ESERCIZIO W18D1 PRATICA 2

Rapporto sulla Sicurezza dei Dati per l'Azienda X

Confidenzialità dei Dati:

La confidenzialità dei dati si riferisce alla protezione dei dati da accessi non autorizzati. Questo significa garantire che solo le persone autorizzate possano accedere alle informazioni sensibili dell'azienda.

Potenziali minacce:
Accesso non autorizzato: Minaccia da parte di dipendenti non autorizzati o hacker esterni che possono ottenere accesso ai dati sensibili.
Perdita fisica dei dispositivi di archiviazione: Perdita o furto di dispositivi come laptop o dischi rigidi esterni contenenti dati aziendali sensibili.

Violazione del GDPR: Il GDPR (General Data Protection Regulation) è un regolamento dell'Unione Europea che riguarda la protezione dei dati personali e la privacy dei cittadini dell'UE.

Rischio di non conformità alle normative GDPR che potrebbero compromettere la privacy dei dati.

Contromisure:
Autenticazione a più fattori (MFA): Implementare l'autenticazione a più fattori per ridurre il rischio di accessi non autorizzati.

Crittografia dei dati sensibili: Crittografare i dati sensibili sia in transito che a riposo per proteggerli in caso di accesso non autorizzato ai dispositivi.

Policy di accesso: Implementare politiche rigorose di gestione degli accessi per garantire che solo coloro che hanno l'autorizzazione possano accedere ai dati.

Crittografia: Utilizzare la crittografia per proteggere i dati sensibili sia in transito che a riposo, garantendo che i dati siano illeggibili per chi non è autorizzato.

Integrità dei Dati:

L'integrità dei dati si riferisce alla protezione dei dati da modifiche non autorizzate o dannose. I dati devono rimanere accurati, completi e validi.

Potenziali minacce:
Man-in-the-Middle (MITM): Il MITM è una minaccia in cui un attaccante intercetta la comunicazione tra due parti e altera o manipola i dati scambiati tra di esse senza che le parti coinvolte ne siano consapevoli.
Modifiche non autorizzate: Modifiche o manipolazioni dei dati da parte di individui non autorizzati, causando danni o manipolazioni malevole.
Corruzione dei dati: Errori accidentali o intenzionali che compromettono l'integrità dei dati.

Contromisure:

Controlli di accesso basati sui ruoli: Limitare l'accesso ai dati in base ai ruoli e applicare controlli rigorosi per modificare i dati sensibili.

Utilizzo di firme digitali e hash crittografici: Applicare firme digitali o hash crittografici per verificare l'integrità dei dati e rilevare modifiche non autorizzate.

Disponibilità dei Dati:

La disponibilità dei dati si riferisce alla garanzia che i dati siano accessibili e utilizzabili quando necessario da parte degli utenti autorizzati.

Potenziali minacce:
Attacchi di denial of service (DoS): Tentativi di interrompere o ridurre l'accesso ai servizi aziendali, rendendo i dati inaccessibili.
Guasti hardware o software: Malfunzionamenti dei sistemi o errori hardware che possono causare interruzioni e perdita di disponibilità dei dati.

Contromisure:

Piani di ripristino di emergenza e di continuità aziendale: Implementare piani e procedure per il ripristino rapido dei servizi in caso di interruzioni.

Utilizzo di sistemi di backup regolari: Effettuare backup regolari dei dati critici e archiviarli in modo sicuro per garantire la disponibilità continua.

Generatori di corrente e UPS: Installare generatori di corrente e sistemi di alimentazione ininterrotta per prevenire interruzioni di servizio dovute a blackout.

In conclusione, per migliorare la sicurezza dei dati dell'azienda X, è fondamentale implementare un approccio che protegga la confidenzialità, l'integrità e la disponibilità dei dati.

Le contromisure suggerite aiuteranno a mitigare le potenziali minacce identificate e a rafforzare complessivamente la sicurezza dei sistemi informatici dell'azienda.