Confidenzialità dei dati:

La confidenzialità dei dati è la proprietà che garantisce che le informazioni sensibili siano accessibili solo a persone autorizzate. L'obiettivo è proteggere i dati da accessi non autorizzati, sia interni che esterni.

Minacce:

Accesso non autorizzato: gli hacker o gli utenti malevoli possono tentare di accedere a informazioni riservate per scopi illeciti o dannosi.

Furti di dati: possono verificarsi violazioni dei dati in cui i criminali informatici riescono a ottenere accesso a informazioni sensibili, come numeri di carte di credito o informazioni personali.

Vulnerabilità della rete: le reti non sicure o le connessioni Wi-Fi non protette possono facilitare l'intercettazione delle comunicazioni e l'accesso ai dati confidenziali.

Contromisure suggerite:

Crittografia dei dati: l'utilizzo di algoritmi di crittografia può proteggere i dati sensibili durante la trasmissione e lo stoccaggio, rendendoli illeggibili per chi non possiede la chiave di decrittazione.

Gestione degli accessi: implementare un sistema di controllo degli accessi per garantire che solo gli utenti autorizzati possano accedere ai dati sensibili.

Formazione sulla sicurezza: educare gli utenti sull'importanza della sicurezza dei dati, come l'uso di password complesse, il riconoscimento di attacchi di phishing e l'adozione di pratiche sicure nella gestione dei dati.

Integrità dei dati:

L'integrità dei dati riguarda la garanzia che le informazioni siano accurate, coerenti e non alterate in modo non autorizzato durante la trasmissione, lo stoccaggio o l'elaborazione.

Minacce:

Modifica non autorizzata: un attaccante potrebbe tentare di alterare i dati critici per scopi malevoli, come manipolare registrazioni finanziarie o modificare i dettagli di un contratto.

Attacchi di malware: i malware possono essere progettati per modificare i dati presenti su un sistema, compromettendo l'integrità delle informazioni.

Errori umani: gli errori umani, come l'eliminazione accidentale di file o la modifica non intenzionale di dati critici, possono minare l'integrità dei dati.

Contromisure suggerite:

Firma digitale: l'utilizzo di firme digitali o hash crittografici consente di verificare l'integrità dei dati, garantendo che non siano stati alterati durante la trasmissione o lo stoccaggio.

Backup regolari: effettuare regolarmente copie di backup dei dati critici e verificare la loro integrità per ripristinare i dati in caso di incidenti o modifiche non autorizzate.

Controllo degli accessi: limitare l'accesso ai dati solo agli utenti autorizzati e implementare procedure per monitorare e tracciare le modifiche ai dati sensibili.

Disponibilità dei dati:

La disponibilità dei dati riguarda la garanzia che le informazioni siano sempre accessibili e utilizzabili quando necessario, senza interruzioni o degrado delle prestazioni.

Minacce:

Attacchi di tipo DoS (Denial of Service): un attaccante può sovraccaricare un sistema o una rete con traffico dannoso o richieste di servizio legittime al fine di interrompere o limitare l'accesso legittimo ai dati.

Guasti hardware o software: malfunzionamenti o errori hardware/software possono causare interruzioni dei servizi e impedire l'accesso ai dati.

Errori di configurazione: configurazioni errate o non ottimali possono causare problemi di disponibilità, come la limitazione delle risorse di rete o l'esposizione a vulnerabilità.

Contromisure suggerite:

Ridondanza: implementare sistemi ridondanti, come server replicati o connessioni di rete alternative, per garantire la disponibilità dei dati anche in caso di guasti o interruzioni.

Monitoraggio dei sistemi: utilizzare strumenti di monitoraggio per rilevare tempestivamente eventuali anomalie o sovraccarichi di traffico, consentendo di intervenire prontamente per ripristinare la disponibilità.

Pianificazione dei test di ripristino: condurre regolarmente test di ripristino dei dati e dei sistemi per verificare che i processi di backup e ripristino funzionino correttamente e che i tempi di ripristino siano adeguati.