M5 D5

ESERCIZIO 1

GIORNO 2 – THREAT INTELLIGENCE

1) **Raccolta informazioni:**

   Cercare info sulle minacce alla sicurezza informatica utilizzando fonti aperte, siti web di sicurezza informatica e forum di discussione.

   Alcune fonti affidabili includono:
   - Siti web di organizzazioni di sicurezza informatica come il CERT (Computer Emergency Response Team) o agenzie governative responsabili della sicurezza informatica;
   - Siti web di fornitori di soluzioni di sicurezza informatica che forniscono informazioni sulle minacce attuali e sulle contromisure;
   - Forum di discussione dedicati alla sicurezza informatica, dove gli esperti condividono informazioni e discutono le ultime minacce.

2) **Analisi delle minacce:**

   Dopo aver raccolto le informazioni, analizzare ciascuna minaccia in dettaglio per comprendere come può essere utilizzata per compromettere la sicurezza e i danni che può causare.

   Alcuni aspetti importanti da considerare includono:
   - Modalità di diffusione: come la minaccia si diffonde (ad esempio, tramite email, siti web compromessi, collegamenti malevoli, etc.);
   - Meccanismi di attacco: come la minaccia interagisce con i sistemi o gli utenti per ottenere accesso non autorizzato o per diffondersi;
   - Obiettivi e danni: quali sono gli obiettivi primari della minaccia e quali danni può causare all'azienda, come il furto di dati sensibili, l'interruzione dei servizi o danni finanziari.

3) **Creazione dell'elenco delle minacce:**

   Utilizzare informazioni raccolte e l'analisi effettuata per creare un elenco delle minacce più comuni che possono colpire un'azienda come:
   - Phishing: tentativi di frode che mirano ad ottenere informazioni sensibili come password o numeri di carta di credito utilizzando tecniche di ingegneria sociale;
   - Malware: software dannoso progettato per compromettere i sistemi, come virus, worm, trojan, ransomware, spyware, etc;
   - Attacchi DDoS: attacchi distribuiti di negazione del servizio che mirano a sovraccaricare i sistemi o le reti, causando l'interruzione dei servizi;
   - Furto di dati: illecita acquisizione di informazioni sensibili o riservate, come dati personali dei clienti o informazioni aziendali riservate.

   Da fornire dettagli su ciascuna minaccia nell'elenco, come il modo in cui viene eseguita, i segni di riconoscimento e le misure di prevenzione consigliate.