EPICODE

Progetto S3 – L5

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](mailto: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 dà 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.

PROGETTO

Corso di formazione sulla sicurezza informatica per i dipendenti di Epicodesecurity.

Data: 15/12/2023

* 09:00 – Introduzione alla sicurezza informatica
* 09:30 – Ingegneria sociale
* 10:00 – Phishing
* 10:45 – Pausa caffè
* 11:00 – Come riconoscere un attacco di Phishing
* 12:00 – Domande e risposte
* Introduzione alla sicurezza informatica  
  Una breve introduzione in cui si accenna all’importanza della sicurezza informatica e alla protezione dei dati sensibili propri e dell’azienda.
* Ingegneria sociale  
  Spiegare di cosa si tratta e mostrare alcuni esempi.  
  L’ingegneria sociale è una pratica in cui si cercano di ottenere informazioni riservate agendo non sui sistemi informatici, ma sulle persone. Sfruttando la natura umana si manipolano le vittime, le si induce a fare determinate azioni, le si inganna, oppure si sfrutta la fiducia delle vittime per scopi fraudolenti. In questo modo il criminale informatico può ottenere dati sensibili senza dover affrontare le difese delle reti. Proprio per questo motivo è un metodo molto utilizzato e in alcuni casi estremamente pericoloso. Questi attacchi possono essere di vario tipo. Alcuni esempi sono: Phishing (tramite mail), Vishing e Smishing (tramite chiamata / messaggio), Baiting (una trappola come una “curiosa” chiavetta USB con malware), Pretexting (un pretesto per ottenere informazioni, come fingersi un tecnico informatico).
* Phishing  
  Il Phishing è sicuramente uno dei metodi più diffusi. Consiste nel tentativo di rubare dati personali, di accesso o finanziari fingendosi un ente affidabile. Avviene attraverso l’invio di una mail che copia quelle dell’ente di cui la vittima ha fiducia. Cliccando sul link della mail si è già potenzialmente esposti. Spesso poi si finisce su un finto sito che è visivamente identico a quello dell’ente. Se non si hanno le competenze necessarie a riconoscerlo è facile cascarci e rilasciare informazioni sensibili.
* Come riconoscere un attacco di Phishing  
  Per riconoscere un attacco di Phishing è generalmente sufficiente conoscere alcuni semplici ma importanti accorgimenti. Quando si riceve una mail è necessario andare a vedere alcuni parametri. Il primo parametro utile è l’indirizzo del mittente, se è un indirizzo che non corrisponde con il nome dell’azienda o è “strano” è indubbiamente un cattivo indicatore. I due parametri fondamentali che devono necessariamente esserci per poter ritenere una mail sicura sono il SPF e il DKIM. Per i dipendenti è sufficiente sapere che devono guardare il mittente e soprattutto accertarsi di poter vedere questi due parametri.  
  Una breve spiegazione di quest’ultimi.  
  - SPF: verifica che l'indirizzo IP che invia un'email sia autorizzato a farlo per conto del dominio specificato. Il proprietario del dominio specifica nei record DNS quali server sono autorizzati a farlo. Il server destinatario verifica che l'indirizzo IP del server mittente sia elencato come autorizzato.  
  - DKIM: Garantisce l'integrità e l'autenticità del contenuto di un'email mediante la firma digitale. Il mittente firma digitalmente il contenuto dell'email con una chiave privata, e il destinatario può verificare l'autenticità utilizzando la chiave pubblica associata.

Trascorso almeno un mese dal giorno di formazione è utile svolgere, in accordo con il responsabile dell’azienda, un attacco di Phishing controllato (concordato e con danni nulli o gestiti) come test.

L’attacco, per essere più efficace, può considerare diversi fattori. Come, per esempio, il tipo di azienda, le capacità e gli interessi in comune dei dipendenti, i prodotti che vengono venduti, i fornitori. In questa maniera è possibile personalizzare l’attacco per avere il massimo effetto possibile. In un certo senso questo tipo di operazione è simile alle campagne di marketing mirate e al neuromarketing.

Utilizzando un programma come gophish o social engineering toolkit è possibile effettuare questi tipi di attacchi. Con gopish è anche possibile monitorare con un’interfaccia user friendly tutta la situazione in tempo reale (numero di click sul link ecc).

In questo caso il tipo di attacco Phishing che andrei a fare è l’invio di una mail a tutti i dipendenti (con il logo ed i colori di Epicodesecurity) in cui si richiede di cliccare il link per leggere una comunicazione data dai responsabili per quanto riguarda una nuova ed importante comunicazione a livello di taglio del budget sul personale. Probabilmente nell’agitazione di poter perdere il lavoro in molti aprirebbero il link senza controllare nessun parametro.