ESERCIZIO 2 M5 D3

SECURITY OPERATION: AZIONI PREVENTIVE

Confidenzialità dei dati:

La confidenzialità dei dati si riferisce alla garanzia che le informazioni siano accessibili solo a coloro che hanno l'autorizzazione e il diritto di accedervi. In altre parole, significa che i dati sono protetti da accessi non autorizzati.

- Potenziali minacce alla confidenzialità dei dati dell'azienda:

1. Accesso non autorizzato: un'eventuale minaccia potrebbe essere l'accesso da parte di individui non autorizzati ai dati sensibili dell'azienda, ad esempio attraverso hackeraggio o furto di credenziali.
2. Fuga di informazioni: un'altra minaccia potrebbe essere la divulgazione non autorizzata di dati sensibili, sia intenzionale che accidentale, come ad esempio attraverso la perdita o il furto di dispositivi contenenti dati aziendali.

- Contromisure per proteggere i dati da queste minacce:

1. Implementare controlli di accesso: impostare un sistema di autenticazione e autorizzazione robusto per garantire che solo le persone autorizzate possano accedere ai dati. Utilizza password complesse, autenticazione a due fattori e limitazioni di accesso basate sui ruoli.
2. Crittografia dei dati: utilizza la crittografia per proteggere i dati sia in transito che a riposo. La crittografia garantisce che i dati siano illeggibili per chiunque non disponga delle chiavi di decrittografia appropriate.

Integrità dei dati:

L'integrità dei dati riguarda l'affidabilità, l'accuratezza e la coerenza dei dati nel corso del tempo. Ciò significa che i dati non devono essere alterati o manipolati in modo non autorizzato o non intenzionale.

- Potenziali minacce all'integrità dei dati dell'azienda:

1. Alterazione dei dati: un possibile rischio potrebbe essere l'alterazione dei dati da parte di attaccanti o di persone non autorizzate, con l'obiettivo di modificare o corrompere le informazioni.
2. Errori umani: un'altra minaccia potrebbe derivare da errori umani, come ad esempio l'inserimento accidentale di dati errati o la modifica non intenzionale di informazioni critiche.

- Contromisure per proteggere i dati da queste minacce:

1. Utilizzo di firme digitali: l'utilizzo di firme digitali o hash crittografici può garantire l'integrità dei dati. Questi metodi consentono di verificare se i dati sono stati modificati in modo non autorizzato.
2. Implementazione di controlli di validazione dei dati: verificare l'accuratezza dei dati attraverso controlli di validazione, come ad esempio la verifica della coerenza delle informazioni o l'implementazione di meccanismi di rilevazione degli errori.

Disponibilità dei dati:

La disponibilità dei dati si riferisce alla garanzia che i dati siano accessibili e utilizzabili quando necessario, senza interruzioni o ritardi e senza che siano resi inaccessibili da eventi imprevisti o intenzionali.

- Potenziali minacce alla disponibilità dei dati dell'azienda:

1. Attacchi di tipo DoS (Denial of Service): Gli attacchi DoS mirano a sovraccaricare il sistema o la rete, rendendo i dati inaccessibili agli utenti legittimi.
2. Guasti hardware o errori di sistema: Problemi tecnici, come guasti hardware o errori di sistema, possono causare la perdita temporanea o permanente dell'accesso ai dati.

- Contromisure per proteggere i dati da queste minacce:

1. Implementazione di sistemi di rilevamento e prevenzione degli attacchi DoS: utilizza soluzioni come firewall e sistemi di rilevamento degli intrusi per identificare e mitigare gli attacchi DoS in modo tempestivo.
2. Implementazione di politiche di backup e ripristino: eseguire regolari backup dei dati critici e implementare procedure di ripristino per garantire che in caso di guasti hardware o errori di sistema i dati possano essere rapidamente ripristinati e resi nuovamente disponibili.