Confidenzialità

Definizione:

La confidenzialità dei dati si riferisce alla protezione delle informazioni dall'accesso non autorizzato, garantendo che solo le persone autorizzate possano accedere e visualizzare i dati sensibili. È uno dei principi fondamentali della sicurezza informatica, volto a prevenire la divulgazione di informazioni riservate a individui non autorizzati.

Potenziali minacce alla confidenzialità dei dati dell'azienda:

1. **Accessi non autorizzati:** Hacker o insider malintenzionati che accedono ai dati sensibili senza permesso.
2. **Intercettazioni:** L'uso di strumenti di sniffing per intercettare i dati durante la loro trasmissione attraverso reti non sicure.

Contromisure per proteggere i dati da queste minacce:

3. **Crittografia:** Utilizzare la crittografia per proteggere i dati sia a riposo che in transito. In questo modo, anche se i dati vengono intercettati, non saranno leggibili senza la chiave di decrittazione.
4. **Autenticazione a più fattori (MFA):** Implementare MFA per garantire che solo gli utenti autorizzati possano accedere ai dati sensibili, aggiungendo un ulteriore livello di sicurezza oltre la semplice password.

Integrità

Definizione:

L'integrità dei dati riguarda la precisione e la completezza delle informazioni, assicurando che i dati non vengano alterati o distrutti in modo non autorizzato. È fondamentale che i dati siano affidabili e rappresentino correttamente l'informazione originaria.

Potenziali minacce all'integrità dei dati dell'azienda:

5. **Manomissione dei dati:** Attacchi in cui gli hacker alterano o manipolano i dati per scopi fraudolenti.
6. **Malware:** Software malevolo come virus o trojan che possono corrompere o modificare i dati aziendali.

Contromisure per proteggere i dati da queste minacce:

7. **Controllo delle versioni e backup:** Implementare sistemi di controllo delle versioni e backup regolari dei dati, in modo che sia possibile ripristinare i dati originali in caso di manipolazione o corruzione.
8. **Hashing e firme digitali:** Utilizzare algoritmi di hashing e firme digitali per verificare l'integrità dei dati, garantendo che i dati non siano stati alterati tra il momento in cui sono stati creati e il momento in cui vengono utilizzati.

Disponibilità

Definizione:

La disponibilità dei dati si riferisce alla capacità di accedere e utilizzare i dati quando necessario. Assicura che le informazioni siano sempre accessibili agli utenti autorizzati, specialmente in contesti aziendali critici.

Potenziali minacce alla disponibilità dei dati dell'azienda:

9. **Attacchi DDoS (Distributed Denial of Service):** Attacchi che mirano a sovraccaricare i sistemi aziendali, rendendo i servizi inaccessibili.
10. **Guasti hardware o software:** Malfunzionamenti di componenti hardware o software critici che possono rendere i dati inaccessibili.

Contromisure per proteggere i dati da queste minacce:

11. **Ridondanza e failover:** Implementare sistemi di ridondanza e meccanismi di failover per garantire che, in caso di guasto di un componente, un altro possa prendere il suo posto senza interruzioni del servizio.
12. **Firewall e sistemi di prevenzione degli attacchi DDoS:** Utilizzare firewall avanzati e servizi di mitigazione degli attacchi DDoS per proteggere l'infrastruttura aziendale da attacchi che potrebbero compromettere la disponibilità dei dati.

Implementando queste misure, un'azienda può migliorare significativamente la sicurezza dei suoi dati, garantendo confidenzialità, integrità e disponibilità.