W18D5

SECURITY OPERATION CIA

La traccia

Obiettivo dell'esercizio: Verificare la comprensione dei concetti di confidenzialità, integrità e disponibilità dei dati.

Scenario: Sei un consulente di sicurezza informatica e un'azienda ti ha assunto per valutare la sicurezza dei suoi sistemi informatici. Durante la tua analisi, ti accorgi che l'azienda ha problemi con la triade CIA. Il tuo compito è identificare e risolvere tali problemi.

Fornisci un breve rapporto in cui indichi le aree di miglioramento e le misure suggerite per aumentare la sicurezza dei dati.

La traccia

Confidenzialità:

Spiega cosa si intende per confidenzialità dei dati.
Identifica due potenziali minacce alla confidenzialità dei dati dell'azienda.
Suggerisci due contromisure per proteggere i dati da queste minacce.

Integrità:

Spiega cosa si intende per integrità dei dati.
Identifica due potenziali minacce alla integrità dei dati dell'azienda.
Suggerisci due contromisure per proteggere i dati da queste minacce.

Disponibilità:

Spiega cosa si intende per disponibilità dei dati.
Identifica due potenziale minaccia alla disponibilità dei dati dell'azienda.
Suggerisci due contromisura per proteggere i dati da questa minaccia.

Individuazione dei controlli CIA

Come riferimento per i controlli da attuare in merito alla sicurezza informatica di un'azienda prendiamo in considerazione l' **ISO/IEC 27001:2022**, in particolare l'allegato A dove sono elencati i controlli, e l' **ISO/IEC 27002:2022** dove vengono forniti i dettagli relativi a tali controlli.

I controlli in questione possono attenere a una o più dimensioni della CIA, principio cardine per valutare lo stato di sicurezza delle informazioni.
Per ognuna delle dimensioni verranno esposti due esempi di controlli.

Controlli relativi alla ‘Confidenzialità’

Confidentiality: secondo tale principio l’accesso al dato deve essere garantito solo agli utenti autorizzati.

7.7 Clear desk and clear screen

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Physical_security	#Protection

Questo è un controllo di tipo **preventivo** e prevede: regole di pulizia per documenti e supporti di memorizzazione rimovibili e le regole di pulizia dello schermo per le strutture di elaborazione delle informazioni che dovrebbero essere definite e applicate in modo appropriato.

Le **minacce** sono di perdita e danneggiamento delle informazioni su scrivanie, schermi e in altre posizioni accessibili durante e al di fuori dell'orario di lavoro normale.

Esempi di contromisure possono essere:

- Proteggere i dispositivi endpoint degli utenti con serrature a chiave o altri mezzi di sicurezza quando non sono in uso o non sorvegliati.
- Cancellare le informazioni sensibili o critiche dalle lavagne e da altri tipi di schermi quando non sono più necessarie.

8.10 Information deletion

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Information_protection #Legal_and_compliance	#Protection

Questo è un controllo di tipo **preventivo** e prevede che le informazioni memorizzate nei sistemi informativi, nei dispositivi o in qualsiasi altro supporto di archiviazione devono essere cancellate quando non sono più necessarie.

Le **minacce** sono una esposizione non necessaria di informazioni sensibili e il non rispetto dei requisiti legali, statutari, normativi e contrattuali per la cancellazione delle informazioni.

Esempi di contromisure possono essere adottare diversi metodi di rimozione dati:

a) Configurare i sistemi per distruggere in modo sicuro le informazioni quando non sono più necessarie (ad esempio, dopo un periodo definito soggetto alla politica specifica sull'archiviazione dei dati o su richiesta di accesso soggetto);
b) Eliminare le versioni obsolete, le copie e i file temporanei ovunque si trovino.

Controlli relativi alla ‘Integrity’

Integrity: si riferisce alla garanzia che i dati siano accurati, completi e non manomessi.

8.17 Clock synchronization

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Integrity	#Protect #Detect	#Information_security_event_management	#Protection #Defence

Questo è un controllo di tipo **investigativo** e prevede che i dispositivi di elaborazione delle informazioni utilizzati dall'organizzazione dovrebbero essere sincronizzati con fonti di tempo approvate.

Le **minacce** consistono nel fatto che gli errori di sequenza e difficoltà nelle indagini possono compromettere l'integrità delle informazioni registrate nei log, mettendo a rischio la credibilità delle prove e l'efficacia delle risposte agli incidenti.

Esempi di contromisure possono essere adottare diversi metodi di rimozione dati:

Un orologio collegato a una trasmissione radio temporizzata da un orologio atomico nazionale o dal sistema di posizionamento globale (GPS) dovrebbe essere utilizzato come orologio di riferimento per i sistemi di registrazione; una fonte di data e ora coerente e affidabile per garantire timestamp precisi. Protocolli come il protocollo di tempo di rete (NTP) o il protocollo di tempo di precisione (PTP) dovrebbero essere utilizzati per mantenere tutti i sistemi in rete sincronizzati con un orologio di riferimento. L'organizzazione può utilizzare contemporaneamente due fonti di tempo esterne al fine di migliorare l'affidabilità degli orologi esterni e gestire adeguatamente eventuali variazioni.

Controlli relativi alla ‘Availability’

Availability: si riferisce alla disponibilità del dato che deve essere garantita in ogni situazione.

8.13 Information backup

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection

Questo è un controllo di tipo **correttivo** e prevede che le copie di backup delle informazioni, del software e dei sistemi dovrebbero essere mantenute e regolarmente testate in conformità alla politica specifica sull'argomento concordata sul backup.

Le **minacce** consistono semplicemente nella perdita dei dati e questo controllo vale sia per l'integrity che per l'availability.

Dovrebbero essere fornite strutture di backup adeguate per garantire che tutte le informazioni essenziali e il software possano essere ripristinati in caso di incidenti, guasti o perdita dei supporti di archiviazione. Nella progettazione di un piano di backup, dovrebbero essere prese in considerazione le seguenti voci:
a) produrre registrazioni accurate e complete delle copie di backup e procedure documentate di ripristino;
b) riflettere i requisiti aziendali dell'organizzazione, i requisiti di sicurezza delle informazioni coinvolte e la criticità delle informazioni per il funzionamento continuato dell'organizzazione nell'entità (ad es. backup completo o differenziale) e la frequenza dei backup;
c) memorizzare i backup in un luogo remoto sicuro, a una distanza sufficiente per evitare danni da un disastro presso il sito principale;

8.14 Redundancy of information processing facilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Availability	#Protect	#Continuity #Asset_management	#Protection #Resilience

Questo è un controllo di tipo **preventivo** e prevede che le strutture di elaborazione delle informazioni devono essere implementate con una ridondanza sufficiente per soddisfare i requisiti di disponibilità.

Le **minacce** consistono nel fatto che l'implementazione di ridondanze può comportare rischi per l'integrità e la riservatezza delle informazioni, come errori introdotti durante la copia dei dati o controlli di sicurezza deboli. La ridondanza non affronta di solito l'indisponibilità delle applicazioni dovuta a difetti all'interno di un'applicazione stessa.

L'organizzazione deve garantire che i servizi aziendali e i sistemi informativi siano sempre disponibili. Per fare ciò, è necessario progettare e implementare un'architettura con ridondanza adeguata, duplicando le strutture di elaborazione delle informazioni e attivando procedure per gestire i componenti ridondanti.
Al momento di implementare sistemi ridondanti, l'organizzazione dovrebbe considerare diverse strategie, come:

a) contrattare con due o più fornitori di rete e infrastrutture critiche, come fornitori di servizi Internet;
b) utilizzare reti ridondanti;
c) utilizzare due data center geograficamente separati con sistemi duplicati;