Report Esercizio

W19-D2

Redatto da Andrea Sciattella

25/06/2024

TRACCIA

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

1. Inizia raccogliendo informazioni sulle minacce alla sicurezza informatica, utilizzando fonti aperte, i siti web di sicurezza informatica e i forum di discussione.
2. 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.
3. 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.

SVOLGIMENTO ESERCIZIO

Abbiamo riassunto in elenco alcune delle minacce più comuni che possono colpire un'azienda, descrivendo dettagliatamente ciascuna minaccia e il modo in cui può essere utilizzata per compromettere la sicurezza informatica e i danni che può causare:

1. Phishing

Il phishing è una tecnica di ingegneria sociale in cui gli attaccanti inviano e-mail, messaggi o siti web fraudolenti per indurre le vittime a rivelare informazioni sensibili come credenziali di accesso, informazioni finanziarie o dati personali.

Modalità di attacco:

- **E-mail di phishing**: Messaggi che sembrano provenire da fonti affidabili (banche, colleghi, servizi online) contenenti link a siti web falsi o allegati dannosi.
- **Spear phishing**: Attacchi mirati verso individui specifici, spesso personalizzati per aumentare le probabilità di successo.
- **Phishing via SMS (smishing) e via telefono (vishing**): Utilizzo di SMS e chiamate telefoniche per ottenere informazioni personali.

Danni:

- Compromissione delle credenziali di accesso.
- Furto di dati personali e finanziari.
- Accesso non autorizzato ai sistemi aziendali.
- Perdita di fiducia dei clienti e danni alla reputazione aziendale.

2. Malware

Il malware è un software dannoso progettato per danneggiare, infiltrarsi o rubare informazioni dai sistemi informatici. Include virus, worm, trojan, ransomware, spyware e adware.

Modalità di attacco:

- **Virus:** Programmi che si replicano e si diffondono tramite file infetti.

- **Worm:** Malware che si diffonde autonomamente attraverso reti informatiche.
- **Trojan:** Software che sembra legittimo ma contiene funzioni dannose.
- **Ransomware:** Cripta i dati dell'utente, richiedendo un riscatto per decriptarli.
- **Spyware:** Raccoglie informazioni sugli utenti senza il loro consenso.
- **Adware:** Mostra annunci indesiderati e può tracciare le attività online.

Danni:

- Perdita o danneggiamento di dati.
- Interruzione dei servizi aziendali.
- Furto di informazioni sensibili.
- Costi finanziari per la rimozione del malware e il recupero dei dati.
- Rischi legali e perdita di fiducia dei clienti.

3. Attacchi DDoS (Distributed Denial of Service)

Gli attacchi DDoS mirano a rendere un servizio o un sito web inaccessibile sovraccaricando il server con un flusso massiccio di traffico da più fonti.

Modalità di attacco:

- **Botnet:** Reti di computer infetti (zombie) controllati da un attaccante per generare traffico massiccio verso il bersaglio.
- **Amplification attacks:** Utilizzo di richieste a server vulnerabili che rispondono con un volume maggiore di dati per sovraccaricare il bersaglio.

Danni:

- Interruzione dei servizi online.
- Perdita di entrate a causa dell'inaccessibilità del sito web o del servizio.
- Costi di mitigazione e riparazione.
- Danni alla reputazione aziendale.

4. Furto di dati (Data Breach)

Il furto di dati si verifica quando informazioni sensibili vengono accedute, copiate o divulgate senza autorizzazione.

Modalità di attacco:

- **Exfiltrazione:** Prelievo di dati attraverso accesso non autorizzato ai sistemi informatici.
- **Insider threats:** Dipendenti o collaboratori che rubano dati dall'interno dell'azienda.
- **Hacking:** Accesso non autorizzato ai database attraverso vulnerabilità nei sistemi di sicurezza.

***Danni*:**

- Compromissione di informazioni sensibili (dati personali, finanziari, proprietari).
- Danni finanziari dovuti a sanzioni legali e costi di notifica.
- Perdita di fiducia dei clienti e danni alla reputazione.
- Possibili cause legali e responsabilità civile.

5. Attacchi di Social Engineering

Gli attacchi di social engineering manipolano le persone per ottenere informazioni confidenziali o accesso non autorizzato ai sistemi aziendali.

Modalità di attacco:

- **Pretexting:** Creazione di una falsa identità per ottenere informazioni.
- **Baiting:** Offerta di un incentivo per indurre le vittime a rivelare informazioni o eseguire azioni.
- **Tailgating:** Accesso fisico non autorizzato agli edifici aziendali seguendo una persona autorizzata.

Danni:

- Compromissione di sistemi e dati aziendali.
- Rischi di sicurezza fisica e informatica.
- Perdita di fiducia dei clienti e danni alla reputazione.

6. Vulnerabilità del software

Descrizione: Le vulnerabilità del software sono difetti o debolezze nel codice che possono essere sfruttate per compromettere la sicurezza di un sistema.

Modalità di attacco:

- **Exploits:** Codice che sfrutta le vulnerabilità del software per ottenere accesso non autorizzato o eseguire codice dannoso.

- **Zero-day attacks:** Attacchi che sfruttano vulnerabilità non ancora note o patchate.

Danni:

- Accesso non autorizzato ai sistemi informatici.
- Esecuzione di codice dannoso.
- Interruzione dei servizi e perdita di dati.
- Costi di patching e aggiornamento del software.

7. Insider Threats

Le minacce interne derivano da dipendenti, ex dipendenti, appaltatori o partner che hanno accesso legittimo ai sistemi aziendali e abusano di tale accesso.

Modalità di attacco:

- **Sabotaggio:** Danneggiamento intenzionale dei sistemi aziendali.
- **Furto di dati:** Prelievo di informazioni sensibili per uso personale o vendita.
- **Frode:** Manipolazione dei sistemi per scopi fraudolenti.

***Danni*:**

- Compromissione di dati sensibili.
- Danni finanziari e legali.
- Perdita di fiducia dei clienti e danni alla reputazione.

8. Attacchi APT (Advanced Persistent Threats)

Gli APT sono attacchi sofisticati e mirati che si protraggono nel tempo, con l'obiettivo di rubare informazioni sensibili o sabotare le operazioni aziendali.

Modalità di attacco:

- **Phishing e spear phishing:** Per ottenere accesso iniziale.
- **Malware customizzato:** Progettato per rimanere nascosto e raccogliere informazioni.
- **Movimento laterale:** Espansione del controllo all'interno della rete aziendale.

Danni:

- Furto di informazioni sensibili a lungo termine.
- Compromissione della sicurezza nazionale (se colpisce infrastrutture critiche).

- Danni finanziari e di reputazione.

9. Attacchi Man-in-the-Middle (MitM)

Gli attacchi MitM si verificano quando un attaccante si inserisce in una comunicazione tra due parti, intercettando e alterando le informazioni scambiate.

Modalità di attacco:

- **Intercettazione delle comunicazioni:** Utilizzando reti Wi-Fi non sicure o vulnerabilità nei protocolli di comunicazione.
- **Sostituzione di certificati:** Per falsificare siti web sicuri e intercettare dati sensibili.

Danni:

- Furto di credenziali di accesso e dati sensibili.
- Manipolazione delle comunicazioni.
- Perdita di fiducia dei clienti e danni alla reputazione.

10. Ransomware

Il ransomware è un tipo di malware che cripta i file della vittima, richiedendo un riscatto per decriptarli.

Modalità di attacco:

- **Phishing:** Diffusione del malware tramite e-mail contenenti allegati o link infetti.
- **Vulnerabilità del software:** Sfruttamento di falle nei sistemi per distribuire il malware.

Danni:

- Inaccessibilità ai dati critici.
- Costi del riscatto e delle operazioni di ripristino.
- Danni finanziari e operativi.
- Rischi legali e perdita di fiducia dei clienti.

11. Whaling

Il whaling è una forma di phishing mirato che prende di mira i dirigenti di alto livello (come CEO, CFO e altri executive) all'interno di un'azienda. Questo tipo di attacco sfrutta tecniche di ingegneria sociale altamente sofisticate per indurre le vittime a rivelare informazioni sensibili o a eseguire azioni dannose.

Modalità di attacco:

- **E-mail di spoofing:** Gli attaccanti inviano e-mail che sembrano provenire da fonti fidate, come colleghi o partner commerciali, richiedendo azioni urgenti come il trasferimento di fondi o la divulgazione di informazioni riservate.
- **Falsi siti web:** Creazione di siti web fasulli che imitano quelli legittimi per ingannare la vittima e indurla a inserire le proprie credenziali di accesso.
- **Social engineering:** Raccolta di informazioni dettagliate sulle vittime attraverso fonti pubbliche e private per rendere gli attacchi più convincenti e personalizzati.

Danni:

- **Furto di informazioni sensibili:** Compromissione di dati aziendali critici, inclusi segreti commerciali e piani strategici.
- **Perdite finanziarie:** Trasferimenti di fondi non autorizzati che possono causare significative perdite economiche.
- **Danni reputazionali:** Perdita di fiducia dei clienti, partner commerciali e azionisti, con conseguenze negative a lungo termine sulla reputazione aziendale.
- **Rischi legali:** Potenziali cause legali e sanzioni normative a causa della compromissione dei dati sensibili e delle informazioni personali.

12. Cryptojacking

Il cryptojacking è una pratica in cui i criminali informatici utilizzano in modo non autorizzato le risorse di calcolo di un dispositivo (computer, smartphone, server) per minare criptovalute. Questo tipo di attacco sfrutta il potere di elaborazione delle macchine infette senza il consenso del proprietario.

Modalità di attacco:

- **Malware:** Installazione di malware sui dispositivi della vittima che esegue il mining di criptovalute.

- **Script web:** Inserimento di script di mining in siti web compromessi. Quando un utente visita il sito infetto, il suo browser esegue lo script di mining senza che lui ne sia consapevole.
- **Applicazioni infette:** Distribuzione di applicazioni contenenti codici di mining tramite app store o siti web di download.

Danni:

- **Riduzione delle prestazioni:** L'uso non autorizzato delle risorse di calcolo può rallentare significativamente i dispositivi infetti, riducendo le prestazioni e l'efficienza operativa.
- **Aumento dei costi operativi:** Maggior consumo di energia elettrica e risorse hardware, portando a costi aggiuntivi per l'azienda.
- **Sicurezza compromessa:** La presenza di malware di cryptojacking può indicare falle di sicurezza nei sistemi aziendali, che potrebbero essere sfruttate per ulteriori attacchi.
- **Usura dell'hardware:** L'uso intensivo delle risorse di calcolo può accelerare l'usura dell'hardware, riducendone la vita utile e aumentando i costi di manutenzione e sostituzione.