Security Operation : CIA

Il primo principio della CIA è la confidentiality o riservatezza. Si riferisce al concetto di protezione delle informazioni in modo che siano accessibili solo alle persone o alle entità autorizzate, e, che non cadano nelle mani di individui non autorizzati.

Due potenziali minacce alla confidenzialità dei dati di un'azienda possono essere :

Accesso non autorizzato: Questa minaccia si verifica quando persone non autorizzate, come hacker, utenti malintenzionati o utenti non autorizzati, ottengono accesso a dati sensibili dell'azienda. Ciò può accedere a causa di debolezze nella sicurezza, password deboli o compromesse, o errori umani.

Perdita o furto fisico : Questa minaccia riguarda la perdita fisica o il furto di dispositivi di archiviazione dati o documenti contenenti informazioni sensibili.

Ad esempio se un laptop aziendale contenente informazioni confidenziali viene smarrito, può compromettere la confidenzialità dell'azienda.

Per proteggere la confidenzialità dei dati, le aziende implementano misure di sicurezza come l'accesso basato su ruoli, l'autenticazione forte, l'encrypting dei dati, le politiche di sicurezza dell'informazione e la formazione dei dipendenti sulla sicurezza informatica.

Questa fase è molto importante per la gestione della sicurezza delle informazioni in un'organizzazione.

L’integrità dei dati è uno dei principi fondamentali della sicurezza delle informazioni, ed è strettamente legata alla protezione e all’assicurazione che i dati rimangano accurati, completi e invariati durante tutto il loro ciclo di vita.

In questo caso, quando si parla di integrità, si intende che i dati non siano alterati o danneggiati in modo non autorizzato o accidentale.

Due minacce possono essere :

Alterazione non autorizzata dei dati : Si verifica quando un individuo o un processo modificano i dati senza autorizzazione. Questo processo può essere fatto da hacker che ha compromesso un sistema, o da un utente malintenzionato.

Corruzione dei dati: Questa minaccia riguarda il danneggiamento accidentale o deliberato dei dati in modo che diventino illeggibili.

Questo può accadere a causa di un guasto all’hardware, errori di trasmissione dei dati, o attacchi informatici che cercano di danneggiare i dati.

Per proteggere i dati si possono prende diverse contromisure:

Controlli di accesso: Limita l’accesso ai dati solo alle persone o sistemi autorizzati.

Backup regolari : Esegui backup regolari dei dati in modo da poter ripristinare le versioni integre in caso di modifiche.

Monitoraggio delle attività : Monitora l’attività del sistema per individuare comportamenti sospetti o tentativi di alterare i dati.

Formazione degli utenti : Fornisci formazione ai dipendenti sull’importanza dell’integrità dei dati e sulla prevenzione delle minacce alla sicurezza.

La disponibilità dei dati è uno dei tre pilastri fondamentali della sicurezza delle informazioni. Si riferisce al principio secondo il quale i dati devono essere accessibili e utilizzabili quando necessario e desiderato.

due potenziali minacce alla disponibilità dei dati di un'azienda sono:

Attacchi di negazione del servizio(DOS) : Questa minaccia si verifica quando un attaccante tenta di saturare o sovraccaricare un sistema o una rete in modo che diventino inaccessibili agli utenti legittimi. Il risultato è che gli utenti autorizzati non riescono a ottenere accesso ai dati o ai servizi necessari.

Ransomware: Questa minaccia riguarda l'uso di malware, come il ransomware, per crittografare i dati aziendali e richiedere un riscatto per la loro decrittazione. Quando i dati sono crittografati da un attaccante, diventano inaccessibili agli utenti aziendali fino a quando il riscatto non viene pagato e i dati vengono ripristinati. Ciò può avere un impatto significativo sulla disponibilità dei dati.

Per evitare ciò, si possono prende alcune contromisure :

Pianificazione della capacità: Assicurati che i tuoi sistemi e le tue reti abbiano sufficiente capacità per gestire il carico di lavoro previsto e le picchi di utilizzo.

Backup e ripristino dei dati: Esegui regolarmente backup dei dati critici e sviluppa un piano di ripristino dei dati in modo da poter recuperare rapidamente in caso di perdita di dati o di attacchi ransomware.

Pianificazione della continuità aziendale: Sviluppa piani di continuità aziendale e di ripristino del servizio in modo da poter affrontare situazioni di emergenza e ripristinare la disponibilità dei dati il più rapidamente possibile.