Progetto S3-L5

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.

Abbiamo detto che L'ingegneria sociale è una forma di manipolazione psicologica in cui gli attaccanti cercano di ottenere informazioni sensibili o indurre le persone a compiere determinate azioni attraverso l'inganno, la manipolazione e l'uso delle relazioni umane. In sostanza, si tratta di sfruttare gli aspetti sociali e psicologici per raggiungere scopi malevoli, come l'accesso non autorizzato a informazioni riservate o sistemi informatici.

La formazione verso i dipendenti :

1. Informare i dipendenti come funziona l’ingegneria sociale che sfrutta la natura umana, le emozioni e le interazioni sociali per ottenere accesso non autorizzato o informazioni sensibili.
2. Mentre le organizzazioni investono in sicurezza informatica avanzata, l'ingegneria sociale si basa più sulla manipolazione psicologica .

Tra i vari attacchi di ingegneria sociale, il phishing è uno dei più diffusi e pericolosi.

1. E-mail o Messaggio Ingannevole:

Gli attaccanti inviano e-mail o messaggi che sembrano provenire da fonti affidabili, come istituzioni finanziarie, servizi online popolari o aziende con cui la vittima potrebbe avere una relazione.

1. Contenuto Ingannevole:

Il contenuto del messaggio spesso contiene elementi ingannevoli, come loghi ufficiali, testi persuasivi o richieste di azioni immediate.

1. Richiesta di Azioni Immediate:

Le vittime vengono sollecitate a compiere azioni immediate, come fare clic su un link, inserire informazioni di accesso o scaricare allegati.

4 – Richiesta di Azioni Immediate:

Le vittime vengono sollecitate a compiere azioni immediate, come fare clic su un link, inserire informazioni di accesso o scaricare allegati.

Quindi il phishing e un azione per ricavare dati per scopo di utilizzo malevole .

Dopo aver informato i dipendenti come funziona l’ingegneria sociale e il phishing , informo loro come possono proteggersi :

1. Verifica delle Fonti:

Le vittime devono verificare attentamente la fonte del messaggio, specialmente quando si tratta di richieste di informazioni sensibili. La verifica può includere contattare direttamente l'azienda o l'organizzazione apparentemente coinvolta.

In questo caso i dipendenti devono controllare il nome domain del mittente il SPF e il DKIM e il DMARC che e subordinato al SPF e il DKIM e si puo utilizzare come un modo di protezione come gli altri due menzionati per proteggersi dal phishing in quanto limitano l’arrivo dei email da fonti indesiderati in quanto dkim e legato al codice privato e pubblico e il codice stesso e integrato alla chiave privata .

Immagine che contiene testo, schermata, ricevuta

Descrizione generata automaticamente

Anche se l’aspetto del email phishing può esser identico ad un email normale cliccando sui tre puntini al latoImmagine che contiene testo, schermata, Sito Web, Pagina Web

Descrizione generata automaticamente

Possiamo vedere :

che non contiene il Pass dal SPF ( il quale e un tipo di firewall che protegge andando a verificare l’ip e il dominio del mittente )

e neanche il pass dal DKIM , in più il nome domain e differente . vedendo queste informazioni i dipendenti possono accertarsi che non e un email fasulla .

Immagine che contiene testo, schermata

Descrizione generata automaticamente

Per esseguire una phishing utilizziamo il programma gophish il quale ci permette di creare un email template copiando l’email originale , poi ci permette di importare il landing page [www.Epicodesecurity.it](http://www.Epicodesecurity.it). Creando un dominio .com del azienda .

Poi modifichiamo il landing profile facendolo piu indentico al [Epicodesecurity@semoforti.com](mailto:Epicodesecurity@semoforti.com)

Poi creamo la nuova campagnia e vediamo chi vede l’email e chi clicca sul link siccome il proggrama ci permette di monitorare tutto in tempo reale .