CORSO INTRODUTTIVO SULLE MISURE DI PREVENZIONE CONTRO IL PHISHING

Corso ideato Da Lorenzo Mazzoni in collaborazione con l'azienda "EpicodeSecurity", per aiutare, istruire e mettere in guardia, i suoi dipendenti su uno degli attacchi informatici più usati al mondo il "Phishing". "Il direttore presta il suo consenso affinché lo svolgimento del corso si possa attuare, dichiarando di essere consapevole delle misure e del controllo effettuato alla fine del corso che andrà a valutare e a verificare se i dipendenti hanno appreso e compreso appieno le basi per prevenire questo tipo di attacco nel miglior modo possibile nei limiti delle loro conoscenze".

1) Cosa è il Phishing;
2) Cosa devono vedere ed analizzare in una finta e-mail affinché evitino di cadere in un tranello;
3) Come difendersi;
4) Test per la verifica dei concetti e delle soluzioni analizzate durante il percorso.

Questo percorso si svolgerà nell'arco di una settimana, le lezioni guida ci saranno il lunedì, mercoledì e sabato e ogni lezione guida sarà della durata di due ore.

Prima lezione:

1) Cos'è il Phishing:

Il phishing è una tecnica, che permette di penetrare un sistema informatico, sfruttando l'ingegneria sociale ovvero, 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. I malintenzionati possono così aver accesso a qualsiasi tipo di informazione riguardante l'azienda e tutto il personale. Si avvalgono quasi sempre di e-mail finte, generate da software informatici che riescono a riprodurre (molto spesso), in modo impeccabile, la forma e il contenuto dell'e-mail stessa. Possono chiedere di inserire credenziali (ad esempio per banche, posta o altri enti o istituzioni), o possono chiedere di cliccare su link che permetteranno all'utente malintenzionato di avere il controllo e l'accesso del dispositivo "vittima", nelle aziende potrebbero simulare un'e-mail inviata da un collega che per accedere a dei file di lavoro chiederanno di cliccare su quel link o richiederanno delle informazioni sensibili sull'azienda stessa.

2) Cosa devono vedere ed analizzare in una finta e-mail affinché si eviti di cadere in un tranello

Le e-mail generate in modo ingannevole lasciano tracce anche se poco visibili dagli utenti meno esperti, molte volte invece di esserci scritto ad esempio www.Poste...", ci saranno una serie di numeri come 172.168.0... questo è un codice identificativo chiamato indirizzo IP, utilizzato da tutti noi per navigare su Internet, le grandi istituzioni hanno sempre un dome dominio ovvero "www.poste...", in caso anche loro utilizzassero un nome dominio controllare bene il nome avrà imprecisioni nella scrittura esempio "www.postre...".

3) Come difendersi?

Si può utilizzare l'autenticazione multifattore, anche se le credenziali vengono compromesse (credenziali intese come nome utente e password), colui che attaccherà avrà bisogno di altri dati per accedere come un codice aggiuntivo o la risposta a una o più domande, personali che normalmente solo l'utente legittimato dovrebbe conoscere. Ci sono anche dei parametri nelle e-mail su cui bisogna concentrarsi per verificarne l'autenticità e questi sono:

● SPF (Sender Policy Framework): verifica che quell'indirizzo IP sia autorizzato a inviare quell'e-mail;

● DKIM (DomainKeys Identified Mail): verifica l'autenticità e l'integrità del contenuto dell'e-mail tramite quella che viene chiamata "Firma Digitale", però per questo ci vorrà una chiave privata utilizzata dal mittente e una pubblica utilizzata dal destinatario per verificarne l'autenticità. (La firma è memorizzata nell'Header dell'e-mail);

● DMARC (Domain-based Message Authentication, Reporting, and Conformance): questo parametro richiede che gli altri due siano stati autenticati per verificarne la sicurezza, questo valuterà le e-mail come spam, o può direttamente rifiutarle.

4) Test per la verifica dei concetti e delle soluzioni analizzate durante il percorso.

Passato un periodo di tempo non dichiarato (un mese, un mese e mezzo), si effettueranno dei test, sui dipendenti. Verrà utilizzato un programma come Gophish, che ricreerà delle e-mail fatte su misura per trarre in inganno i dipendenti, ad esempio utilizzando un'e-mail di sondaggi sui lavoratori dell'azienda (accordandosi con il titolare), o un'e-mail sulle proposte innovative che vorrebbero esporre all'azienda in modo anonimo. Se si volesse utilizzare qualcosa di più accattivante, si potrebbe sfruttare il tempo, la fretta, la

confusione e il sangue freddo inviando e-mail, di imminente pericolo di furto dati richiedendo di cliccare, link malevoli o inserimento di dati sensibili.