Ingegneria sociale

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.

Epicodesecurity formation

Introduzione:

Come evitare di cadere nei tranelli dei black hat per evitare di compromettere i dati di se stessi e dell'azienda illustrando i rischi dell'ingegneria sociale in un corso di formazione di circa due settimane . Tratteremo principalmente il phishing.

Il Phishing è:

Uno dei più diffusi e pericolosi. Coinvolge messaggi ingannevoli inducendo le persone a rivelare informazioni personali, come nomi utente, password o dati finanziari. Questo attacco sfrutta la fiducia della vittima, convincendola erroneamente che il messaggio provenga da una fonte affidabile o legittima.

Come difendersi?

Per evitare di cadere in questi tranelli bisogna saper distinguere un'email reale da una di phishing. Nel caso in cui vengano richieste informazioni personali, tempestività di accedere usando le proprie credenziali o banalmente il contenuto può risultare ingannevole è sempre il caso di verificare il mittente.

Si possono applicare anche dei filtri specifici per evitare email del genere anche perché spesso possono essere e-mail di carattere spam.

Aggiungere un' autentificazione a più fattori per aver una maggior sicurezza nel caso in cui il black hat tenti l'accesso con le vostre credenziali.

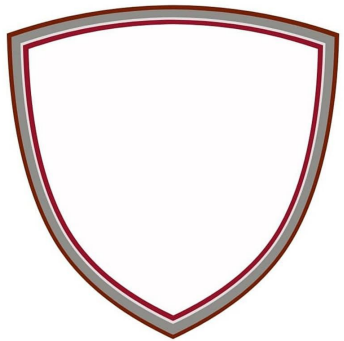
Filtri specifici:

SPF: Sender Policy Framework

DKIM: DomainKeys Identified Mail

DMARC: Domain-based Message Authentication, Reporting, and Conformance

Sono standard di autenticazione e sicurezza utilizzati per mitigare il rischio di spam, phishing ed altro. Svolgono un ruolo specifico nel rafforzare l'autenticazione delle e-mail.



SPF: E' fondamentale per capire il dominio IP da cui proviene l'e-mail per constatare se è davvero chi afferma di essere.

DKIM: E' una chiave digitale creata dal mittente, e il destinatario può verificare l'autenticità utilizzando la chiave pubblica associata.

DMARC: E' un'unione tra SPF e DKIM che contrassegna le e-mail che identifica come spam o altro.

Autorizzazione del direttore:

Se dopo l’autorizzazione il direttore da il permesso di creare un’area di test consapevole (Phishing controllato) si potranno mandare e-mail phishing ai partecipanti del corso per testare se si è compresa la formazione.

Come fare?

L’azienda Epicodesecurity risponde all’e-mail di dominio www.epicodesecurity.it andremo a realizzare qualcosa di simile e copieremo tramite kali il sito grazie a tool set. Imposteremo un indirizzo IP pubblico per far credere all’autenticità dell’e-mail. Manderemo un’email di urgenza ad uno dei dipendenti in cui chiederemo di accedere il prima possibile per risolvere un problema per un mal caricamento del lavoro svolto e che subirà delle penalità aziendali. Se il dipendente darà le credenziali nella e-mail di phishing avremo i suoi dati sensibili ed il nostro primo compito sarà quello di cambiare le credenziali di accesso.