Report di Analisi di Sicurezza e Mitigazione delle Minacce in un Contesto Aziendale

Scenario:

Lavoro in un'azienda globale che opera nel settore finanziario, con un SOC (Security Operations Center) e un CSIRT (Computer Security Incident Response Team) dedicati alla protezione dei dati sensibili dei clienti e delle operazioni finanziarie. Recentemente, due utenti hanno segnalato problemi sui loro computer e hanno chiesto assistenza al reparto tecnico, che sono io. Questi problemi sembrano essere i primi sintomi di una più vasta campagna di attacchi mirati contro l'azienda.

Segnalazioni:

1. **Utente A**: Ha ricevuto un'email con un link sospetto che, una volta cliccato, ha aperto una pagina web che richiedeva il login con le credenziali aziendali.
2. **Utente B**: Ha notato un rallentamento significativo del computer dopo aver visitato un sito web per scaricare un software apparentemente legittimo.

Passaggi dell'Analisi:

1. **Raccolta Informazioni**
2. **Analisi Forense**
3. **Mitigazione delle Minacce**
4. **Risoluzione del Problema**
5. **Prevenzione e Raccomandazioni**

Passaggio 1: Raccolta Informazioni

Email di Phishing (Utente A):

- **Indirizzo email del mittente**: unknown@example.com
- **Oggetto dell'email**: "Urgent: Verify Your Account"
- **Link sospetto**: https://example.com/verify

Sito Web Sospetto (Utente B):

- **URL visitato**: https://example.com/download
- **Descrizione del problema**: Rallentamento del sistema e comportamento anomalo

Passaggio 2: Analisi Forense

Analisi dell'Email di Phishing:

1. **VirusTotal**:
    - **Risultati**: 7 su 70 motori rilevano il link come dannoso.
    - **Tipo di minaccia**: Phishing.

- **Dettagli**: Il link reindirizza a una pagina di login falsa che imita il sito dell'azienda.

2. **Header dell'Email**:
    - **Analisi**: I dettagli dell'header indicano che l'email proviene da un server non autenticato, con evidenti segnali di spoofing.
3. **Contenuto dell'Email**:
    - **Testo**: Messaggio urgente che richiede la verifica dell'account tramite un link.
    - **Link**: Punta a una pagina web che raccoglie credenziali.

Analisi del Sito Web Sospetto:

1. **VirusTotal**:
    - **Risultati**: 15 su 70 motori rilevano il link come dannoso.
    - **Tipo di minaccia**: Distribuzione di malware.
    - **Dettagli**: Il link scarica un file eseguibile dannoso.
2. **Sucuri SiteCheck**:
    - **Malware**: Malware rilevato, il sito tenta di scaricare un file dannoso.
    - **Blacklist**: Il sito è presente in diverse blacklist.
    - **Dettagli**: Il sito utilizza tecniche di ingegneria sociale per convincere gli utenti a scaricare il file.
3. **Sandbox Any.Run**:
    - **Comportamento**: Il file scaricato tenta di connettersi a un server remoto e di installare un trojan.
    - **Dettagli**: Attività anomale nel sistema dopo l'esecuzione del file, incluso il tentativo di esfiltrare dati.

Passaggio 3: Mitigazione delle Minacce

Email di Phishing:

1. **Isolamento dell'Utente A**: Disconnettere il dispositivo di Utente A dalla rete aziendale per evitare la propagazione della minaccia.
2. **Analisi del Dispositivo**: Eseguire una scansione approfondita del sistema per rilevare eventuali compromissioni utilizzando strumenti di sicurezza avanzati come EDR (Endpoint Detection and Response).
3. **Blocco del Mittente**: Aggiornare i filtri antispam per bloccare il mittente dell'email sospetta e aggiungere il dominio alla lista nera.
4. **Notifica agli Utenti**: Inviare un avviso a tutti gli utenti aziendali sulla campagna di phishing in corso, includendo suggerimenti su come riconoscere email sospette.

Sito Web Sospetto:

1. **Isolamento dell'Utente B**: Disconnettere il dispositivo di Utente B dalla rete aziendale per prevenire ulteriori danni.
2. **Analisi del Dispositivo**: Eseguire una scansione approfondita del sistema per rilevare e rimuovere il malware utilizzando software di sicurezza e strumenti di sandboxing.
3. **Aggiornamento delle Policy di Sicurezza**: Implementare restrizioni per impedire il download di software non autorizzato e aggiornare le regole del firewall per bloccare accessi a siti noti per distribuzione di malware.
4. **Monitoraggio del Traffico**: Verificare se altri dispositivi hanno visitato il sito sospetto e adottare misure preventive per evitare future compromissioni.

Passaggio 4: Risoluzione del Problema

1. **Pulizia dei Dispositivi**:
    - **Utente A**: Nessuna compromissione rilevata dopo la scansione; dispositivo sicuro.
    - **Utente B**: Malware rilevato e rimosso; il dispositivo è stato ripristinato a uno stato sicuro.
2. **Aggiornamento dei Sistemi di Sicurezza**:
    - **Antivirus e Antimalware**: Aggiornare tutti i software di sicurezza sui dispositivi aziendali per assicurare la protezione contro le minacce più recenti.
    - **Filtri Email**: Rafforzare i filtri per bloccare email di phishing future e implementare autenticazione avanzata come SPF, DKIM e DMARC.
    - **Firewall**: Configurare il firewall per bloccare accessi a siti sospetti e monitorare il traffico in entrata e uscita.

Passaggio 5: Prevenzione e Raccomandazioni

1. **Formazione degli Utenti**:
    - **Campagne di Sensibilizzazione**: Condurre sessioni di formazione periodiche sulla sicurezza per educare gli utenti sui rischi di phishing e malware.
    - **Esercitazioni di Phishing**: Simulare attacchi di phishing per valutare la prontezza degli utenti e migliorare la loro capacità di riconoscere minacce.
2. **Strumenti di Sicurezza**:
    - **Endpoint Detection and Response (EDR)**: Implementare soluzioni EDR per monitorare e rispondere alle minacce in tempo reale, migliorando la visibilità sui dispositivi aziendali.
    - **Sistemi di Intrusion Detection and Prevention (IDPS)**: Rafforzare le misure di rilevamento e prevenzione delle intrusioni per proteggere l'infrastruttura di rete.
3. **Monitoraggio Continuo**:

- **Log di Sicurezza**: Analizzare regolarmente i log di sicurezza per individuare attività sospette e migliorare le capacità di risposta agli incidenti.
- **Analisi del Traffico di Rete**: Monitorare il traffico di rete per rilevare e bloccare eventuali tentativi di esfiltrazione di dati o attività malevole.

Report Dettagliato

1. Descrizione degli Incidente:

- **Utente A**: Email di phishing con link a una pagina di login falsa. Dopo l'analisi forense, è emerso che il link mirava a raccogliere credenziali aziendali.
- **Utente B**: Rallentamento del sistema dopo aver visitato un sito web per scaricare software dannoso. L'analisi ha rivelato che il sito distribuiva un trojan che tentava di esfiltrare dati.

2. Analisi dei Link:

- **Link 1**: Identificato come phishing, tenta di raccogliere credenziali di login. Rilevato da 7 motori su VirusTotal.
- **Link 2**: Identificato come fonte di malware, tenta di scaricare e installare un trojan. Rilevato da 15 motori su VirusTotal.

3. Azioni Consigliate:

- **Link 1**: Disconnettere il dispositivo di Utente A, eseguire una scansione approfondita, bloccare il mittente, e avvisare tutti gli utenti.
- **Link 2**: Disconnettere il dispositivo di Utente B, eseguire una scansione approfondita, aggiornare le policy di sicurezza, e monitorare il traffico di rete.

4. Conclusioni:

- Entrambi i link rappresentano minacce significative alla sicurezza dell'azienda. È essenziale migliorare la formazione degli utenti sulla sicurezza e rafforzare le misure di difesa per prevenire futuri incidenti simili.

5. Prevenzione:

- **Formazione**: Condurre sessioni di formazione periodiche e esercitazioni di phishing.
- **Strumenti di Sicurezza**: Implementare soluzioni EDR e IDPS.
- **Monitoraggio Continuo**: Analizzare regolarmente i log di sicurezza e monitorare il traffico di rete.

Note Aggiuntive:

- **Rapporto Continuo con gli Utenti**: Mantenere una comunicazione costante con gli utenti per aggiornarli sulle minacce attuali e le migliori pratiche di sicurezza.
- **Revisione delle Policy di Sicurezza**: Aggiornare regolarmente le policy di sicurezza aziendali per adattarsi alle nuove minacce.
- **Esercitazioni Periodiche**: Condurre esercitazioni periodiche per testare la prontezza della risposta agli incidenti e migliorare continuamente i processi di sicurezza.