La sigla "CIA" , Confidentiality, Integrity, and Availability (riservatezza, integrità e disponibilità).

Confidentiality:

La confidenzialità dei dati si riferisce alla protezione e al controllo dell'accesso alle informazioni riservate. In sostanza, si tratta di assicurarsi che solo le persone autorizzate possano accedere a determinati dati o informazioni sensibili.

Ecco due potenziali minacce per la confidenzialità dei dati nell'azienda:

a) Accesso non autorizzato: Questa minaccia si verifica quando persone non autorizzate ottengono accesso ai dati sensibili dell'azienda. Potrebbe essere attraverso l'uso di credenziali di accesso rubate, vulnerabilità nella rete o nelle applicazioni, o mancanza di controlli adeguati sulle autorizzazioni degli utenti.

b) Perdita di dati: Questa minaccia si riferisce alla situazione in cui i dati sensibili vengono persi o divulgati in modo non autorizzato. Ciò potrebbe accadere a causa di un malfunzionamento dell'hardware o del software, errori umani, attacchi informatici o furti fisici dei dispositivi contenenti i dati.

Ecco due contromisure per risolvere le minacce alla confidenzialità dei dati:

a) Implementazione di controlli di accesso: Assicurarsi che solo le persone autorizzate abbiano accesso ai dati sensibili. Ciò può essere fatto tramite l'adozione di un sistema di gestione degli accessi basato su ruoli (RBAC) che assegna i diritti di accesso in base ai ruoli degli utenti. Inoltre, è importante implementare una politica di autenticazione forte, come l'utilizzo di password complesse, l'autenticazione a due fattori o l'uso di certificati digitali.

b) Crittografia dei dati: La crittografia è un'importante misura per proteggere la confidenzialità dei dati. Crittografare i dati sensibili durante la trasmissione e lo stoccaggio li rende incomprensibili e inaccessibili a persone non autorizzate. È possibile utilizzare algoritmi di crittografia robusti e implementare una gestione delle chiavi sicura per garantire che solo le persone autorizzate possano decifrare i dati.

Integrity:

L'integrità dei dati si riferisce alla protezione e al mantenimento dell'accuratezza, completezza e coerenza dei dati nel corso del tempo. In altre parole, l'integrità dei dati garantisce che i dati non siano stati alterati o manipolati in modo non autorizzato o accidentale.

Ecco due potenziali minacce per l'integrità dei dati nell'azienda:

a) Modifiche non autorizzate: Questa minaccia si verifica quando i dati vengono alterati, modificati o manomessi da persone non autorizzate. Ciò potrebbe accadere tramite accesso non autorizzato ai sistemi o alle applicazioni, violazione delle politiche di gestione dei dati o sfruttando vulnerabilità nelle misure di sicurezza.

b) Errori umani: Gli errori umani possono rappresentare una minaccia all'integrità dei dati. Questi errori possono essere causati da operazioni sbagliate, caricamento di dati errati o involontaria sovrascrittura o cancellazione di dati importanti.

Ecco due contromisure per risolvere le minacce all'integrità dei dati:

a) Implementazione di controlli di accesso e autorizzazione: Limita l'accesso ai dati solo alle persone autorizzate e assegna i diritti di accesso in modo appropriato. Adotta un sistema di gestione degli accessi che permetta di tracciare e controllare le modifiche ai dati. Inoltre, implementa una politica di controllo delle modifiche che richieda l'autorizzazione e la verifica prima di apportare modifiche importanti ai dati.

b) Backup e ripristino dei dati: Mantieni regolari copie di backup dei dati critici. Questo assicura che, in caso di perdita di dati o di modifiche indesiderate, sia possibile ripristinare una versione precedente dei dati. Assicurati che i backup siano conservati in un luogo sicuro e testa periodicamente il processo di ripristino per verificare che i dati siano recuperabili.

Availability:

La disponibilità dei dati si riferisce alla capacità di accedere ai dati in modo tempestivo e affidabile quando necessario. È importante che i dati siano sempre disponibili per gli utenti autorizzati e che non siano soggetti a interruzioni o indisponibilità prolungate.

Ecco due potenziali minacce per la disponibilità dei dati nell'azienda:

a) Interruzioni del sistema: Questa minaccia si verifica quando si verificano guasti hardware o software, malfunzionamenti del sistema o errori umani che provocano l'interruzione dei servizi e l'indisponibilità dei dati. Ciò potrebbe includere guasti del server, problemi di rete, attacchi informatici che bloccano l'accesso ai servizi, ecc.

b) Attacchi DDoS: Un attacco Distributed Denial of Service (DDoS) mira a sovraccaricare un sistema o una rete con un alto volume di traffico, rendendo i servizi inaccessibili agli utenti legittimi. Questo tipo di attacco può causare gravi interruzioni e una significativa diminuzione della disponibilità dei dati.

Ecco due contromisure per risolvere le minacce alla disponibilità dei dati:

a) Implementazione di sistemi di ridondanza: Introduce un'architettura ridondante che garantisce la disponibilità dei dati anche in caso di guasti o interruzioni. Ciò potrebbe includere la replicazione dei dati su server multipli o l'utilizzo di servizi di cloud computing che offrono una maggiore resilienza e ridondanza.

b) Monitoraggio e rilevamento delle minacce: Utilizza strumenti di monitoraggio per individuare tempestivamente eventuali anomalie o attività sospette che potrebbero indicare un attacco o una violazione in corso. Il monitoraggio proattivo consente di prendere misure preventive per mitigare gli effetti delle minacce e mantenere alta la disponibilità dei dati.