M5 D3

ESERCIZIO 2

SECURITY OPERATION: CIA

1) **Confidenzialità dei dati**

La confidenzialità dei dati si riferisce alla protezione delle informazioni sensibili da accessi non autorizzati. Due potenziali minacce alla confidenzialità dei dati aziendali potrebbero essere:

a) Accesso non autorizzato: Un attaccante potrebbe tentare di ottenere accesso non autorizzato ai dati aziendali attraverso tecniche come il furto di credenziali, l'ingegneria sociale o l'utilizzo di malware.

Per proteggere i dati da questa minaccia, puoi adottare le seguenti contromisure:

- Implementare un sistema di autenticazione forte, come l'autenticazione a due fattori o l'utilizzo di certificati digitali.
- Applicare e concedere l'accesso ai dati solo al personale autorizzato.

b) Perdita di dati: I dati aziendali potrebbero essere esposti a rischi di perdita a causa di incidenti come guasti hardware, errori umani o attacchi ransomware.

Per proteggere i dati da questa minaccia, puoi prendere le seguenti precauzioni:

- Effettuare regolari backup dei dati e archiviare le copie di backup in un luogo sicuro.
- Crittografare i dati sensibili sia durante il trasferimento che durante l'archiviazione per impedirne la lettura non autorizzata.

2) **Integrità dei dati:**

L'integrità dei dati riguarda la garanzia che i dati non siano stati alterati in modo non autorizzato o involontario. Due potenziali minacce all'integrità dei dati aziendali potrebbero essere:

a) Alterazione dei dati: Un attaccante potrebbe tentare di modificare o alterare i dati aziendali durante la trasmissione o l'archiviazione.

Per proteggere i dati da questa minaccia, puoi considerare le seguenti contromisure:

-Utilizzare firme digitali o hash crittografici per verificare l'integrità dei dati durante il trasferimento.
- Implementare controlli di accesso basati su ruoli e limitare i privilegi di modifica dei dati solo al personale autorizzato.

b) Errori umani: Gli errori umani, come la manipolazione involontaria dei dati o l'inserimento di informazioni errate, possono compromettere l'integrità dei dati aziendali.

Per mitigare questa minaccia, puoi adottare le seguenti precauzioni:

- Implementare procedure di controllo della qualità dei dati per identificare e correggere gli errori prima che possano causare danni significativi.
- Fornire adeguata formazione e consapevolezza al personale sull'importanza della corretta manipolazione dei dati.

3) Disponibilità dei dati:

La disponibilità dei dati si riferisce alla garanzia che i dati siano accessibili e utilizzabili quando necessario. Due potenziali minacce alla disponibilità dei dati aziendali potrebbero essere:

a) Attacchi di tipo DoS (Denial of Service): Un attaccante potrebbe tentare di sovraccaricare i sistemi aziendali o interrompere l'accesso ai servizi critici, rendendo i dati inaccessibili.

Per proteggere i dati da questa minaccia, puoi considerare le seguenti contromisure:

- Implementare soluzioni di protezione contro gli attacchi DoS, come i firewall o i servizi di mitigazione degli attacchi DDoS (Distributed Denial of Service).
- Distribuire i servizi critici su infrastrutture ridondanti per garantire la continuità operativa in caso di attacchi.

b) Incidenti fisici o catastrofi naturali: Eventi come incendi, alluvioni o guasti elettrici possono causare interruzioni nella disponibilità dei dati.

Per proteggere i dati da questa minaccia, puoi adottare le seguenti precauzioni:

- Effettuare regolari backup dei dati e archiviarli in un luogo esterno sicuro o utilizzare servizi di archiviazione cloud affidabili.
- Implementare un piano di continuità aziendale che includa procedure per il ripristino dei dati in caso di incidenti o catastrofi.