Condurre una simulazione di attacco ransomware mirata all'infrastruttura aziendale. L'obiettivo è testare le capacità di rilevamento, contenimento e ripristino, e identificare aree di miglioramento nelle politiche di sicurezza.

Scenario:
Un utente malintenzionato riesce a distribuire un ransomware attraverso un'email di phishing. Il ransomware si propaga nei sistemi aziendali, crittografando i file critici e chiedendo un riscatto. L'organizzazione deve rispondere dell'incidente e attuare misure per prevenirne di futuri.

Fase 1: Infiltrazione e Distribuzione del Ransomware

- Simulare un attacco di phishing: inviare email di phishing con allegati o link dannosi a utenti selezionati.
- Monitorare le reazioni degli utenti: verificare se qualcuno apre il file o clicca sul link, innescando l'infezione.
- Simulare la crittografia dei file: una volta che il ransomware è attivato, dimostrare come si diffonde attraverso la rete e crittografa i dati essenziali.

Fase 2: Diffusione e Richiesta di Riscatto

- Riprodurre la propagazione del ransomware sulla rete, simulando come compromette ulteriori dispositivi e server.
- Generare una schermata di riscatto che avvisa l'utente del blocco dei dati e richiede il pagamento.
- Verificare se i team di sicurezza rilevano tempestivamente l'attacco e attuano le prime contromisure.

Fase 3: Contenimento e Misure di Protezione

- Formazione e consapevolezza: valutare l'efficacia dei programmi di formazione per riconoscere il phishing.
- Segmentazione della rete: simulare l'efficacia della segmentazione nel limitare la diffusione del malware.
- Backup sicuri: testare la presenza di backup regolari e offline, capaci di garantire il recupero dei dati senza ricorrere al pagamento.
- Monitoraggio attivo: verificare l'efficacia degli strumenti di rilevamento automatico (come gli EDR) nel bloccare attività sospette.

Fase 4: Recupero e Ripristino

- Simulare l'uso del piano di disaster recovery per ripristinare i sistemi colpiti dai backup.
- Valutare la capacità dei team di sicurezza di isolare l'incidente, contenere la diffusione e riportare i sistemi in funzione in tempi rapidi.
- Testare le procedure di risposta per capire come i team di sicurezza identificano, segnalano e reagiscono all'attacco in tempo reale.

Fase 5: Lezioni Apprese e Miglioramento Continuo

- Organizzare una sessione di "lessons learned" con tutti i team coinvolti per rivedere le azioni intraprese durante la simulazione.
- Identificare i punti deboli nelle procedure di sicurezza, nella formazione degli utenti o nelle tecnologie utilizzate.
- Aggiornare le policy di incident response e migliorare le procedure per prevenire future infezioni ransomware.

Conclusione:
Questa simulazione di attacco ransomware consente alla tua organizzazione di testare la propria resilienza e di implementare misure preventive, come la segmentazione di rete, backup sicuri e formazione avanzata per il personale, garantendo una maggiore sicurezza contro futuri attacchi.

ESERCIZIO EXTRA (FACOLTATIVO)

Il 2024 Data Breach Investigations Report (DBIR) di Verizon presenta un'analisi dettagliata su 30.458 incidenti di sicurezza, con 10.626 violazioni confermate in 94 paesi. Ecco i principali punti salienti:

1. Attacchi Ransomware ed Estorsione: Questi attacchi continuano a rappresentare una minaccia significativa, presenti nel 23% delle violazioni. Tuttavia, sono in crescita i metodi di estorsione pura, senza crittografia, che costituiscono il 32% delle violazioni totali. Questo riflette le nuove strategie degli attori malevoli motivati finanziariamente.
2. Sfruttamento delle Vulnerabilità: C'è stato un aumento significativo (180%) delle violazioni causate dallo sfruttamento di vulnerabilità, spesso legate a exploit zero-day come MOVEit. Questo sottolinea l'importanza critica della gestione delle patch.
3. Componente Umana nelle Violazioni: Circa il 68% delle violazioni coinvolge errori umani o manipolazione (phishing, abuso di privilegi, ecc.). Il phishing rimane un problema rilevante, con attacchi spesso diretti alla compromissione di credenziali e applicazioni web.
4. Attacchi alla Catena di Fornitura: L'implicazione di terze parti, sia attraverso la violazione di partner diretti che mediante vulnerabilità nella catena di fornitura del software, è aumentata fino al 15% delle violazioni, con un incremento del 68% rispetto all'anno precedente.
5. Impatto sui Settori Specifici: Gli attacchi ransomware ed estorsione hanno colpito il 92% dei settori, con sanità e pubblica amministrazione tra i più bersagliati.

6. Costo del Ransomware: Il report sottolinea che la perdita mediana dovuta agli attacchi ransomware è stata di 46.000 dollari, ma può variare ampiamente in base alla dimensione dell'organizzazione, con richieste di riscatto che spesso oscillano tra l'1,34% e l'8,30% del fatturato aziendale.

7. Crescente Minaccia dell'Ingegneria Sociale: Il Compromesso di Email Aziendali (BEC) e gli attacchi di pretexting rappresentano una porzione significativa delle violazioni, con una perdita media per transazione di circa 50.000 dollari.

8. Gestione delle Vulnerabilità: Il tempo medio per applicare patch a vulnerabilità critiche nel catalogo CISA di Vulnerabilità Sfruttate è di circa 55 giorni, ma molte organizzazioni sono lente nel farlo, rimanendo esposte ad attacchi rapidi.

Il report enfatizza l'importanza di una gestione rapida delle vulnerabilità, della formazione degli utenti per ridurre i rischi di phishing e di un approccio solido alla gestione del rischio di terze parti. Il messaggio chiave è che le minacce informatiche stanno diventando più sofisticate, e le organizzazioni devono adottare un approccio più proattivo e strategico alla sicurezza .