazioni di tracciamento.

5.4.4 Raccomandazioni generali per eventi di "Alarm Detection"

L'attivazione ed il tracciamento per gli eventi di Alarm Detection, di seguito elencati, sono fortemente raccomandati, poichè riguardano alcune delle principali debolezze applicative che, se utilizzate per scopi malevoli, possono comportare un elevato fattore di rischio:

- **Validazione Input**: si devono tracciare tutti gli input (provenienti da Client o da Server) non conformi con quanto atteso dall'applicativo (Cfr. [paragrafo 5.2.7]);
- **Buffer Overflow**: si devono tracciare tutti gli avvisi e/o le eccezioni generate dall'applicativo a fronte di un evento di Buffer Overflow (Cfr. [paragrafo 6.1.7]);
- **Sessioni applicative anomale**: si devono tracciare le occorrenze di eventi che non rientrano nella corretta gestione delle sessioni applicative, come tentativi massivi di autenticazione, sessioni multiple dell'utente non previste e/o consentite, presenza di cookie con contenuti incomprensibili, referrer errato o inconsistente con la funzione o con la pagina chiamata, etc.(Cfr.[paragrafo 6.1.2]);