CONSEGNA [SETTIMANA 3 LEZIONE 5]
Ingegneria sociale

PREFAZIONE

Sono stato contattato da un'azienda chiamata **Epicodesecurity**, questa azienda possiede un sito web personale con dominio *www.epicodesecurity.it* e un server mail con mail aziendale *epicodesecurity@semoforti.com*

OBBIETTIVI

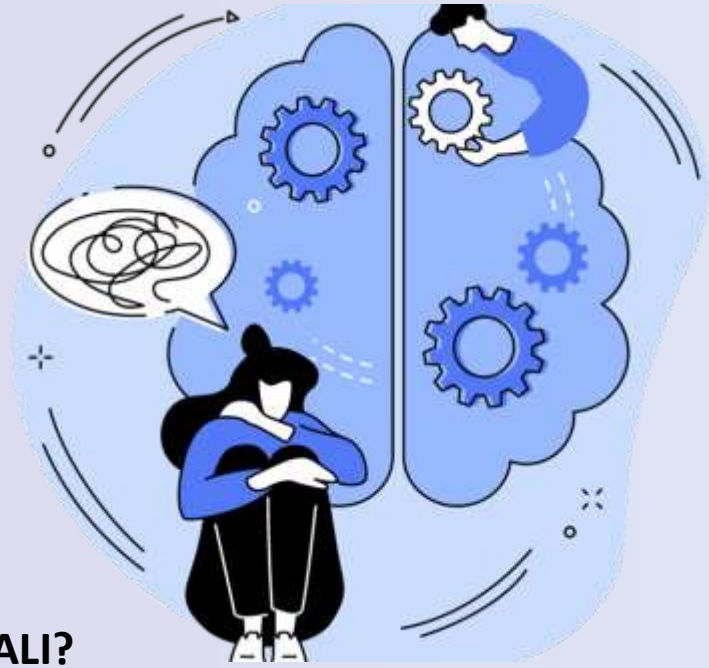
- Informare i dipendenti dell'azienda riguardo i rischi di attacchi di ingegneria sociale, in particolar modo il phishing
- Evidenziare quali sono i parametri da valutare per non cadere vittime di questi attacchi
- Eseguire un phishing controllato

STRUTTURA DEL CORSO

- Ore 8:20 – 9:00 | Introduzione alla ingegneria sociale
- Ore 9:00 – 9:30 | Attacchi di phishing
- Ore 9:30 – 9:45 | Accenni agli attacchi di smishing e quishing

CONSEGNA [SETTIMANA 3 LEZIONE 5]
Ingegneria sociale

COSA SI INTENDE PER INGEGNERIA SOCIALE



Con *ingegneria sociale* facciamo riferimento ad una forma di **manipolazione psicologica**, con la quale un ipotetico malintezionato cerca di ottenere **informazioni private** oppure cerca di condurre il malcapitato a compiere certe azioni che si potrebbero rivelare dannose per sè stesso o l'azienda a cui fa fede.

In pratica, l'ingegneria sociale è uno strumento che viene sfruttato per ottenere risultati malevoli, come **l'accesso a credenziali riservate** o, in molti casi, **interi sistemi informatici**, causando così un grande **problema di sicurezza informatica.**

QUALI SONO LE CARATTERISTICHE PRINCIPALI?

- ***Sfruttamento dell'ingenuità dell'essere umano e della sua fiducia***
  Un attacco di ingegneria sociale tende a far leva su situazioni in cui il malcapitato si sente al sicuro, non sospettando di un potenziale danno a sua insaputa.

- ***Polimorfismo degli attacchi***
  Un attacco di ingegneria sociale può essere modulato in base al contesto in cui si trova e alla persona che viene attaccata.

- ***Mancanza di istruzione per dipendenti e aziende***
  Spesso molte persone non sono a conoscenza dei principali metodi di attacco e come riconoscerli, sarebbe opportune quindi una formazione a riguardo per non cadere vittima di tali processi ed evitare danni a sè stessi e all'azienda.

I PRINCIPALI ATTACCHI DI INGEGNERIA SOCIALE

IL PHISING

Uno degli attacchi di ingegneria sociale più utilizzati e pericolosi è il **phishing**, ovvero l'invio di e-mail a scopo malevolo che cercano di recuperare, tramite la manipolazione, informazioni riservate come **nome utente, password o altri dati di natura personale**.

Questo tipo di attacco, come molti altri, si basa **sull'ingenuità della persona coinvolta e sulla sua fiducia**, dando l'idea che il messaggio arrivi da **fonti sicure e verificate** (un esempio può essere una mail di phishing che simula una conferma da parte di un servizio di spedizioni o un servizio di acquisti online, ma anche provenienti da fonti come poste, banche, servizi di telefonia e molto altro).

Si può notare in queste mail malevole una specie di pattern che viene ripetuto per ottenere informazioni personali come:

- Sussistenza di un problema legato ad un account / ordine / problema informatico
- Richiesta di una azione immediata per risolvere tale problema
- Inserimento di informazioni sensibili come nome utente e password

COME POSSIAMO DIFENDERCI?

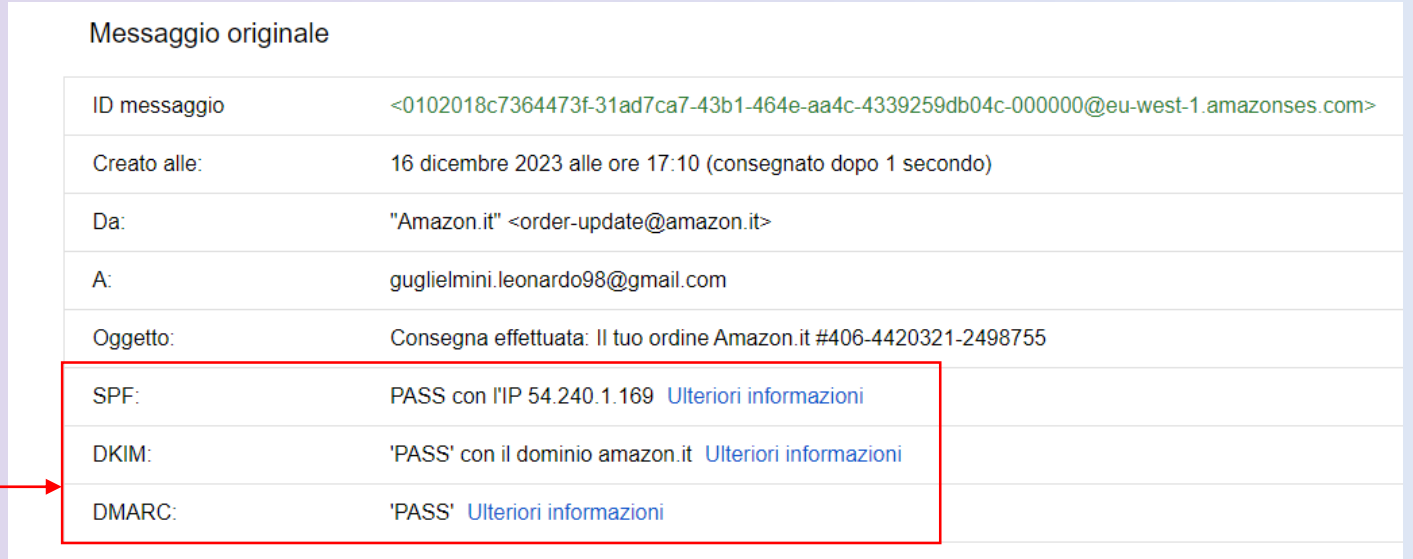
Sono molti i metodi che possiamo usare per difenderci da tali minacce, di seguito ne elenchiamo alcuni di essi:

- ***Istruzione riguardo gli attacchi***, tramite corsi di formazione ed eventualmente di aggiornamento tenuti da professionisti del settore
- ***Autenticazione a fattori multipli***, ovvero una seconda difesa nel caso vengano compromesse le credenziali di accesso (ad esempio l'utilizzo di un codice OTP – one time password- che si riceve sul proprio telefono).
- ***Verifica dell'autenticità della fonte*** tramite SPF, DKIM e DMARC

COME RICONOSCERE LE E-MAIL DI PHISHING

Come accennato prima è possibile in alcuni casi, prestando attenzione, riconoscere le e-mail di phishing, ma come?
Inanzitutto occorre controllare **l'indirizzo email del mittente**, spesso e-mail di phising hanno un indirizzo molto simile ma non uguale a quello originale (ad esempio una mail di phising apparentemente proveniente dalle poste italiane potrebbe avere lettere doppie nel suo indirizzo – posteiitaliane.it).
Esistono inoltre tre fattori che si possono verificare per accertarsi dell'autenticità della e-mail, non ci addentreremo nel loro concreto utilizzo o nel funzionamento, ma è indispensabile sapere dove si trovano questi fattori e cosa identificano.

- **SPF (Sender Policy Framework)**
  Certifica che l'indirizzo IP del mittente sia autorizzato ad inviare una mail per conto del dominio specificato
- **DKIM (DomanKeys Identified Mail)**
  Garantisce l'autenticità del contenuto della mail tramite firma digitale
- **DMARC (Domain-based Message Authentication, Reporting and Conformance)**
  Fornisce un meccanismo per l'autenticazione delle mail e specifica come email non autenticate devono essere gestite


Messaggio originale

ID messaggio	<0102018c7364473f-31ad7ca7-43b1-464e-aa4c-4339259db04c-000000@eu-west-1.amazonses.com>
Creato alle:	16 dicembre 2023 alle ore 17:10 (consegnato dopo 1 secondo)
Da:	"Amazon.it" <order-update@amazon.it>
A:	guglielmini.leonardo98@gmail.com
Oggetto:	Consegna effettuata: Il tuo ordine Amazon.it #406-4420321-2498755
SPF:	PASS con l'IP 54.240.1.169 Ulteriori informazioni
DKIM:	'PASS' con il dominio amazon.it Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

ALTRI ATTACCHI DI INGEGNERIA SOCIALE
SMISHING E QUISHING

Oltre al phishing esistono ulteriori attacchi di ingegneria sociale, due che si stanno rivelando altrettanto efficaci e diffuse sono lo **smishing** e il **quishing**, che utilizzano rispettivamente *sms* e *codici qr* per I loro scopi malevoli.

Come nelle e-mail di phishing anche tramite sms e codici qr, l'obbiettivo è quello di ottenere informazioni riservate e sensibili del malcapitato, nel caso specifico dello smishing sono spesso usati come pretesto problemi di sicurezza legati a istituti finanziari (come la propria banca che richiede una modifica repentina delle credenziali di accesso) oppure sms ricevuti da fornitori di linea o servizi che propongono offerte molto vantaggiose. In questi casi non ci è possible verificare SPF, DKIM E DMARC ma siamo comunque in grado, sempre con molta attenzione, di verificare alcune particolarità che potrebbero farci storcere il naso:

- Gli istituti finanziari come banche non invieranno mai tramite SMS una richiesta di modifica delle credenziali di accesso, nel caso non si fosse sicuri è opportuno telefonare alla propria filiale di riferimento
- Offerte, coupon e altre forme di vendita tramite SMS sono da considerarsi preventivamente come attacchi di smishing
- Per precauzione è sempre meglio non cliccare eventuali link contenuti in SMS di cui non si è certi della provenienza e dell'autenticità

Allo stesso modo, il quishing tenta di ottenere informazioni sensibili tramite la scansione di un codice qr da parte del malcapitato, in questo caso è sempre meglio astenersi dallo scansionare codici di cui non siamo certi della loro provenienza da fonti verificate.

CONSEGNA [SETTIMANA 3 LEZIONE 5]
Ingegneria sociale

ESECUZIONE CONTROLLATA DI UN PHISHING

Mi è stata data l'occasione di effettuare un phishing controllato per verificare che i dipendenti abbiano compreso la gravità dell'ingegneria sociale e che sappiano effettivamente riconoscere un attacco in corso.

Per effettuare questo attacco mi servirò di un potente strumento open-source chiamato ***gophish***, che permette la creazione controllata di e-mail di phishing a scopo di test per aziende e privati.
Per ottenere la massima efficacia e poter ingannare al meglio i dipendenti occorre trovare una facciata che possa facilmente essere ingannevole e di cui si potrebbero insospettire difficilmente, in questo caso ho optato per una e-mail che fa riferimento ad un eventuale aggiornamento delle credenziali necessario dopo un periodo di tempo (in quanto un dipendente è difficile che utilizzi mail aziendali per effettuare accessi a app / siti web di terze parti – come amazon - per scopo personale).

Dopo che il dipendente ha aperto la mail e cliccato sul link malevolo, trovandosi davanti un ipotetica pagina web identica a quella originale, difficilmente metterà in dubbio la autenticità della pagina e inserirà le proprie credenziali, dando così accesso alle proprie informazioni personali, oltre che al proprio account.

In questo caso, ipotizzando che il server di posta sia associato ad un servizio come Outlook, una possible e-mail di phishing potrebbe essere quella mostrata a fianco.
Già da una prima osservazione è possibile notare qualche errore nell'indirizzo di posta del mittente (outloo.teeam@outlook.com)