CS Operation Report

Aree di miglioramento e misure suggerite per aumentare la sicurezza dei dati

Per valutare lo stato della sicurezza delle informazioni di un dato ambiente uno dei principi più importanti è il «CIA principle» (detto anche CIA triade), dove:

- **C**, sta per **Confidentiality**, ovvero la riservatezza del dato
- **I**, sta per **Integrity**, ovvero l'integrità del dato
- **A**, sta per **Availability**, ovvero la disponibilità del dato

Confidentiality - Confidenzialità dei dati:

La confidenzialità dei dati si riferisce riservatezza delle informazioni, ovvero alla protezione delle stesse da accessi non autorizzati o divulgazione. Ciò significa impedire o minimizzare gli accessi non autorizzati, con lo scopo di garantire che solo coloro che hanno il permesso di vedere un dato specifico possano accedervi.

Potenziali minacce:

1. Phishing: Questi sono attacchi in cui gli hacker cercano di ingannare gli utenti per ottenere le credenziali di accesso.
2. Intrusioni nelle reti aziendali: Se la rete aziendale viene compromessa, dati sensibili possono essere esposti a malintenzionati.

Contromisure:

1. Educazione e formazione dei dipendenti: Fornire una formazione regolare sui rischi di sicurezza e sulle migliori pratiche.
2. Implementazione di firewall e sistemi di rilevamento delle intrusioni per monitorare e proteggere la rete aziendale.

Altri controlli sulla sicurezza che contribuiscono a garantire la sicurezza del dato sono la cifratura dei dati e l'implementazione di misure per il controllo degli accessi.

Integrity - Integrità dei dati:

L'integrità dei dati si concentra sull'affidabilità e sulla correttezza dei dati nel corso del tempo. Proteggere l'integrità significa garantire che le informazioni non vengano modificate in modo inappropriato, sia accidentalmente che deliberatamente.

Potenziali minacce:

1. Malware: Software maligni che possono alterare, cancellare o corrompere i dati.
2. Errori umani: Modifiche accidentali o cancellazione di dati.

Contromisure:

L'integrità del dato dipende dalla riservatezza del dato. Le misure di sicurezza che impattano positivamente sulla riservatezza del dato, impattano quindi positivamente anche sulla sua integrità.

Altre misure possibili sono:

1. Backup regolari: Garantire che ci sia sempre una copia pulita e sicura dei dati che può essere ripristinata se necessario.
2. Controllo degli accessi: Limitare l'accesso ai dati solo a chi ne ha veramente bisogno e monitorare le modifiche.

Se i dati sono cifrati, è inoltre, possibile implementare meccanismi di verifica degli hash, o checksum, atti a controllare se i dati sono stati alterati dal momento della trasmissione al momento della loro ricezione e lettura.

Availability - Disponibilità dei dati:

La disponibilità dei dati si riferisce alla garanzia che le informazioni siano sempre accessibili agli utenti autorizzati. La disponibilità deve essere sempre garantita, anche in caso di errori applicativi o crash del sistema.

Potenziali minacce:

1. Attacchi DDoS (Distributed Denial of Service): Questi attacchi inondano un sistema con traffico, rendendo impossibile l'accesso ai dati.
2. Guasti hardware: Come un crash del server o un guasto al disco rigido.

Contromisure:

1. Implementazione di meccanismi anti-DdoS per identificare e mitigare rapidamente il traffico dannoso.
2. Ridondanza hardware: avere hardware di backup in posizione, come server di riserva o array di dischi rigidi, per garantire la continuità dell'accesso ai dati.