Come riconoscere le minacce online: Ingegneria sociale, Phishing e Spear Phishing

Consapevolezza, la prima fase della sicurezza.

Cari Colleghi,

L'implementazione di nuovi sistemi informatici e tecnologie all'avanguardia all'interno dei nostri processi aziendali, in mano a malintenzionati, potrebbero essere utilizzati per **commettere atti illeciti** e frodi informatiche.
In questa quarta Newsletter vogliamo affrontare **il tema dell'utilizzo della tecnologia a fini malevoli**. Ci riferiamo alle tecniche sociali utilizzate per esfiltrare informazioni tramite attacchi informatici che hanno come **vittima i dipendenti aziendali**. Dunque, riportiamo di seguito le più comuni.

L'ingegneria sociale

Il Social engineering è **un'arte di manipolazione psicologica** utilizzata dai criminali informatici per ottenere informazioni riservate, accesso a sistemi informatici o **persuadere le persone a compiere azioni contro la propria volontà**. Questa tecnica sfrutta la fiducia delle persone e la loro propensione a rispondere a richieste di aiuto, autorità o premi. I metodi di Social engineering possono essere sia online che offline e possono coinvolgere una serie di tattiche psicologiche sofisticate. Ecco alcuni dei principali metodi utilizzati:

- **Phishing e Spear Phishing**: alcune delle forme più comuni di Ingegneria sociale sono il phishing e lo Spear phishing. Ad esempio, i criminali informatici possono inviare e-mail o messaggi fraudolenti che sembrano provenire da fonti attendibili, come banche, aziende o istituzioni governative. Verranno affrontati più avanti in maniera specifica.

- **Messaggi "esca"**: i malintenzionati possono inviare messaggi, e-mail ecc. con pretesti convincenti per ottenere la fiducia delle vittime. Ad esempio, possono fingersi tecnici IT richiedendo l'accesso da remoto al computer del dipendente per risolvere un problema tecnico inesistente.

- **Autorità falsa**: i criminali informatici si fingono rappresentanti di autorità o istituzioni autorevoli, come polizia o banche, per ottenere la fiducia delle vittime e convincerle a condividere informazioni sensibili o compiere azioni dannose.

Ingegneria sociale offline: il Social engineering può avvenire anche offline, tramite telefonate o incontri di persona. I malintenzionati possono fingere di essere dipendenti di un nostro fornitore esterno per ottenere informazioni riservate o accesso fisico ai sistemi informatici.

Manipolazione emotiva: i criminali informatici sfruttano le emozioni umane, come la paura, l'avidità o la curiosità, per manipolare le persone. Ad esempio, possono minacciare sanzioni legali o finanziarie per indurre le vittime a compiere azioni contro la propria volontà.

La consapevolezza e l'istruzione sui rischi dell'Ingegneria sociale possono garantire una maggiore protezione da tali attacchi. Riportiamo di seguito alcuni consigli:

Essere cauti con le informazioni personali: evitate di condividere informazioni sensibili, come nomi utente, password o dettagli personali, con persone sconosciute o non autorizzate. Prima di fornire qualsiasi informazione, è importante verificare l'identità del richiedente e la legittimità della richiesta.

Verificare l'identità: prima di rispondere a richieste di informazioni o compiere azioni, verificate attentamente l'identità della persona che le richiede. Chiedete dettagli aggiuntivi o contattate direttamente l'organizzazione o l'individuo tramite canali affidabili per confermare l'autenticità della richiesta.

Essere consapevoli delle tattiche di manipolazione: essere consapevoli delle tattiche comuni utilizzate dai malintenzionati (es. l'inganno psicologico, l'uso di autorità fittizie e la manipolazione emotiva) può aiutarci a rimanere vigili di fronte a richieste sospette o comportamenti inusuali.

Segnalare comportamenti sospetti: se si sospetta di essere vittime di un tentativo di Social engineering o si osservano comportamenti sospetti da parte dei colleghi, è importante segnalarlo immediatamente. Questo ci può aiutare a prevenire potenziali attacchi e proteggere la Regione.

Dunque, come anticipato, vedremo di seguito **le due tecniche più utilizzate** dai malintenzionati per esfiltrare informazioni direttamente ai dipendenti aziendali: Phishing e Spear phishing.

Il Phishing

Il phishing rappresenta una minaccia per la sicurezza informatica delle aziende e dei loro dipendenti. Gli attacchi di phishing vengono solitamente effettuati attraverso e-mail che sembrano provenire da fonti affidabili e sono progettate con loghi, testo e link che sembrano provenire da vere società. Tuttavia, i link portano spesso a siti web falsi o compromessi che **cercano di raccogliere informazioni personali**. Questi siti web **possono anche contenere malware** che possono infettare il sistema. Ecco come funziona tipicamente un attacco di phishing:

I criminali informatici **inviano e-mail, messaggi di testo o messaggi su social media** che sembrano provenire da fonti affidabili;

Il messaggio di phishing solitamente **contiene un pretesto convincente per indurre la vittima a compiere un'azione**, come cliccare su un link, scaricare un allegato o inserire informazioni personali su un sito web contraffatto;

I link presenti nel messaggio di phishing **ci indirizzano a un sito web contraffatto**. Questi siti spesso richiedono di inserire informazioni sensibili, come nome utente e password, o installano, all'insaputa dell'utente, malware sul dispositivo;

Una volta che abbiamo inserito le nostre informazioni sensibili sul sito web contraffatto, i criminali le catturano e **le utilizzano per scopi dannosi**, come frodi finanziarie, furto di identità o accesso non autorizzato ai sistemi informatici.

È importante saper riconoscere ed evitare gli attacchi di phishing, adottando pratiche di sicurezza come la verifica degli URL prima di cliccare sui link, l'attenzione **agli errori di ortografia e grammatica** nei messaggi, la correttezza dell'indirizzo e-mail e la consultazione diretta delle fonti affidabili in caso di dubbi sulla legittimità del messaggio. **La formazione e la consapevolezza sono fondamentali** per proteggere le nostre informazioni sensibili dai rischi legati al phishing.

Lo Spear phishing

Lo Spear phishing è **una forma mirata di phishing**, in cui i malintenzionati **personalizzano gli attacchi per adattarli alle caratteristiche specifiche delle vittime**. A differenza del phishing classico, che mira a un vasto pubblico inviando messaggi generici, lo Spear phishing prende di mira individui specifici o gruppi ristretti di persone. I malintenzionati **conducono una ricerca dettagliata sulle vittime**, raccogliendo informazioni personali e professionali da fonti pubbliche online, che vengono poi utilizzate per creare messaggi di phishing altamente credibili e specifici.
Dunque, lo Spear phishing ha come obiettivo quello di ottenere accesso anche a **informazioni aziendali riservate**, per compromettere la sicurezza dei sistemi informatici o rubare dati sensibili da bersagli selezionati.

I criminali informatici **impiegano tempo e risorse per identificare le vittime**. Una volta individuate, personalizzano i messaggi di phishing in base alle informazioni raccolte. Questo può includere l'utilizzo di nomi, **titoli di lavoro, informazioni sul settore e relazioni professionali** per rendere i messaggi più credibili e convincenti. I malintenzionati sfruttano informazioni specifiche sulle attività e gli interessi delle vittime, ad esempio, inviando un'e-mail falsificata a un dipendente facendosi passare per un collega o un superiore, chiedendo di condividere informazioni riservate o di eseguire azioni dannose. Spesso **sfruttano tecniche sofisticate di ingegneria sociale per manipolare le vittime** e indurle a compiere azioni contro la propria volontà come l'urgenza o la paura per convincere le vittime ad agire senza pensare.

Come di consueto, alcuni consigli possono aiutarci a identificare gli attacchi e non caderne vittima:

Prima di agire su un'e-mail, è importante **esaminare attentamente il contenuto** e le richieste presenti. Se l'e-mail sembra sospetta o richiede azioni insolite, come fornire informazioni personali o scaricare file allegati, è meglio **essere prudenti** e non agire di impulso.

I malintenzionati cercano di indurre le vittime a compiere azioni immediate e irrazionali utilizzando toni urgenti o minacciosi nelle e-mail. In caso di richieste di azioni urgenti, è meglio **prendersi del tempo** per valutare attentamente la situazione e verificare l'autenticità della richiesta.

La maggior parte dei nostri sistemi informatici implementano nativamente **soluzioni di filtraggio e-mail avanzate** in grado di rilevare e bloccare automaticamente messaggi di phishing e altri attacchi informatici prima che raggiungano le caselle di posta. Verificate che siano attive sulla vostra casella mail.

La sicurezza informatica è una **responsabilità condivisa** e ogni azione che intraprendiamo per proteggere i nostri dati e i nostri sistemi **contribuisce a rafforzare la sicurezza dell'intera Regione**. La nostra sicurezza informatica **dipende** non solo dalle misure tecniche adottate, ma anche **dalla nostra consapevolezza** e prontezza nel riconoscere e rispondere alle potenziali minacce. Pertanto, vi incoraggiamo ad attuare i suggerimenti e le strategie condivise in questa Newsletter e ad applicarli nella vostra vita lavorativa quotidiana.
Grazie per il vostro impegno e la vostra attenzione su questo importante tema**.**
Insieme possiamo fare la differenza nel mantenere un ambiente di lavoro sicuro e protetto.

Saluti,
Settore "Infrastrutture Digitali e Sicurezza",
Responsabile Protezione Dati,
Ufficio Privacy Regione Calabria.