Report Esercizio

W18-D3

Redatto da Andrea Sciattella

23/06/2024

TRACCIA

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.

1. ***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.

2. ***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.

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

SVOLGIMENTO ESERCIZIO

L'azienda "X" ci ha richiesto un'analisi della sicurezza dei propri sistemi informatici, dando particolare importanza alla triade della sicurezza informatica: **Confidenzialità, Integrità e Disponibilità (CIA).** Durante la nostra valutazione, sono emerse diverse aree di miglioramento che, se affrontate, possono aumentare significativamente la sicurezza complessiva dei dati aziendali.

Confidenzialità

La confidenzialità dei dati si riferisce alla protezione delle informazioni da accessi non autorizzati, garantendo che solo le persone autorizzate possano accedere e visualizzare le informazioni sensibili.

Potenziali Minacce:

1. **Accesso non autorizzato**: Dipendenti o attori esterni possono ottenere accesso ai dati sensibili senza autorizzazione.
2. **Furto di credenziali**: Le credenziali di accesso possono essere rubate attraverso phishing o malware, permettendo agli attaccanti di accedere ai dati confidenziali.

Contromisure Suggerite:

1. **Crittografia dei Dati**: Implementare la crittografia dei dati sia a riposo che in transito per proteggere le informazioni sensibili. Questo garantisce che, anche se i dati vengono intercettati, non siano leggibili senza le chiavi di decrittazione appropriate.
2. **Controlli di Accesso Basati su Ruoli (RBAC):** Implementare un sistema di controllo degli accessi basato su ruoli, in cui l'accesso ai dati è limitato solo a coloro che ne hanno effettiva necessità per svolgere il proprio lavoro. Questo riduce il rischio di accesso non autorizzato.

Integrità

L'integrità dei dati si riferisce alla protezione delle informazioni da modifiche non autorizzate o accidentali, garantendo che i dati rimangano accurati e affidabili nel tempo.

Potenziali Minacce:

1. **Manomissione dei dati**: Attori interni o esterni possono alterare i dati in modo non autorizzato, compromettendo l'affidabilità delle informazioni.
2. **Errori umani**: Modifiche accidentali ai dati possono avvenire a causa di errori umani, influenzando l'integrità delle informazioni.

Contromisure Suggerite:

1. **Controlli di Versione e Audit**: Implementare sistemi di controllo delle versioni e log di audit per monitorare e registrare tutte le modifiche ai dati. Questo permette di tracciare e ripristinare eventuali modifiche non autorizzate o accidentali.
2. **Validazione e Verifica dei Dati**: Implementare procedure di validazione e verifica dei dati per garantire che tutte le modifiche siano corrette e autorizzate. Questo può includere l'uso di checksum, hash e firme digitali.

Disponibilità

La disponibilità dei dati si riferisce alla garanzia che le informazioni siano accessibili e utilizzabili quando necessario, senza interruzioni o ritardi indebiti.

Potenziali Minacce:

1. **Attacchi DDoS (Distributed Denial of Service):** Attacchi che mirano a sovraccaricare i sistemi, rendendo i dati inaccessibili agli utenti legittimi.
2. **Guasti Hardware**: Malfunzionamenti o guasti dei componenti hardware possono rendere i dati inaccessibili.

Contromisure Suggerite:

1. **Implementazione di Sistemi di Backup e Ripristino**: Avere un sistema di backup regolare e un piano di ripristino ben definito garantisce che i dati possano essere recuperati rapidamente in caso di guasto hardware o perdita di dati.
2. **Protezione DDoS**: Utilizzare soluzioni di protezione DDoS per monitorare e mitigare gli attacchi, assicurando che i sistemi rimangano operativi e i dati accessibili anche durante un attacco.

CONCLUSIONI

Affrontare le problematiche emerse nella triade CIA permetterà all'azienda “X” di migliorare significativamente la sicurezza dei propri sistemi informatici.

L'implementazione delle contromisure suggerite ridurrà il rischio di accesso non autorizzato, garantirà l'affidabilità dei dati e assicurerà la loro disponibilità continua.

Inoltre, è raccomandato di effettuare periodiche valutazioni della sicurezza per adattarsi alle nuove minacce e mantenere un alto livello di protezione.