Rapporto di Valutazione della Sicurezza Informatica

Confidenzialità

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

Potenziali minacce alla confidenzialità dei dati:

1. **Accessi non autorizzati:** Gli hacker o i dipendenti interni malintenzionati potrebbero ottenere accesso non autorizzato ai dati sensibili.
2. **Intercettazione delle comunicazioni:** Durante la trasmissione dei dati, questi potrebbero essere intercettati da attaccanti tramite tecniche come l'intercettazione delle comunicazioni di rete.

Contromisure suggerite:

1. **Implementazione della crittografia:** Utilizzare protocolli di crittografia robusti per proteggere i dati sia a riposo che in transito. Tecnologie come SSL/TLS per le comunicazioni web e la crittografia AES per i dati memorizzati possono prevenire l'intercettazione e l'accesso non autorizzato.
2. **Controllo degli accessi:** Implementare un rigoroso sistema di controllo degli accessi basato su ruoli (RBAC), insieme all'autenticazione a due fattori (2FA) per garantire che solo gli utenti autorizzati possano accedere ai dati sensibili.

Integrità

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

Potenziali minacce all'integrità dei dati:

1. **Modifiche non autorizzate:** Gli attacchi di malware o i dipendenti malintenzionati potrebbero alterare o corrompere i dati.
2. **Errori umani:** Errori durante l'inserimento o la modifica dei dati possono compromettere l'integrità delle informazioni.

Contromisure suggerite:

1. **Utilizzo di checksum e hash:** Implementare meccanismi di verifica come checksum o hash (es. SHA-256) per garantire che i dati non siano stati alterati. Qualsiasi modifica ai dati può essere rilevata confrontando il valore hash memorizzato con quello calcolato.
2. **Controlli di versione e audit:** Utilizzare sistemi di controllo di versione e tenere traccia delle modifiche attraverso log di audit. In caso di errore o modifica non autorizzata, è possibile ripristinare la versione precedente dei dati.

Disponibilità

Definizione:
La disponibilità dei dati si riferisce alla garanzia che le informazioni siano accessibili e utilizzabili su richiesta, garantendo un accesso tempestivo ai dati necessari per le operazioni aziendali.

Potenziali minacce alla disponibilità dei dati:

1. **Attacchi DDoS:** Attacchi di tipo Distributed Denial of Service possono sovraccaricare i server aziendali, rendendo i servizi inaccessibili.
2. **Guasti hardware:** Guasti ai componenti hardware critici possono interrompere l'accesso ai dati.

Contromisure suggerite:

1. **Implementazione di soluzioni di alta disponibilità:** Utilizzare soluzioni di failover e bilanciamento del carico per garantire la continuità operativa. La ridondanza dei server e l'uso di sistemi di backup off-site possono minimizzare l'impatto di un guasto hardware.
2. **Protezione contro attacchi DDoS:** Implementare soluzioni di mitigazione DDoS, come i servizi di protezione cloud-based, che possono rilevare e bloccare il traffico malevolo prima che raggiunga l'infrastruttura aziendale.

Conclusioni

Per migliorare la sicurezza dei sistemi informatici dell'azienda, è fondamentale adottare un approccio olistico che consideri tutte le dimensioni della triade CIA. Le contromisure suggerite sopra rappresentano passi cruciali per proteggere la confidenzialità, l'integrità e la disponibilità dei dati, garantendo un ambiente IT sicuro e affidabile. Raccomando inoltre di eseguire regolarmente audit di sicurezza e aggiornare continuamente le misure di protezione per affrontare le nuove minacce emergenti.