S3/L5

Traccia:

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.

Programma del giorno in data 15/12: corso di formazione presso Epicodesecurity.

Oggetto e strutturazione del corso:

* 9.00 -10.00 Presentazione, introduzione e spiegazione su cosa è l’ingegneria sociale.
* 10.00 -11.00 Quali sono gli attacchi più diffusi dell’ingegneria sociale.
* 11.00 -12.00 Come capire se siamo stati attaccati e le regole da sapere.
* 12.00 -13.00 Conclusioni e Q&A con i dipendenti.

9.00 – 10.00

L’ingegneria sociale è una pratica che coinvolge la manipolazione psicologica delle persone fisiche al fine di ottenere informazioni riservate, dati sensibili per l’accesso ai dati personali e sistemi informatici. Nella sicurezza informatica consiste nell’utilizzo da parte degli hacker informatici o meglio definiti come black hat, di metodi che hanno lo scopo di ottenere informazioni tramite l’inganno, sfruttando per esempio la fiducia, o più spesso la mancanza di attenzione da parte delle persone. Importante ricordare che in primis è un attacco alla persona e non al sistema informatico in sé.

10.00 – 11.00

L’ingegneria sociale presenta al suo interno delle sottocategorie di attacchi informatici.

Uno degli attacchi più diffusi in assoluto è il phishing.

Il phishing è dunque una forma di attacco che mira ad ottenere informazioni personali, come nomi utente, password e dettagli finanziari attraverso l’invio di e-mail malevole.

L’e-mail, solo apparentemente proviene da istituti finanziari (banche o società emittenti di carte di credito) o da siti web che richiedono l'accesso previa registrazione (web-mail, e-commerce ecc.). Solitamente nel messaggio, per rassicurare l'utente è indicato un collegamento (link) che rimanda  apparentemente al sito web dell'istituto di credito o del servizio a cui si è registrati; in realtà è una pagina web contraffatta uguale all’originale. Qualora l'utente inserisce i propri dati riservati, questi saranno a disposizione dei criminali informatici. E’ importante ricordare che gli attacchi possono provenire non solo da fonti come istituti o servizi online, ma possono far finta di provenire anche da colleghi, per cui in ambito aziendale anche su questo punto risulta fondamentale non farsi influenzare dalla sfera emotiva e personale della persona.

Un’altra sottocategoria di attacchi riguardanti l’ingegneria sociale è lo smishing, derivante da sms + phishing. Per cui come possiamo intuire, in questo caso l’attacco riguarda l’invio di messaggi di testo fraudolenti da parte dei criminali sempre con lo scopo di ottenere informazioni personali o finanziarie, ingannando la persona. Un esempio di smishing può riguardare l’invio di sms su smartphone da parte di un corriere per la spedizione di un pacco fermo in dogana e che si richiede l’importo da pagare per sdoganarlo; oppure la verifica (tramite username e password) dell’account bancario per un accesso non autorizzato.

Infine, un’altra allarmante tecnica di ingegneria sociale in aumento è il quishing. Ovvero, una tecnica di phishing che sfrutta i QR code i quali una volta scansionati, scaricano malware o reindirizzano le vittime su siti web malevoli.

11.00 – 12.00

Passiamo ora alla parte più importante del corso di formazione, ovvero come capire se stiamo subendo un attacco phishing.

Quali sono i parametri che io dipendente posso verificare se l’email è malevola o meno?

Per prima cosa, è sempre buono non cliccare mai direttamente su un link o qualsiasi cosa richieda il corpo dell’email ma, cliccare su “mostra originale” . Il messaggio originale ci darà una tabella con delle informazioni molto importanti: ID del messaggio, la data in cui è stato creato e di seguito 4 informazioni che rappresentano il sistema di difesa per riconoscere un phishing nel server che riceve l’email:

* l’indirizzo email del mittente, se corrisponde o meno al sito o alla casella di posta elettronica
* SPF, (sender policy framework), è una riga di codice informatico nella quale l’utente ricevente dell’email può verificare l’IP del mittente. Infatti, altro non è che una lista di indirizzi IP e istruzioni che i provider di servizi internet devono seguire nel gestire il traffico email. L’SPF fornisce quindi un primo livello di protezione e per essere sicuro di fianco deve esserci scritto ‘PASS’. SPF funziona attraverso dei livelli di rischio, più si abbassa la soglia del rischio, più sarà sicuro. Per controllare questa soglia, possiamo copiare l’IP mittente nella barra di ricerca di un database (per esempio exchange.xforce.ibmcloud.com) il quale ci mostra il livello di rischio associato a quell’indirizzo IP; se è 1 sarà molto sicuro. Tuttavia, si può facilmente “ingannare” questo primo step di verifica tramite un proxy.
* DKIM, (domain keys identified mail), è una sorta di firma digitale, essenzialmente uno standard di autenticazione delle email progettato per verificare l’autenticità del messaggio, protegge dunque dagli attacchi alle modifiche di email, iban ecc… Anche in questo caso la cosa essenziale per noi è verificare che vi sia scritto ‘PASS’ nel messaggio originale.

Come funziona? Il server di posta del mittente firma il messaggio con una chiave crittografata privata, incorporata nel messaggio. Il server email ricevente esegue una ricerca nel DNS per verificare la chiave pubblica, se il server trova la chiave di DKIM pubblica la apre e se la firma nel messaggio corrisponde alla firma pubblicata nel DNS, il server e-mail ricevente considera valido il messaggio, in caso contrario il messaggio può non raggiungere la casella di posta elettronica o finire nello spam. In sintesi, ora abbiamo due step di verifica perché anche se l’attaccante cambia l’IP di conseguenza aumenterà il “rischio” e torniamo all’SPF che la blocca.

* DMARC, fornisce un terzo livello di protezione dopo SPD e DKIM. Il DMARC consente di comunicare al tuo provider di servizi email se rifiutare l’email da fonti sconosciute in base alle informazioni ricevute dai primi due step. Per cui permette ai proprietari dei domini di definire le politiche su come devono essere gestite l’email se non superano le verifiche di autenticazione. Anche in questo caso, verifichiamo che vi sia scritto ‘PASS’.

12.00 – 13.00

In conclusione, è di fondamentale importanza ad oggi saper riconoscere se siamo sotto attacco di phishing. Quali parametri bisogna verificare?

1. Non aprire e cliccare sull’email che arriva nella casella di posta elettronica
2. Cliccare su “mostra messaggio originale” di solito nella barra di ricerca a destra del messaggio
3. Verificare che:

DA = indirizzo mittente, deve corrispondere il nome del dominio

SPF (verifica indirizzo IP/nome dominio) = PASS

DKIM (verifica firma digitale) = PASS

DMARC (politiche di consegna dei messaggi) = PASS

Finito il corso di formazione, il direttore dell’azienda ci autorizza ad effettuare un attacco di phishing controllato a distanza di 6 giorni. Quindi come abbiamo specificato:

* data del corso di formazione 15/12
* data dell’attacco 21/12

Di solito è sempre meglio aspettare minimo un mese per effettuare l’attacco, in questo caso però abbiamo optato per un lasso di tempo breve in quanto la nostra campagna di phishing si basa sull’invio di un’email fraudolenta da parte di [Epicodesecurity@semoforti.com](mailto:Epicodesecurity@semoforti.com) in cui si chiederà al team di Epicode di rispondere all’email per voler partecipare o meno alla cena aziendale prima di Natale. [Epicodesecurity@semoforti.com](mailto:Epicodesecurity@semoforti.com) è l’email aziendale, dove per l’appunto la posta elettronica passerà per il server di Epicode con IP pubblico dove al suo interno vi è un programma che gestisce la posta sul server web e dove si imposta il livello di sicurezza del SPF.

Tramite un tool open source, in questo caso GoPhish, è possibile simulare una campagna di attacco phishing. Consente l'invio di email fraudolente, la creazione della landing page e il monitoraggio della campagna.

Obiettivo della campagna: cercare di ingannare i dipendenti di Epicodesecurity portandoli a cliccare, tramite l’invio di email malevola, sul sito clonato di www.Epicodesecurity.it

Oggetto: invito alla cena aziendale di Natale

Cari colleghi,

Con grande gioia vi scrivo per annunciare l’organizzazione della nostra cena aziendale di Natale.

Data: 22/12

Ora: 20.00

Luogo: Palazzo Brancaccio, Viale del Monte Oppio, 7, 00184 Roma RM

La cena sarà un’occasione per condividere momenti di allegria e rafforzare i legami tra i membri del team. Per rendere la serata ancora più speciale abbiamo organizzato un menù delizioso, se avete restrizioni alimentari o particolari esigenze vi preghiamo di comunicarcele in modo di garantire che la serata sia piacevole per tutti. Per confermare la vostra partecipazione vi chiediamo gentilmente di rispondere a questa e-mail cliccando sul sito qui sotto.

www.Epicodesecurity.it

Vi aspettiamo numerosi,

Cordiali saluti

Tramite GoPhish sulla sezione “email template” inseriamo il codice html, css della rispettiva email, ovviamente il dominio dell’email non sarà uguale a [Epicodesecurity@semoforti.com](mailto:Epicodesecurity@semoforti.com) ma possibilmente sarà simile in modo tale da ingannare più facilmente. Nella sezione “landing page” copiamo l’URL della vera pagina di Epicode presa da internet, la importiamo ed abbiamo clonato il sito. Settiamo il nostro server su “sending profile” per il lancio della nostra campagna ed una volta cliccato su campaign🡪 new campaign 🡪 view results, abbiamo una schermata in cui vedremo la nostra timeline dell’attacco di phishing:

* Orario della campagna creata,
* L’invio dell’email fraudolenta,
* Quante volte è stata aperta l’email,
* Quante volte è stato cliccato e aperto il link del sito clonato

Sara Spaccialbelli