Traccia

Esercizio di oggi: Siete stati chiamati da un'azienda di nome Epicodesecurity, questa azienda ha un sito web suo personale con il nome di dominio www.Epicodesecurity.it. un server email con l'email aziendale Epicodesecurity@semoforti.com

Il vostro ruolo è quello di spiegare e informare i dipendenti dell'azienda Epicodesecurity sui rischi di attacchi di ingegneria sociale, in particolar modo contro il phishing.

Come impostate la formazione? (spiegare cos'è il phishing).

Cosa devono vedere, in particolar modo, i dipendenti per non cadere nel phishing?(quali parametri vedere per identificarlo.Esempio: SPF).

Il direttore vi da il permesso di creare un phishing controllato.

- - Descrivere come agireste.(Usare dei programmi è opzionale).
- - L'obiettivo è cercare di ingannare le persone nel miglior modo possibile.

Come seguirà la formazione ?

Lunedì ore 8-9 presentazione del nostro team di sicurezza informatica (SecureNet Solutions)

Martedì ore 8 – 10 Introduzione al Phishing ed ingegneria sociale

- Mercoledì ore 8 – 12 Pratica formativa per proteggersi da questi tipi di attacco (**SPF, DKIM, DMARC**)

Giovedì ore 8 – 17 Attacco controllato per sensibilizzare i dipendenti

Lunedi :

Titolo della Presentazione: "Proteggiamo il Futuro Digitale: La Missione di SecureNet Solutions"

Slide 1: Introduzione

- Benvenuti a tutti! Grazie per essere qui oggi.
- Chi siamo: SecureNet Solutions, il vostro partner nella sicurezza informatica.

Slide 2: Panoramica su SecureNet Solutions

- Breve descrizione della nostra azienda e della nostra esperienza.
- Missione: Proteggere le organizzazioni dalle minacce informatiche.

Slide 3: Il Nostro Team di Sicurezza

- Presentazione dei membri chiave del team.
- Esperienza, certificazioni e competenze.

Slide 4: Obiettivi della Presentazione

- Sensibilizzare i dipendenti di EpicodeSecurity sugli attacchi informatici.
- Focus su phishing e ingegneria sociale.

Slide 5: Phishing: Cos'è e Come Riconoscerlo

- Definizione di phishing.
- Esempi di e-mail sospette.
- Consigli su come riconoscere un attacco di phishing.

(martedì)

Slide 6: Ingegneria Sociale: Un Approfondimento

- Spiegazione di cosa sia l'ingegneria sociale.
- Tecniche comuni utilizzate dagli attaccanti.
- Come difendersi dalle tattiche di ingegneria sociale.

(martedì)

Slide 7: Statistiche e Tendenze Attuali

- Dati recenti sugli attacchi informatici.
- Tendenze emergenti nel mondo della cybersecurity.

Slide 8: La Nostra Offerta per EpicodeSecurity

- Breve presentazione dei servizi offerti da SecureNet Solutions.
- Come possiamo collaborare per rafforzare la sicurezza informatica di EpicodeSecurity.

Slide 9: Azioni Consigliate per Tutti i Dipendenti

- Linee guida e best practices per una sicurezza informatica personale.
- Coinvolgimento attivo nella prevenzione degli attacchi.

(giovedì)

Chiusura: Grazie per la Vostra Attenzione

- Riepilogo dell'importanza della sicurezza informatica.
- Contatti di SecureNet Solutions per ulteriori informazioni.

Martedì :

Dalle 8 alle 9:30 i dipendenti di EpicodeSecurity parteciperanno ad una lezione introduttiva sul Phishing ed Ingegneria sociale. In particolare questa sarà la spiegazione trattata :

1. Phishing:

Il phishing è una tecnica di attacco informatico in cui gli aggressori cercano di ottenere informazioni sensibili o indurre le persone a compiere azioni indesiderate, fingendosi di essere una fonte affidabile. Tipicamente, questo avviene attraverso e-mail, messaggi istantanei o siti web contraffatti. Gli attaccanti possono presentarsi come istituzioni finanziarie, fornitori di servizi o anche colleghi di lavoro. L'obiettivo è ingannare le vittime in modo che condividano informazioni sensibili come password, dati finanziari o accesso a sistemi aziendali. Riconoscere le truffe di phishing è essenziale per proteggere i dati aziendali e personali.

2. Ingegneria Sociale:

L'ingegneria sociale è un approccio psicologico utilizzato dagli attaccanti per manipolare le persone al fine di ottenere accesso a informazioni riservate o compiere azioni dannose. Questo può avvenire attraverso la manipolazione emotiva, la creazione di scenari falsi o la sfruttamento della fiducia delle persone. Ad esempio, un attaccante potrebbe fingere di essere un dipendente aziendale o un fornitore legittimo per ottenere informazioni confidenziali. L'ingegneria sociale spesso si combina con altre tecniche, come il phishing, per massimizzare l'efficacia degli attacchi. La consapevolezza e l'educazione delle persone sono fondamentali per prevenire gli attacchi basati sull'ingegneria sociale e proteggere l'azienda da minacce interne ed esterne.

9:30 – 10 Q&A

Mercoledì ore 8 – 12: Pratica Formativa su SPF, DKIM, DMARC per la Sicurezza Aziendale

8:00 - 8:15: Registrazione e Benvenuto

- Breve introduzione alla sessione pratica.
- Importanza della sicurezza aziendale.

8:15 - 8:30: Revisione Rapida di Phishing e Ingegneria Sociale

- Breve ripasso dei concetti di phishing e ingegneria sociale.
- Sottolineare l'importanza di difendersi da queste minacce.

8:30 - 9:00: SPF (Sender Policy Framework) - Che cos'è e Come Funziona

- Definizione di SPF.
- Come SPF protegge da attacchi di spoofing.
- Implementazione di SPF per la propria azienda.

- **Definizione di SPF:** Il Sender Policy Framework (SPF) è uno standard di autenticazione delle e-mail che aiuta a prevenire l'invio di e-mail contraffatte o spoofed. Si basa su un record DNS che specifica quali server sono autorizzati a inviare e-mail a nome del dominio aziendale.
- **Come SPF protegge da attacchi di spoofing:** SPF protegge da attacchi di spoofing fornendo un meccanismo di autenticazione che permette ai server di posta elettronica di verificare che un messaggio provenga da un server autorizzato. Ciò impedisce agli attaccanti di inviare e-mail fraudolente utilizzando il proprio dominio.
- **Implementazione di SPF per la propria azienda:** La sessione coprirà passo-passo l'implementazione di SPF, compresa la creazione del record DNS appropriato. Saranno forniti consigli pratici per garantire una corretta configurazione e mantenere la sicurezza.

9:00 - 9:30: DKIM (DomainKeys Identified Mail) - Approfondimento

- Descrizione di DKIM e del suo ruolo nella sicurezza delle e-mail.
- Firma digitale delle e-mail e verifica dell'autenticità.
- Pratica: Implementare DKIM per la propria infrastruttura aziendale.

- **Descrizione di DKIM e del suo ruolo nella sicurezza delle e-mail:** DKIM è un sistema di firma digitale per le e-mail che consente di verificare l'autenticità del messaggio e l'integrità del suo contenuto. Questo riduce il rischio di manipolazione durante il transito.
- **Firma digitale delle e-mail e verifica dell'autenticità:** La sessione illustrerà come DKIM utilizza chiavi crittografiche per apporre una firma digitale a ciascun messaggio. Sarà

esaminato il processo di verifica che i server di posta elettronica utilizzano per garantire l'autenticità del mittente.
- **Pratica: Implementare DKIM per la propria infrastruttura aziendale:** Un'approfondita guida pratica condurrà i partecipanti nell'implementazione di DKIM per la loro infrastruttura, con esempi pratici e consigli utili.

9:30 - 10:00: DMARC (Domain-based Message Authentication, Reporting, and Conformance) - Una Panoramica

- Spiegazione di DMARC e come si integra con SPF e DKIM.
- Utilizzo di DMARC per rafforzare la sicurezza delle e-mail.
- Esempi di configurazione DMARC.

- **Spiegazione di DMARC e come si integra con SPF e DKIM:** DMARC è un framework che si basa su SPF e DKIM per migliorare ulteriormente l'autenticazione delle e-mail. La sessione fornirà una panoramica completa del suo funzionamento e del suo ruolo nella sicurezza delle e-mail.
- **Utilizzo di DMARC per rafforzare la sicurezza delle e-mail:** Saranno presentati i benefici di DMARC nella prevenzione dell'invio di e-mail spoofed e falsificate, nonché il suo ruolo nel migliorare la consegna delle e-mail legittime.
- **Esempi di configurazione DMARC:** La sessione illustrerà esempi pratici di configurazione DMARC, con indicazioni su come personalizzare i parametri per adattarli alle esigenze aziendali.

10:00 - 10:30: Pausa Caffè e Networking

10:30 - 12:00: Best Practices e Risorse Aggiuntive

- Raccomandazioni per mantenere le configurazioni di sicurezza.
- Risorse online e strumenti utili per la gestione di SPF, DKIM, DMARC.
- Conclusioni e ringraziamenti.

Chiusura: Grazie per la Partecipazione

- Invito a mettere in pratica quanto appreso.
- Informazioni di contatto per ulteriori domande.

Giovedì :

L’obiettivo è ingannare i dipendenti.

La primissima cosa è creare un email con nome fittizio che vada ad ingannare i dipendenti ad esempio support It , la mai deve essere scritta bene e contenere alcuni dati del dipendente per farlo cadere nel tranello, successivamente verrà chiesto all’utente di resettare la sua password una volta resettata il mio sito fittizio avrà questi dati e posso entrare nell’azienda come dipendente.

Warm up finale :

1. ** **Sii Sospettoso: - Sii scettico riguardo alle e-mail, messaggi o chiamate inaspettate che richiedono informazioni personali o finanziarie. - Verifica l'autenticità delle comunicazioni con il mittente attraverso un canale separato, se possibile.

2. ** **Esamina l'Indirizzo e-Mail: - Controlla attentamente l'indirizzo e-mail del mittente. I truffatori spesso utilizzano indirizzi simili a quelli legittimi con piccole variazioni.

3. ** **Non Cliccare su Collegamenti Sospetti: - Evita di cliccare su link o scaricare allegati provenienti da fonti non attendibili o sconosciute. - Passa il mouse sopra i link per visualizzare l'URL effettivo prima di fare clic.

4. ** **Verifica i Siti Web: - Accertati che i siti web che visiti siano sicuri, utilizzando connessioni HTTPS e verificandone l'affidabilità. - Evita di inserire informazioni sensibili su siti web non sicuri.

5. ** **Autenticazione a Due Fattori (2FA): - Abilita l'autenticazione a due fattori quando possibile, specialmente per account sensibili. - Questa aggiunta di sicurezza rende più difficile agli attaccanti ottenere accesso ai tuoi account.

6. ** **Educazione Continua: - Fornisci formazione regolare sui rischi di phishing e ingegneria sociale ai dipendenti. - Mantieni il personale informato sulle ultime minacce e tecniche utilizzate dagli attaccanti.

7. ** **Verifica l'Identità al Telefono: - In caso di richieste di informazioni sensibili via telefono, verifica l'identità della persona chiamante prima di condividere dati personali o aziendali.

8. ** **Aggiorna Software e App: - Mantieni tutti i tuoi software e applicazioni aggiornati per beneficiare delle ultime correzioni di sicurezza. - Utilizza un software antivirus affidabile.

9. ** **Segnala Tentativi di Phishing: - Se ricevi un'e-mail sospetta, segnalala al tuo team IT o al fornitore di servizi e-mail. - Le segnalazioni possono contribuire a migliorare i filtri anti-phishing.

10. ** **Condividi Solo Ciò che è Necessario: - Evita di condividere informazioni personali o aziendali più del necessario. - Limita l'accesso alle informazioni solo a coloro che ne hanno bisogno.