DOI: 10.26314/GARR-Conf32-proceedings 13

Phishing simulato: le campagne di phishing sono tutte equivalenti?

Fabrizio Fioravanti, Marius Bogdan Spinu, Marco Alamanni

Università degli Studi di Firenze

Abstract. Nel presente articolo, partendo dalla consapevolezza che il fattore umano è uno degli elementi più critici nella catena della sicurezza informatica, viene presentato l'utilizzo di campagne di phishing come strumento di valutazione dei reali rischi aziendali e quindi finalizzate all'aumento della consapevolezza del rischio cyber degli utenti all'interno dell'Organizzazione. L'analisi è stata quindi estesa alle tipologie di campagne di phishing simulato studiandone gli impatti sull'organizzazione

Keywords. cybersecurity, awareness, phishing, training, risk

Introduzione

La tematica della sicurezza informatica è diventata ultimamente sempre più rilevante sia per il significativo aumento della disponibilità di servizi online (quindi un numero maggiore di sistemi informatici target) sia per una situazione geopolitica particolarmente complessa a livello mondiale.

L'analisi della consapevolezza (awareness) in ambito di cybersecurity è un tema molto sentito a livello nazionale (piano triennale per l'informatica nella PA – CAPITOLO 6 [1]), ma ovviamente è comunque di interesse primario per le organizzazioni identificare a quali rischi l'organizzazione stessa sia più esposta in termini di sicurezza informatica.

Una delle principali tematiche da considerare nella valutazione della postura di sicurezza di una organizzazione rimane il fattore umano e come esso possa rendersi complice talvolta inconsapevole di gravi compromissioni di sicurezza che possano portare anche a data breach rilevanti; uno degli elementi principali da valutare in questo contesto è come reagisca l'organizzazione a fronte di tentativi di phishing, in quanto la compromissione dell'identità digitale a mezzo di campagne di phishing è un tema sempre più attuale, diffuso e monetizzabile in vari modi da gruppi hacker.

Phishing simulato come strumento di indagine

Le campagne di phishing simulato, ove si inviano false e-mail di phishing con lo scopo di verificare come il bersaglio di queste campagne reagisca, è uno strumento importante non tanto per puntare l'attenzione sui comportamenti dei singoli, ma bensì per capire a quali rischi l'organizzazione nel suo complesso sia più esposta, programmando quindi percorsi informativi e formativi maggiormente efficaci.

Nel 2020 è iniziata una ricerca di mercato per individuare potenziali strumenti capaci di inviare campagne di phishing efficaci e nel 2021 e 2022 sono stati adottati 2 prodotti

Firenze, 14-16 giugno 2023 - ISBN: 978-88-946629-2-4

commerciali diversi per inviare a campioni casuali del personale dell'Ateneo campagne di phishing simulato.
La scelta dei prodotti, oltre che per la loro specifica usabilità è stata guidata anche dalla letteratura esistente in termini di campagne di phishing e della loro capacità di generare campagne con l'efficacia desiderata [2][3].
Di conseguenza, durante gli anni 2021 e 2022 all'interno dell'Ateneo Fiorentino sono state condotte analisi in questo senso, ma questo articolo non si concentra sui risultati numerici e sulle percentuali di persone che hanno avuto un certo comportamento bensì sugli strumenti adottati e sulle informazioni che sono state ricavate usandoli in maniera propria ed efficace per trarre informazioni sull'organizzazione nel suo complesso.
Le campagne di phishing non sono infatti tutte equivalenti e per avere una valutazione reale dei rischi a cui è esposta l'organizzazione è necessario non solo valutare la percentuale di persone che hanno fatto click su link malevoli o che hanno fornito le loro credenziali, ma anche e soprattutto gli stimoli a cui sono stati sottoposti.
Un aspetto rilevante considerato nella progettazione delle diverse campagne è stato quello di realizzarle a partire da informazioni e strumenti reperibili pubblicamente (elenchi di mail, pagine web, relazioni gerarchiche, etc) che fossero quindi anche nella disponibilità di un potenziale attaccante.
Il NIST (National Institute of Standards and Technology) ha proposto infatti di categorizzare una campagna di phishing sia sulla base del numero di indizi (number of cues) che sono presenti nella campagna stessa, ma anche su quanto la campagna sia correlata all'ambiente lavorativo o personale (premise alignment) del bersaglio.
Per indizi si intendono normalmente le caratteristiche quali, ad esempio, il fatto che ci siano link non pertinenti, mittenti esterni all'organizzazione oppure che la campagna voglia suggerire un senso di urgenza o che abbia errori di ortografia.
L'influenza predominante che anche nella nostra analisi abbiamo verificato essere presente, riguarda proprio questo ultimo aspetto, in quanto costruendo campagne con lo stesso numero e tipologia di indizi, la percentuale di persone che cadono nel phishing è decisamente più elevata se la simulazione riporta a contesti lavorativi o personali del soggetto.
Nella Tab. 1 è stata riportata anche una schematizzazione della difficoltà percepita dal soggetto nell'identificare come phishing la simulazione sulla base di questi fattori.

Tab. 1
Esempio di impatto dei diversi fattori di una campagna di phishing sulla complessità percepita

Number of cues	Premise alignment	Detection difficulty
Few (more difficult)	High	Very difficult
	Medium	Very difficult
	Low	Moderately difficult
Some	High	Very difficult
	Medium	Moderately difficult
	Low	Moderately to Least difficult
Many (less difficult)	High	Moderately difficult
	Medium	Moderately difficult
	Low	Least difficult

Nelle campagne erogate in Ateneo il numero di indizi era sempre basso, anche se alcuni elementi come link non consoni e mittenti non istituzionali erano sempre presenti proprio come spia di un phishing, al fine di permettere di rendere riconoscibile la campagna come tale.
Nella nostra esperienza infatti abbiamo verificato che sottoponendo a campagne di phishing generaliste il campione di soggetti, notavamo una buona postura di sicurezza generale dell'organizzazione mentre la risposta cambiava molto, a parità di difficoltà di identificazione della mail di phishing, se modificavamo la rilevanza a livello lavorativo o si applicava a contesti abituali per l'utente.
Quanto più il phishing era correlato all'attività lavorativa ed all'uso abituale dell'e-mail ed a strumenti quotidiani dell'attività lavorativa, tanto più si alzavano le percentuali di successo del phishing stesso.
Questa analisi ha permesso quindi di esaminare ed estrapolare con precisione la reale postura di sicurezza ed identificare a quali rischi le diverse categorie del personale fossero più esposte tracciando un profilo abbastanza preciso dell'utenza e degli ambiti di vulnerabilità; questo non sarebbe stato possibile utilizzando strumenti che sottoponevano il campione a campagne di phishing casuali senza una valutazione precisa sia della difficoltà di individuazione e dell'attinenza al soggetto obiettivo dell'analisi. La creazione quindi di campagne mirate controllando tutti gli aspetti dalla progettazione della campagna insieme alla resa grafica di essa ed al target ha permesso di ricavare importanti informazioni su come proteggere meglio l'organizzazione da questo rischio.
L'analisi si è spinta fino alla creazione di simulazioni di phishing molto mirato focalizzandosi sulle possibili leve a cui il soggetto poteva essere sensibile. In questo modo chi è caduto nel tranello della simulazione, ha permesso proprio di identificare le potenziali aree di criticità all'interno dell'organizzazione e non soltanto di fare statistiche circa le persone avevano avuto un certo tipo di risposta; questo insieme di informazioni ha fornito quindi indicazioni su quali fossero gli elementi su cui porre maggiore attenzione sia a livello organizzativo che in termini di proposizione di percorsi formativi ed informativi oltre che indicazioni puntuali a particolari categorie di utenti particolarmente rilevanti all'interno dell'organizzazione per il loro ruolo.

Conclusioni

Dopo 2 anni di sperimentazione e alcune campagne di phishing simulato erogate la nostra conclusione conferma l'ipotesi che per ottenere informazioni rilevanti sui rischi correlati al phishing non basti erogare campagne generaliste uguali per tutti o estratte casualmente da un pool di campagne non specializzate, soprattutto se tali campagne non sono state classificate per difficoltà e per attinenza, mentre la progettazione di campagne mirate permette di valutare al meglio la reale postura di sicurezza dell'organizzazione.
Le campagne di phishing non sono quindi tutte equivalenti e la realizzazione di una efficace analisi del rischio phishing passa da una progettazione mirata e specifica delle campagne a cui sottoporre il campione selezionato oltre che dalla selezione di informazioni pubblicamente accessibili, più che dall'erogazione massiva di simulazioni generaliste.

Questa analisi conferma e rende evidente il ruolo del "social engineering" e la rilevanza che possono assumere le informazioni che un ente pubblico è vincolato a rendere disponibili pubblicamente (e di conseguenza anche ai potenziali attaccanti) e che possono quindi contribuire a dare maggiore efficacia ad un reale attacco phishing sfruttando il fattore umano.

Riferimenti bibliografici

[1] Piano Triennale per l'informatica nella PA – Aggiornamento 2022/2024 - https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pa_2022-2024.pdf
[2] Michelle Steves, Kristen Greene and Mary Theofanos - A Phish Scale: Rating Human Phishing Message Detection Difficulty - Workshop on Usable Security (USEC) 2019
[3] Michelle Steves, Kristen Greene and Mary Theofanos - Categorizing human phishing difficulty: a Phish Scale - Journal of Cybersecurity, 2020, 1–16

Autori

Fabrizio Fioravanti fabrizio.fioravanti@unifi.it

Fabrizio Fioravanti è attualmente responsabile delle Unità di Processo Sistemi, tecnologie cloud e di sicurezza informatica e ad interim di Reti e postazioni di lavoro. Laureato in Ingegneria Elettronico ha un dottorato di ricerca in Ingegneria Informatica e delle Telecomunicazioni e da oltre 25 anni lavora nel settore ICT. Ha diverse pubblicazioni scientifiche al suo attivo in riviste italiane ed internazionali oltre che in libri e conferenze.

Marius Bogdan Spinu marius.spinu@unifi.it

Ingegnere, Dirigente dell'Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici nonché Responsabile per la Transizione al Digitale dell'Università degli Studi di Firenze. Lunga esperienza come dirigente nel Sistema Sanitario Toscano nell'ambito ICT con riferimento ai processi ospedalieri, amministrativi e della logistica del farmaco. Crede che la tecnologia sia uno dei principali driver dei processi di crescita e che la sicurezza sia un elemento trasversale di tali processi.

Marco Alamanni marco.alamanni@unifi.it

Marco Alamanni si occupa attualmente di sicurezza informatica, all'interno dell'Unità di processo "Sistemi, tecnologie cloud e di sicurezza informatica"
del Sistema Informatico dell'Ateneo.
È laureato in Informatica presso l'Università di Pisa, dove ha anche frequentato il corso di Laurea Magistrale in Sicurezza Informatica.
Tra i suoi interessi principali nell'ambito della sicurezza informatica, ci sono threat intelligence, digital forensics e Osint.