Prompt:
Nella nostra azienda stiamo valutando la reattività di risposta ad un possibile attacco ransomware di modello avanzato. Puoi creare uno scenario che simuli una campagna ransomware mirata, eseguita manualmente da un attaccante (umano)?

Scenario

La mia azienda ha deciso di mettere alla prova la propria capacità di affrontare un attacco ransomware sofisticato e mirato. Per fare ciò, ho creato un ambiente di test controllato, all'interno del quale verrà simulato un attacco. L'obiettivo è analizzare in dettaglio ogni fase dell'attacco, identificare le debolezze sfruttate dagli aggressori e sviluppare un piano di difesa solido per proteggere la mia azienda da future minacce simili.

Obiettivi della Simulazione

1. **Riprodurre un attacco ransomware avanzato**: Simulare un attacco realistico per comprendere come il ransomware potrebbe penetrare e diffondersi nella rete aziendale.
2. **Esaminare le fasi dell'attacco**: Studiare attentamente le tecniche di infezione, propagazione, cifratura dei dati e richiesta di riscatto.
3. **Individuare vulnerabilità**: Capire quali punti deboli della rete e dei sistemi potrebbero essere sfruttati per ottenere l'accesso iniziale e per muoversi lateralmente nella rete.
4. **Definire contromisure pratiche**: Proporre soluzioni mirate per prevenire e rispondere efficacemente a un attacco di questo tipo.

Fasi dell'Attacco Simulato

Per replicare un attacco ransomware mirato, il processo sarà suddiviso in diverse fasi, ciascuna focalizzata su un aspetto

specifico dell’attacco e su come questo possa evolvere all'interno dell'azienda.

Fase 1: Raccolta delle Informazioni (Ricognizione)

- **Obiettivo**: Scoprire dettagli sulla struttura interna dell’azienda, la sua rete, i dispositivi utilizzati e i dipendenti chiave.
- **Metodi utilizzati**:
  - **Social Engineering**: Verranno simulate telefonate fraudolente in cui ci si finge tecnici del supporto IT per estorcere informazioni. Inoltre, saranno inviate e-mail di phishing mirate, studiando i profili social dei dipendenti per personalizzare i messaggi e aumentare l’efficacia.
  - **Ricognizione passiva**: Utilizzo di strumenti come Shodan e motori di ricerca specializzati per individuare dispositivi esposti, servizi aperti e vulnerabilità potenzialmente sfruttabili senza generare allarmi sulla rete aziendale.

Fase 2: Accesso Iniziale (Infiltrazione)

- **Obiettivo**: Compromettere uno o più punti di ingresso nella rete aziendale.
- **Metodi**:
  - **E-mail di Phishing mirate**: Creazione di messaggi ingannevoli con allegati infetti o link a siti web compromessi, destinati a specifici dipendenti. Si ipotizza che uno di questi messaggi riesca a superare le difese e a infettare il computer del destinatario.
  - **Sfruttamento di vulnerabilità**: Testare le vulnerabilità conosciute nei software utilizzati dall’azienda, come una vulnerabilità non correttamente risolta in un’applicazione interna.

        - **USB Drop**: Lasciare dispositivi USB infetti nelle aree comuni dell'azienda con l’intenzione di indurre un dipendente a collegarlo a un computer aziendale, avviando l’infezione.

Fase 3: Mantenimento dell'Accesso (Persistenza)

- **Obiettivo**: Garantire l'accesso continuo alla rete aziendale, anche in caso di tentativi di rimozione.
- **Metodi**:
    - **Credential Dumping**: Utilizzo di strumenti come Mimikatz per estrarre credenziali sensibili dai sistemi compromessi, consentendo accessi futuri senza necessità di ulteriori exploit.
    - **Installazione di Backdoors**: Configurazione di porte di accesso nascoste che permettono all'attaccante di rientrare nella rete anche se il malware principale viene rimosso.

Fase 4: Aumento dei Privilegi (Escalation dei Privilegi)

- **Obiettivo**: Ottenere permessi amministrativi sui sistemi critici per avere controllo completo della rete.
- **Metodi**:
    - **Tecniche Pass the Hash**: Utilizzo di hash delle password intercettate per autenticarsi sui sistemi aziendali senza necessità di conoscere la password effettiva.
    - **Sfruttamento di vulnerabilità interne**: Individuazione e sfruttamento di bug o configurazioni deboli all'interno dei sistemi già compromessi per aumentare i privilegi.

Fase 5: Spostamento nella rete (Movimento Laterale)

- **Obiettivo**: Propagare l’infezione ad altri dispositivi nella rete aziendale.

- **Metodi**:
  - **Living off the Land**: Uso di strumenti e comandi già presenti nei sistemi operativi, come PowerShell e strumenti di amministrazione remota, per evitare di generare allarmi.
  - **Network Mapping**: Mappatura della rete per identificare altre macchine, server e risorse condivise, valutando i migliori obiettivi da compromettere.

Fase 6: Estrazione dei Dati (Esfiltrazione dei Dati)

- **Obiettivo**: Prelevare informazioni sensibili per creare ulteriore pressione sulla mia azienda affinché paghi il riscatto.
- **Metodi**:
  - **Data Exfiltration**: Utilizzo di canali di comunicazione cifrati per trasferire dati critici all'esterno della rete aziendale, evitando il rilevamento.

Fase 7: Cifratura dei Dati (Distribuzione del Ransomware)

- **Obiettivo**: Cifrare i dati sui sistemi compromessi per richiedere un riscatto.
- **Metodi**:
  - **Script per la Distribuzione**: Automazione della diffusione del ransomware su tutte le macchine collegate alla rete, rendendo l’attacco rapido e difficile da contenere.
  - **Disabilitazione dei Backup**: Individuazione e neutralizzazione dei sistemi di backup per rendere più difficile il ripristino dei dati senza il pagamento del riscatto.

Fase 8: Richiesta di Riscatto e Negoziazione

- **Obiettivo**: Forzare la mia azienda a pagare un riscatto per recuperare i dati cifrati.
- **Metodi**:
  - **Note di Riscatto**: Visualizzazione di istruzioni sui dispositivi compromessi per il pagamento del riscatto.
  - **Comunicazioni Cifrate**: Uso di canali anonimi e cifrati come Tor per negoziare il pagamento con la mia azienda.

Risposta della mia azienda alla simulazione

Durante questa simulazione, la mia azienda dovrà dimostrare la propria capacità di rispondere a ciascuna fase del ransomware, mettendo alla prova i seguenti aspetti:

1. **Rilevamento tempestivo**: Capacità di identificare e rispondere all'attacco nelle prime fasi, come durante la ricognizione e l'infiltrazione.
2. **Isolamento dei sistemi compromessi**: Capacità di isolare i dispositivi infetti per evitare che il ransomware si diffonda nella rete.
3. **Disponibilità di backup e ripristino rapido**: Efficienza nel recuperare i dati critici tramite backup regolari e sicuri.
4. **Comunicazione interna ed esterna**: Capacità di gestire le comunicazioni durante l'incidente, sia con i dipendenti sia con il pubblico, se necessario.
5. **Gestione delle negoziazioni**: Protocollo per decidere come gestire eventuali richieste di riscatto e se coinvolgere le forze dell'ordine.
6. **Analisi post-incidente**: Indagine approfondita delle vulnerabilità sfruttate, per potenziare le difese contro attacchi futuri.

Conclusioni per fare report

Alla fine della simulazione, produrrò un report dettagliato che descriva:

- Le vulnerabilità identificate durante l'attacco simulato.
- I dati compromessi e la capacità di ripristino.
- Le strategie di difesa più efficaci e quelle che necessitano miglioramenti.
- Il piano di mitigazione, con azioni specifiche per migliorare la sicurezza della rete aziendale e prevenire futuri attacchi ransomware.

Report di simulazione di attacco Ransomware nella mia azienda

1. Introduzione

Questo report documenta i risultati della simulazione di un attacco ransomware avanzato e mirato, eseguito per valutare la capacità della mia azienda di rilevare, rispondere e riprendersi da una minaccia simile. La simulazione è stata condotta in un ambiente controllato, replicando le tecniche più comuni utilizzate dagli aggressori, dalla fase di ricognizione alla richiesta di riscatto.

2. Vulnerabilità

Durante la simulazione, sono emerse diverse vulnerabilità sfruttabili da parte degli attaccanti. Le principali aree di debolezza identificate includono:

- **Mancanza di consapevolezza sul phishing**: Alcuni dipendenti non sono riusciti a identificare le e-mail di phishing mirate, aprendo allegati dannosi che hanno dato il via all'infezione.
- **Sistemi non aggiornati**: Alcuni sistemi software risultavano vulnerabili a exploit noti, dovuti alla mancanza di aggiornamenti regolari.

- **Backup online esposti**: I backup aziendali erano accessibili dai sistemi compromessi e non erano protetti adeguatamente con autenticazione a più fattori, consentendo la loro eliminazione da parte dell'attaccante.

3. Dati compromessi e capacità di ripristino

La simulazione ha dimostrato l'efficacia del ransomware nel cifrare rapidamente i dati critici della rete. Tuttavia, è stato anche testato il processo di ripristino dai backup:

- **Perdita temporanea di dati critici**: I file critici sono stati cifrati nel giro di poche ore dall'attivazione del ransomware. Ciò ha causato una perdita temporanea di accesso ai dati.
- **Ripristino dai backup**: Dopo aver rilevato l'attacco, è stato avviato il processo di ripristino utilizzando i backup settimanali. Tuttavia, si è evidenziata una mancanza di backup più recenti, che avrebbe ridotto ulteriormente la perdita di dati e il tempo di inattività.

4. Strategie di difesa efficaci

Durante la simulazione, alcune misure di sicurezza si sono rivelate particolarmente utili per contenere e mitigare l'attacco:

- **Segmentazione della Rete**: La segmentazione della rete ha ridotto la propagazione del ransomware, limitando il numero di dispositivi infetti.
- **IDS/IPS**: Il sistema di rilevamento e prevenzione delle intrusioni (IDS/IPS) ha identificato tempestivamente traffico anomalo generato dal ransomware, permettendo un isolamento rapido dei sistemi infetti.
- **Formazione ai Dipendenti**: Il personale che aveva ricevuto formazione recente sulle minacce di phishing è riuscito a identificare e segnalare tentativi di phishing, limitando l'efficacia dell'attacco iniziale.

5. Aree da Migliorare

La simulazione ha anche messo in evidenza delle aree critiche su cui la mia azienda deve intervenire per rafforzare la propria sicurezza:

- **Miglioramento della frequenza dei backup**: Implementare backup più frequenti (quotidiani o orari) per ridurre ulteriormente l'impatto di una cifratura dei dati.
- **Autenticazione a più fattori sui backup**: Migliorare la protezione dei sistemi di backup con autenticazione a più fattori per evitare che vengano compromessi durante un attacco.
- **Potenziare le strategie di formazione**: Estendere la formazione ai dipendenti su come riconoscere email di phishing sofisticate e migliorare la consapevolezza sulle tecniche di social engineering utilizzate dagli attaccanti.

6. Piano di mitigazione

Per migliorare la sicurezza della rete aziendale, è stato elaborato un piano di mitigazione che include le seguenti azioni:

- **Aggiornamento e patch dei sistemi**: Implementare una politica di aggiornamento continuo per tutti i software utilizzati dall'azienda, garantendo che tutte le vulnerabilità note siano risolte tempestivamente.
- **Implementazione di backup offsite**: Archiviare copie dei backup critici in una posizione offline, scollegata dalla rete principale, per garantire che i dati possano essere recuperati anche in caso di compromissione della rete.
- **Introduzione di EDR (Endpoint Detection and Response)**: Utilizzare soluzioni EDR per monitorare i comportamenti anomali sui dispositivi endpoint e rilevare movimenti laterali non autorizzati.
- **Simulazioni periodiche di attacchi**: Eseguire simulazioni di attacco e test di penetrazione regolari per valutare

continuamente la capacità dell’azienda di rispondere a nuove minacce.

7. Lezioni Apprese

La simulazione ha evidenziato alcune lezioni fondamentali per rafforzare la resilienza della mia azienda contro gli attacchi ransomware:

- **La velocità di reazione è cruciale**: Identificare e isolare tempestivamente i sistemi compromessi può ridurre drasticamente l’impatto del ransomware.
- **La formazione continua è essenziale**: I dipendenti rappresentano spesso il primo e l’ultimo baluardo contro le minacce informatiche. Investire in formazione è una delle migliori strategie per ridurre la superficie di attacco.
- **Non sottovalutare i backup**: I backup rappresentano una delle difese più efficaci contro il ransomware, ma devono essere configurati in modo sicuro e testati regolarmente per garantire l’affidabilità.

8. Conclusioni

La simulazione ha fornito una visione chiara delle vulnerabilità della mia azienda e ha permesso di individuare misure concrete per migliorare la sicurezza. Implementando le azioni indicate nel piano di mitigazione, la mia azienda sarà in grado di rispondere in modo più efficace a un eventuale attacco ransomware, riducendo i tempi di inattività e proteggendo i dati critici.