

ESERCIZIO W21D1

IA e Cybersecurity

Mungiovì Fabio

TASK

Crea un prompt che aiuti la tua organizzazione a implementare delle misure di sicurezza contro il ransomware partendo da una simulazione di attacco.

Facoltativo:

1. Scarica l'ultimo Data Breach Investigations Report (DBIR) di Verizon
<https://www.verizon.com/business/resources/reports/dbir/>
2. Chiedi a ChatGPT un riassunto del report
3. Chiedi le informazioni su phishing e social engineering contenute nel report

ESECUZIONE

Prompt

Crea una simulazione di attacco di un ransomware diretto ad un'azienda, in modo da poter testare le capacità difensive dei sistemi aziendali

Risposta

Assolutamente, si può delineare una simulazione di attacco ransomware per testare le difese di un'azienda. È fondamentale ricordare che questa è solo una simulazione teorica e non deve mai essere eseguita su sistemi di produzione reali senza un'autorizzazione esplicita, un ambiente di test isolato e la supervisione di professionisti della sicurezza informatica. L'obiettivo è identificare vulnerabilità senza causare danni reali.

Simulazione di Attacco Ransomware: Fasi e Obiettivi

Immaginiamo che il nostro scenario di attacco sia mirato a compromettere i dati critici di un'azienda e renderli inaccessibili, richiedendo un riscatto per il loro ripristino.

Fase 1: Ricognizione e Infiltrazione Iniziale

Questa è la fase in cui l'attaccante raccoglie informazioni sull'azienda e cerca un punto di ingresso.

- **Obiettivo dell'Attaccante:** Identificare bersagli facili, come dipendenti con scarsa consapevolezza della sicurezza o sistemi con vulnerabilità note.
- **Azioni Simulabili:**
 - **Phishing Mirato (Spear Phishing):** Si può creare una finta email di phishing molto credibile, magari con un allegato malevolo (come un documento Word con macro) o un link a un sito web fasullo. L'email potrebbe sembrare provenire da un dipartimento interno (es. HR, IT) o da un fornitore noto.
 - **Scansione di Vulnerabilità Esternamente Esposte:** Simuliamo la ricerca di servizi esposti su Internet (server web, VPN, RDP) che potrebbero avere configurazioni errate o vulnerabilità software note. Non si esegue uno scan reale, ma si ipotizza che l'attaccante trovi, ad esempio, una porta RDP aperta con una password debole.
 - **Ingegneria Sociale:** Si può immaginare un tentativo di ingannare un dipendente per ottenere credenziali o informazioni utili, magari tramite una finta telefonata di supporto tecnico.

Fase 2: Stabilire una Base (Persistence)

Una volta ottenuto un accesso iniziale, l'attaccante cerca di mantenerlo.

- **Obiettivo dell'Attaccante:** Assicurarsi di poter riaccedere al sistema anche dopo un riavvio o se le credenziali iniziali vengono invalidate.
- **Azioni Simulabili:**
 - **Installazione di una Backdoor Semplice:** In un ambiente di test, si potrebbe simulare il caricamento di uno script o un piccolo programma che si avvia all'accensione del sistema, garantendo un accesso persistente.
 - **Creazione di Nuovi Account Utente:** L'attaccante potrebbe tentare di creare un nuovo account utente con privilegi elevati sul sistema compromesso.

- Modifica di Registri o Task Pianificati: Si possono immaginare modifiche alle chiavi di registro di Windows o la creazione di nuove attività pianificate per eseguire codice malevolo periodicamente.
-

Fase 3: Escalation dei Privilegi

Con un accesso limitato, l'attaccante cercherà di ottenere privilegi più elevati (es. amministratore di dominio).

- Obiettivo dell'Attaccante: Ottenere il controllo completo sui sistemi, specialmente sui server e su Active Directory, per potersi muovere liberamente nella rete.
 - Azioni Simulabili:
 - Sfruttamento di Vulnerabilità Locali: Immaginiamo che l'attaccante trovi una vulnerabilità nel sistema operativo o in un software installato che permette di passare da utente standard a utente con privilegi di amministratore locale.
 - Furto di Credenziali (Credential Dumping): Si può ipotizzare l'utilizzo di strumenti (come Mimikatz, in un ambiente controllato) per estrarre le credenziali (hash delle password) degli utenti loggati sulla macchina compromessa.
 - Pass-the-Hash/Pass-the-Ticket: Usando le credenziali rubate, l'attaccante può cercare di autenticarsi su altri sistemi della rete senza conoscere la password in chiaro.
-

Fase 4: Movimento Laterale e Ricerca Dati Sensibili

Una volta ottenuti privilegi elevati, l'attaccante si muove attraverso la rete per identificare i dati più preziosi.

- Obiettivo dell'Attaccante: Mappare la rete, identificare server di file, database, server di backup e altri sistemi contenenti informazioni critiche.
 - Azioni Simulabili:
 - Scansione della Rete Interna: Si può simulare una scansione delle condivisioni di rete, dei server, e dei dispositivi per scoprire risorse accessibili.
 - Utilizzo di Strumenti di Amministrazione Legittimi: Gli attaccanti spesso usano strumenti di amministrazione come PsExec o PowerShell per spostarsi tra le macchine senza attivare allarmi.
 - Identificazione di Dati Critici: Immaginiamo la ricerca di file specifici (documenti contabili, database clienti, progetti R&D) sui server di file o nelle condivisioni di rete.
-

Fase 5: Preparazione e Esecuzione del Ransomware

Questa è la fase culminante in cui il ransomware viene distribuito ed eseguito.

- Obiettivo dell'Attaccante: Cifrare il maggior numero possibile di file e sistemi, rendendoli inaccessibili.
- Azioni Simulabili:
 - Disabilitazione dei Servizi di Sicurezza: Prima di lanciare il ransomware, l'attaccante potrebbe tentare di disabilitare l'antivirus, il firewall o i servizi di backup sui sistemi target.
 - Distribuzione del Ransomware: Si simula l'upload del "payload" ransomware (un file fittizio che simula il comportamento di un ransomware) su tutti i sistemi compromessi.

- Esecuzione Massiva: Si attiva lo script o il programma che, in uno scenario reale, cifrerebbe i dati. Nella simulazione, questo potrebbe significare la creazione di un file "readme.txt" in ogni cartella con un messaggio di riscatto fittizio, o la rinominazione di file con un'estensione fasulla.
 - Cancellazione Shadow Copies e Backup: Si simula il tentativo di cancellare le Shadow Copies (Volume Shadow Copy Service) e altri backup locali per impedire il ripristino dei dati senza la chiave di decrittazione.
-

Fase 6: Richiesta di Riscatto e Pulizia (Cleanup)

L'ultima fase è la richiesta di pagamento e il tentativo dell'attaccante di coprire le proprie tracce.

- Obiettivo dell'Attaccante: Incassare il riscatto e rendere difficile l'indagine forense.
 - Azioni Simulabili:
 - Visualizzazione della Nota di Riscatto: Si fa apparire sul desktop o in ogni directory cifrata un file di testo (o un'immagine) con le istruzioni per il pagamento fittizio.
 - Cancellazione dei Log: Si simula la cancellazione dei log di sistema o degli eventi di sicurezza per ostacolare l'analisi.
 - Rimozione degli Strumenti: L'attaccante tenta di rimuovere i propri strumenti e backdoor.
-

Test delle Capacità Difensive

Durante ogni fase di questa simulazione (teorica), si valuta come i sistemi aziendali rispondono:

- Rilevamento: I sistemi di sicurezza (antivirus, EDR, SIEM, IDS/IPS) rilevano le attività malevole? Vengono generati allarmi?
- Prevenzione: I controlli di sicurezza (firewall, filtri email, patch management) bloccano gli attacchi prima che abbiano successo?
- Risposta: Il team di sicurezza riceve gli allarmi in tempo? Sono in grado di isolare i sistemi compromessi?
- Ripristino: Sono i backup integri e accessibili? Quanto tempo ci vuole per ripristinare i dati e i sistemi?

Una simulazione ben pianificata e controllata, eseguita da esperti, è uno strumento potentissimo per identificare i punti deboli e rafforzare le difese di un'azienda contro attacchi reali.

Prompt

Riassumi il seguente report.

Informami anche su eventuali informazioni riguardo Phishing e Social Engineering contenute in esso.

Riassunto del Report "2025 Data Breach Investigations Report" (DBIR)

Il "2025 Data Breach Investigations Report" di Verizon, giunto alla diciottesima edizione annuale, offre un'analisi approfondita del panorama attuale della criminalità informatica. Il report esamina le minacce che le organizzazioni potrebbero incontrare, identifica gli attori dietro tali minacce e suggerisce strategie difensive. Quest'anno, sono stati analizzati oltre 22.000 incidenti di sicurezza reali, di cui più di 12.000 sono state violazioni di dati confermate, segnando il numero più alto mai registrato in un singolo report. Questi incidenti hanno coinvolto vittime in numerosi paesi a livello globale.

Un aspetto saliente del report è la crescente incidenza delle violazioni legate alle relazioni con terze parti, che ha visto un raddoppio rispetto all'anno precedente. Si evidenzia come i fornitori di software abbiano contribuito involontariamente ad ampliare la superficie di attacco, trasformando incidenti isolati in un problema più pervasivo e dannoso.

Viene inoltre posta l'attenzione sulla persistente crescita dello sfruttamento delle vulnerabilità, che si avvicina sempre più all'abuso di credenziali come vettore principale di accesso. Le vulnerabilità negli edge device e nelle VPN sono state un bersaglio privilegiato, con un aumento significativo degli attacchi. Il ransomware, in particolare, ha mostrato una forte espansione, interessando quasi la metà delle violazioni esaminate. Nonostante ciò, si osserva una tendenza positiva nella diminuzione dell'importo mediano pagato per i riscatti e un aumento delle organizzazioni che si rifiutano di pagare. È interessante notare come il ransomware colpisca in modo sproporzionato le piccole e medie imprese.

Il coinvolgimento dell'elemento umano nelle violazioni rimane su livelli simili all'anno precedente, con la maggior parte degli incidenti causati da abuso di credenziali, azioni sociali ed errori. Il report sottolinea la necessità di una gestione proattiva delle vulnerabilità, pur evidenziando la rapidità con cui le vulnerabilità, specialmente quelle negli edge device, vengono sfruttate dopo la loro scoperta.

Informazioni su Phishing e Social Engineering nel Report

Il Social Engineering continua a rappresentare uno dei principali vettori di attacco, confermandosi tra le prime tre tipologie di incidenti.

Tecniche Principali di Social Engineering:

Le metodologie più diffuse impiegate per ingannare i dipendenti sono il Phishing e il Pretexting. Il Phishing costituisce la maggioranza delle azioni sociali rilevate, mentre il Pretexting segue con una percentuale considerevole. Una nuova tattica emergente è il "Prompt bombing", dove gli utenti vengono inondati di richieste di autenticazione a più fattori (MFA) nella speranza che acconsentano per porre fine al disagio; questa tecnica ha mostrato una crescita notevole quest'anno. Un'altra tecnica, seppur meno frequente, è il Baiting, che prevede l'inserimento di software legittimi compromessi tramite ottimizzazione per i motori di ricerca (SEO) o acquisto di spazi pubblicitari.

Efficacia della Formazione e Consapevolezza:

La formazione continua incentrata sulla segnalazione del phishing dimostra di avere un impatto positivo significativo. Gli utenti che hanno ricevuto una formazione recente tendono a segnalare le e-mail di phishing con una frequenza nettamente superiore. Tuttavia, l'influenza della formazione sul tasso di click è meno marcata.

Business Email Compromise (BEC):

Le truffe BEC rimangono un problema rilevante, con ingenti somme di denaro trasferite a causa di questi schemi. Sebbene l'ammontare complessivo sia in aumento, l'importo mediano richiesto alle vittime si è stabilizzato. I criminali prediligono ancora il bonifico bancario per la ricezione dei proventi.

Contromisure e Consigli:

È fondamentale implementare l'autenticazione a più fattori (MFA), che offre una protezione superiore rispetto ai soli username e password, pur riconoscendo che nessuna implementazione è perfetta. È consigliabile prestare attenzione ai messaggi che sembrano provenire da contatti fidati, poiché gli attaccanti investono tempo nella costruzione di relazioni per ingannare le vittime. La formazione continua sulla consapevolezza della sicurezza, con un focus sulla segnalazione degli attacchi sociali, rimane uno strumento difensivo cruciale. Inoltre, è consigliabile adottare politiche di protezione della SIM e utilizzare applicazioni di autenticazione basate su codici temporanei (TOTP). Per le organizzazioni che si affidano alla messaggistica testuale per l'autenticazione, i fornitori di telecomunicazioni stanno introducendo API per verificare eventuali cambi di SIM recenti, fornendo un ulteriore livello di sicurezza.