Rapporto di Valutazione della Sicurezza dei Sistemi Informatici

1. Confidenzialità dei Dati

Definizione: La confidenzialità dei dati si riferisce alla protezione delle informazioni da accessi non autorizzati. Questo garantisce che solo le persone autorizzate possano accedere e visualizzare i dati sensibili, impedendo così la divulgazione a individui o entità non autorizzate.

Potenziali Minacce alla Confidenzialità:

1. **Accessi non autorizzati:** Hacker o dipendenti malintenzionati possono ottenere l'accesso ai dati sensibili senza autorizzazione.
2. **Furto di dispositivi:** Laptop, smartphone o dispositivi di archiviazione fisica contenenti dati sensibili possono essere rubati, consentendo l'accesso ai dati da parte di persone non autorizzate.

Contromisure:

1. **Implementazione di meccanismi di autenticazione robusti:** Utilizzare autenticazione a due fattori (2FA) e sistemi di gestione degli accessi per assicurarsi che solo gli utenti autorizzati possano accedere ai dati sensibili.
2. **Crittografia dei dati:** Crittografare i dati sia in transito che a riposo, per garantire che anche in caso di accesso non autorizzato o furto di dispositivi, i dati rimangano illeggibili senza le chiavi di decrittazione appropriate.

2. Integrità dei Dati

Definizione: L'integrità dei dati si riferisce alla garanzia che le informazioni siano accurate e complete e che non siano state alterate in modo non autorizzato. Questo assicura che i dati rimangano affidabili e corretti durante tutto il loro ciclo di vita.

Potenziali Minacce all'Integrità:

1. **Manomissione dei dati:** Modifiche non autorizzate ai dati da parte di hacker o dipendenti malintenzionati.
2. **Errori umani:** Errori accidentali durante l'inserimento, l'aggiornamento o la cancellazione dei dati possono comprometterne l'integrità.

Contromisure:

1. **Implementazione di controlli di accesso e logging:** Assicurarsi che solo le persone autorizzate possano modificare i dati e mantenere un registro dettagliato di tutte le modifiche ai dati per poter tracciare e correggere eventuali modifiche non autorizzate.
2. **Utilizzo di checksum e hash:** Implementare algoritmi di checksum e hash per verificare l'integrità dei dati. In questo modo, ogni modifica ai dati può essere rilevata immediatamente, garantendo che i dati non siano stati alterati in modo non autorizzato.

3. Disponibilità dei Dati

Definizione: La disponibilità dei dati si riferisce alla capacità di accedere ai dati quando necessario. Questo garantisce che le informazioni siano sempre accessibili agli utenti autorizzati senza interruzioni.

Potenziali Minacce alla Disponibilità:

1. **Attacchi DDoS (Distributed Denial of Service):** Gli attacchi DDoS possono sovraccaricare i server e renderli inaccessibili agli utenti legittimi.
2. **Guasti hardware:** Problemi con l'hardware come guasti ai server, dischi rigidi o altre infrastrutture possono rendere i dati inaccessibili.

Contromisure:

1. **Implementazione di soluzioni di mitigazione DDoS:** Utilizzare servizi di mitigazione DDoS per proteggere i server dagli attacchi e mantenere la disponibilità dei dati anche durante un attacco.
2. **Piani di disaster recovery e backup:** Avere un piano di disaster recovery ben definito e implementare regolari backup dei dati. In caso di guasto hardware o altre emergenze, i dati possono essere rapidamente ripristinati da backup recenti, minimizzando i tempi di inattività.

Conclusione

Attraverso l'implementazione delle misure sopra descritte, l'azienda può migliorare significativamente la sicurezza dei propri sistemi informatici, garantendo confidenzialità, integrità e disponibilità dei dati. Questo non solo proteggerà i dati sensibili da accessi non autorizzati e manomissioni, ma assicurerà anche che le informazioni siano sempre disponibili quando necessario, contribuendo così alla continuità operativa e alla fiducia degli utenti.