Sono stato chiamato da un'azienda di nome Epicodesecurity. Il mio ruolo è quello di spiegare e informare i dipendenti sui rischi degli attacchi di phishing.

Stipulo 4 riunioni in cui affrontare il tema:

1. Riunione 1: Introduzione al Phishing

Presentazione del motivo della formazione:

- La formazione sui rischi di attacchi di ingegneria sociale, in particolare contro il phishing, è essenziale per garantire che i dipendenti di Epicodesecurity siano consapevoli e in grado di riconoscere potenziali minacce

Definizione di phishing e illustrazione di esempi comuni:

- Il phishing è una forma di attacco informatico in cui gli aggressori cercano di ottenere informazioni sensibili, come nomi utente, password e dettagli finanziari, impersonando entità fidate. Questo avviene generalmente attraverso comunicazioni fraudolente che sembrano provenire da fonti legittime, come email, messaggi istantanei o siti web falsi. Esempi comuni di phishing possono essere: Email Bancarie Falsificate, Messaggi di Email da Enti Governativi Falsi, Email di Phishing da Provider di Servizi Online, Richieste di Aggiornamento delle Password, Falsi Siti Web di Shopping Online, Email di Phishing sul Luogo di Lavoro (fingendosi ad esempio un superiore).

Rischi associati:

I rischi associati al phishing includono:

- Furto di dati personali: Gli attaccanti cercano di ottenere informazioni come username, password, numeri di carta di credito o altri dati sensibili.
- Accesso non autorizzato: Una volta ottenute le credenziali, gli hacker possono accedere ai conti online delle vittime, compromettendo la loro sicurezza.
- Malware: I link malevoli presenti nei messaggi di phishing possono scaricare malware sui dispositivi delle vittime, causando danni ai dati e al sistema.
- Rischi finanziari: L'accesso ai dati bancari può portare a transazioni non autorizzate e perdite finanziarie per le vittime.
- Furto di identità: Le informazioni ottenute possono essere utilizzate per impersonare la vittima, causando danni alla reputazione e compiendo attività illecite a loro nome.
- Violazione della privacy: Le informazioni personali rubate possono essere utilizzate per ricattare o minacciare la privacy delle vittime.
- Attacchi mirati: Il phishing può essere utilizzato come parte di attacchi più complessi, come il phishing mirato (spear phishing) contro aziende o individui specifici.
- Perdita di credibilità: Le vittime possono perdere fiducia nei servizi online legittimi a causa di esperienze negative associate al phishing.
- Diffusione di minacce: Le informazioni ottenute possono essere utilizzate per ulteriori attacchi, inclusi quelli rivolti agli amici, familiari o colleghi della vittima.

2. Riunione 2: Riconoscimento di Email Phishing:

Identificazione di segnali di avvertimento nelle email phishing:

La prima cosa che si deve analizzare è controllare attentamente l'indirizzo email del mittente. Fare attenzione a piccole variazioni o a indirizzi sospetti che potrebbero sembrare simili a quelli legittimi:

- Esempio: Epicodesegur1ty@semof0rti.com invece di Epicodesecurity@semoforti.com

Verificare attentamente i link presenti nell'email. Passare il mouse sopra di essi **senza cliccare** per vedere l'URL effettivo. Gli URL contraffatti o sospetti possono essere un chiaro segnale di phishing:

- Esempio: "Clicca qui per accedere al tuo account bancario" con un URL che non corrisponde al sito ufficiale della banca.

Inoltre gli attaccanti cercano spesso di indurre le vittime a agire velocemente senza pensare. Essere cauti se l'email crea un senso di emergenza:

- Esempio: "Il tuo account verrà chiuso, a meno che non clicchi sul link e risolvi il problema entro 5 ore."

Le istituzioni legittime non chiedono mai di fornire password o altre informazioni sensibili tramite email. Essere sospettosi di richieste del genere:

- Esempio: "Abbiamo bisogno della tua password per aggiornare il tuo account."

3. Riunione 3: Autenticazione Email

SPF, DKIM e DMARC:

SPF, DKIM e DMARC sono sistemi di difesa che vengono messi nel server che riceve l'email:

- SPF va a controllare l'indirizzo ip e il nome di dominio e vede se può passare. Si impostano dei livelli, che vanno ad identificare la sicurezza dell'indirizzo ip/nome dominio mittente (es: livello 1 molto sicuro, livello 4 non sicuro). Un sito che si può utilizzare per analizzare se gli indirizzi ip di email sospette sono sicuri, è IBM X-Force Exchange.
- DKIM è simile ad una firma digitale, solo che il messaggio, hash del messaggio, la chiave privata e la chiave pubblica sono uniti tra loro. Il server mittente mette la chiave pubblica nell'intestazione dell'email, così il destinatario decripta la chiave privata con il codice hash. Se un "man in the middle" modifca il testo dell'email, il codice hash originario non corrisponderà con il messaggio modificato e non si riuscirà a vedere l'email, non apriremo possibili malware.
- DMARC si può impostare se entrambi SPF e DKIM devono essere ok, o solamente uno dei due.

Notare come questi 3 sistemi di difesa sono efficaci solamente se l'attaccante non è nel nostro dispositivo.

Per vedere dunque se una email che si riceve è affidabile, basta semplicemente cliccare sul comando "<> Mostra originale", e da lì si potrà osservare se l'email ha avuto il "PASS" dal SPF, DKIM e DMARC.

4. Riunione 4: Aggiornamenti Continui e Conclusioni

- Breve riepilogo delle tematiche trattate nelle 3 riunioni precedenti. Sottolineare che le minacce informatiche, compreso il phishing, sono in continua evoluzione, e di conseguenza rimanere informati sugli ultimi sviluppi per adattarsi alle nuove tattiche degli attaccanti è l'ideale.
- Raccomandare piattaforme online dove si può rimanere aggiornati sugli sviluppi in materia di sicurezza informatica.
- Sottolineare come la sicurezza informatica sia una responsabilità condivisa. Ogni individuo ha un ruolo nell'assicurarsi che le pratiche di sicurezza siano eseguite.

Nel caso in cui il direttore dell'azienda ci dia il permesso di un phishing controllato per verificare se i dipendenti ora sono pronti a riconoscere una email di phishing, potremmo:

Creare una pagina web clone della loro pagina web aziendale www.Epicodesecurity.it. Su Kali Linux utilizziamo "Social-Engineer Toolkit", un semplice programma che ci permetterà con pochi e semplici passaggi di generare il clone di ad esempio la pagina di login del sito web aziendale. Come URL mettiamo un indirizzo il più simile possibile a quello originale, ad esempio se quello originale è "www.Epicodesecurity.it/login", il nostro sarà "www.Ep1codes3curIty.it/login". Possiamo inviare una email di phishing ai dipendenti utilizzando un indirizzo email molto simile a quello dell'azienda, ad esempio Epicodesegur1ty@semof0rti.com. Nella email linkiamo il nostro clone della pagina di login del sito web aziendale.

Scriviamo un testo che invogli il dipendente a cliccare sul link ingannevole, come ad esempio:

"*Oggetto: Importante: Variazioni sugli Orari di Lavoro - Azione Richiesta*

Ciao [Nome del Dipendente],

Spero che questa email ti trovi bene. Vorrei informarti di alcune variazioni importanti sugli orari di lavoro che influenzeranno la tua routine lavorativa. Per garantire che tutte le informazioni siano chiare e aggiornate, ti chiediamo gentilmente di verificare gli orari aggiornati sul nostro sito web.

Puoi accedere alle informazioni dettagliate sulle variazioni degli orari di lavoro visitando la pagina dedicata sul nostro sito e accendendo con le tue credenziali al seguente indirizzo:

www.Ep1codes3curIty.it/login

Ti preghiamo di farlo al più presto possibile per evitare eventuali inconvenienti e per assicurarti di essere sempre al corrente degli ultimi aggiornamenti."

Il dipendente cliccherà sul nostro link, digiterà e invierà le sue credenziali su quello che creda sia il sito web dell'azienda. Le credenziali saranno disponibili e utilizzabili da noi, in quanto saranno visibili sul programma "Social-Engineer Toolkit" che avevamo utilizzato per clonare la pagina web.

Di seguito un esempio di come visualizziamo le credenziali su SET: