

Esercitazione W18D1 - Pratica 2

Security Operation - CIA

Fabio Benevento - 06/03/2024

Traccia

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.

- **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 potenziale minaccia alla disponibilità dei dati dell'azienda.
Suggerisci due contromisura per proteggere i dati da questa minaccia.

Implementazione

Confidenzialità:

La confidenzialità dei dati si riferisce alla protezione delle informazioni riservate e sensibili da accessi non autorizzati. Due potenziali minacce alla confidenzialità dei dati dell'azienda potrebbero essere:

- 
- Accesso non autorizzato da parte di dipendenti interni: Per mitigare questa minaccia, è consigliabile implementare rigorosi controlli di accesso, assegnando privilegi solo a coloro che necessitano di determinate informazioni.
 - Violazione della rete da parte di attaccanti esterni: L'utilizzo di una robusta crittografia per la trasmissione dei dati e l'implementazione di firewall avanzati possono contribuire a proteggere i dati durante il transito attraverso la rete.

Integrità:

L'integrità dei dati riguarda la protezione delle informazioni da modifiche non autorizzate o danni. Due potenziali minacce all'integrità dei dati dell'azienda includono:

- Attacchi di malware o virus: L'implementazione di soluzioni antivirus e l'istruzione dei dipendenti sull'importanza di evitare download non autorizzati possono ridurre il rischio di infezioni.
- Manipolazione dei dati da parte di dipendenti malevoli: L'adozione di controlli di accesso avanzati e la registrazione delle attività possono aiutare a individuare e prevenire manipolazioni indebite dei dati.

Disponibilità:

La disponibilità dei dati si riferisce alla garanzia che le informazioni siano accessibili quando necessario. Due potenziali minacce alla disponibilità dei dati dell'azienda potrebbero essere:

- Attacchi di tipo Denial of Service (DoS): L'implementazione di soluzioni di mitigazione DoS, come sistemi di rilevamento e filtraggio del traffico anomalo, può aiutare a mantenere la disponibilità dei servizi.
- Errori umani che portano a perdite di dati: La regolare esecuzione di backup e la formazione del personale sull'importanza delle pratiche sicure possono contribuire a prevenire la perdita di dati critici.