Pratica 19D1

Traccia:

EPICODE

Esercizio
Threat Intelligence & IOC

Traccia:
Creare un elenco di minacce comuni che possono colpire un'azienda, ad esempio phishing, malware, attacchi DDoS, furto di dati.

- Inizia raccogliendo informazioni sulle minacce alla sicurezza informatica, utilizzando fonti aperte, i siti web di sicurezza informatica e i forum di discussione.
- Analizza ciascuna minaccia in dettaglio, cercando di comprendere il modo in cui può essere utilizzata per compromettere la sicurezza informatica e i danni che può causare.
- Utilizza queste informazioni per creare un elenco delle minacce più comuni, tra cui malware, attacchi di phishing e attacchi DDoS aggiungendo tutte le informazioni raccolte dall'analisi.

Soluzione:

1. Phishing

- **Descrizione**: Il phishing è una tecnica di ingegneria sociale che mira a ingannare gli utenti affinché rivelino informazioni confidenziali, come password e dettagli della carta di credito, attraverso email, messaggi o siti web fraudolenti che sembrano legittimi.
- **Modalità di Attacco**: Gli attaccanti inviano email o messaggi che sembrano provenire da fonti affidabili, invitando le vittime a cliccare su link malevoli o allegati infetti.
- **Danni**: Furto di identità, perdita di dati sensibili, accesso non autorizzato a sistemi critici.

2. Malware

- **Descrizione**: Il termine "malware" si riferisce a qualsiasi software malevolo progettato per danneggiare o sfruttare qualsiasi programma o rete informatica.
- **Tipologie**: Virus, worm, trojan, ransomware, spyware.
- **Modalità di Attacco**: Può essere distribuito tramite email, download da internet, dispositivi di archiviazione infetti e vulnerabilità di rete.
- **Danni**: Danni ai file o ai sistemi, furto di dati, perdita di controllo sui dispositivi infetti, estorsione (nel caso di ransomware).

3. Attacchi DDoS (Distributed Denial of Service)

- **Descrizione**: Un attacco DDoS mira a sovraccaricare le risorse di sistema di un sito web o servizio online, rendendolo inaccessibile agli utenti legittimi.
- **Modalità di Attacco**: Vengono utilizzati numerosi computer infetti (botnet) per generare un volume elevato di richieste verso il target.
- **Danni**: Interruzione dei servizi online, perdite finanziarie, degrado della fiducia degli utenti.

4. Furto di Dati

- **Descrizione**: Questa minaccia comporta l'accesso non autorizzato e il furto di dati aziendali sensibili, come informazioni finanziarie, dati personali dei clienti o proprietà intellettuale.
- **Modalità di Attacco**: Può avvenire tramite breccia di sicurezza, phishing, malware o insider malintenzionati.
- **Danni**: Perdita finanziaria, danno alla reputazione, azioni legali da parte di terzi interessati.

5. Insider Threat

- **Descrizione**: Le minacce interne provengono da individui all'interno dell'organizzazione, come dipendenti, appaltatori o partner commerciali, che hanno accesso a sistemi e dati sensibili.
- **Modalità di Attacco**: Abuso di accessi legittimi per furto di dati, sabotaggio o spionaggio industriale.
- **Danni**: Perdita di dati sensibili, danni ai sistemi interni, perdita di vantaggi competitivi.

6. Zero-Day Exploit

- **Descrizione**: Un exploit zero-day sfrutta una vulnerabilità software non ancora nota al produttore o al pubblico, lasciando agli sviluppatori poco o nessun tempo per rilasciare una patch.
- **Modalità di Attacco**: Gli attaccanti individuano e sfruttano queste vulnerabilità prima che vengano corrette.
- **Danni**: Accesso non autorizzato, furto di dati, installazione di malware.

7. Man-in-the-Middle (MitM) Attacks

- **Descrizione**: In questi attacchi, l'aggressore si interpone tra due parti comunicanti, intercettando e potenzialmente alterando i dati scambiati.
- **Modalità di Attacco**: Spesso si verifica in reti non sicure, come Wi-Fi pubblici, tramite tecniche di spoofing o session hijacking.
- **Danni**: Furto di informazioni sensibili, manipolazione dei dati.