Esercitazione WEEK 18 D1 (2)

Security Operation: CIA

Ettore Farris

Descrizione sintetica

Obiettivo dell'esercizio: Verificare la comprensione dei concetti di confidenzialità, integrità e disponibilità dei dati.

Scenario: Sei un consulente di sicurezza informatica e un'azienda ti ha assunto per valutare la sicurezza dei suoi sistemi informatici. Durante la tua analisi, ti accorgi che l'azienda ha problemi con la triade CIA. Il tuo compito è identificare e risolvere tali problemi. Fornisci un breve rapporto in cui indichi le aree di miglioramento e le misure suggerite per aumentare la sicurezza dei dati.

Esercizio:

Confidenzialità:

- Spiega cosa si intende per confidenzialità dei dati.
- Identifica due potenziali minacce alla confidenzialità dei dati dell'azienda.
- Suggerisci due contromisure per proteggere i dati da queste minacce.

Integrità:

- Spiega cosa si intende per integrità dei dati.
- Identifica due potenziali minacce alla integrità dei dati dell'azienda.
- Suggerisci due contromisure per proteggere i dati da queste minacce.

Disponibilità:

- Spiega cosa si intende per disponibilità dei dati.
- Identifica due potenziali minacce alla disponibilità dei dati dell'azienda.
- Suggerisci due contromisure per proteggere i dati da questa minaccia.

Svolgimento

1) ***Confidenzialità*:**

- ***Spiega cosa si intende per confidenzialità dei dati***

Questo principio sancisce che l'accesso ai dati deve essere garantito solamente agli utenti autorizzati. Nessun utente non autorizzato deve poter accedere ai dati. Immaginiamo, ad esempio, che informazioni militari *top-secret* finiscano nelle mani sbagliate.

- ***Identifica due potenziali minacce alla confidenzialità dei dati dell'azienda***

Potenziali minacce possono essere:

- *Accesso non autorizzato*: potrebbero essere causati da attacchi hacker, malware presenti nel sistema o, ad esempio, da dipendenti ed ex-dipendenti scontenti;
- *Fuga di informazioni*: alcune informazioni potrebbero trapelare all'esterno volontariamente (es. dipendenti o ex-dipendenti scontenti) oppure involontariamente (es. attacchi di ingegneria sociale).

- ***Suggerisci due contromisure per proteggere i dati da queste minacce***

Possibili contromisure:

- *Autenticazione a più fattori*: per garantire più livelli di sicurezza si può implementare un sistema di autenticazione più complesso;
- *Crittografia*: con la crittografia si garantisce che i dati non possano venire decifrati da chi ne entra in possesso in modo non autorizzato.

2) ***Integrità:***

- ***Spiega cosa si intende per integrità dei dati***

L'integrità dei dati si riferisce all'affidabilità e alla correttezza del dato. I dati non devono essere né modificati né alterati. Ad esempio, immaginano gli effetti prodotti da una modifica di dati sanitari o di una transazione bancaria.

- ***Identifica due potenziali minacce alla integrità dei dati dell'azienda***

Potenziali minacce possono essere:

- *Malware*: ransomware o virus potrebbero modificare o alterare il contenuto dei dati in modo illecito minandone quindi l'integrità;
- *Fattore umano*: le persone possono alterare i dati di proposito o accidentalmente.

- ***Suggerisci due contromisure per proteggere i dati da queste minacce***

Possibili contromisure:

- *Crittografia con hash*: l'uso degli hash consente di rilevare anche le modifiche più sottili di un dato;
- *Backup dei dati*: effettuare backup regolare per ripristinare i dati in caso di incidente.

3) *Disponibilità*

- ***Spiega cosa si intende per disponibilità dei dati***

La disponibilità stabilisce che l'accessibilità ai dati deve essere garantita in ogni momento e per i soli utenti autorizzati. Es. accesso al proprio conto in banca o al backend del proprio sito internet hostato su un server.

- ***Identifica due potenziali minacce alla disponibilità dei dati dell'azienda***

Potenziali minacce possono essere:

- *Attacchi DDOS*: questo tipo di attacchi è in grado di mettere fuori uso temporaneamente i sistemi inondandoli con traffico falso e rendendoli inaccessibili agli utenti;
- *Disastri naturali/tecnici*: eventi naturali come terremoti e inondazioni, oppure tecnici come incendi e blackout possono impedire l'accesso ai dati da parte degli utenti.

- ***Suggerisci due contromisure per proteggere i dati da questa minaccia***

Possibili contromisure:

- *Sistemi con elevata fault-tolerance*: un esempio potrebbe essere l'implementazione di sistemi ridondanti potrebbe garantire l'accesso ai dati anche in caso di guasto, incendio o blackout;
- *Definizione di un Business Continuity Plan*: definire un BCP è fondamentale per definire le policy e le procedure da mettere in atto per minimizzare gli impatti negativi sull'operatività di una compagnia in caso di disastro.