KnowBe4
Human error. Conquered.

WHITEPAPER

Phishing: il Punto di Svolta

Efficacia della Formazione, del Phishing Simulato e della Risposta Umana

Executive Summary

L'utilizzo di una programma per la formazione alla consapevolezza dei rischi informatici con test di phishing può costituire un efficace ed utile strumento per ridurre le minacce interne inconsapevoli. Tuttavia, se non ci sono degli indicatori oggettivi per valutarne l'efficacia, i test di phishing possono creare soltanto dei buchi neri. Degli indicatori significativi per la valutazione della suscettibilità al pishing dovrebbero dirti qualcosa di più oltre al tasso di "cliccamento", e permetterti di comprendere i pattern relativi al tipo di lavoro di un impiegato ed al suo ambiente di lavoro.

Esigenze Principali

- Un programma di Security Awareness Training fa la differenza sul lungo e breve periodo: lo staff IT e la dirigenza dovrebbero considerare l'efficacia a lungo termine della formazione al momento di valutare quale programma adottare.
- Anche le truffe più palesi funzionano ancora. È importante comprendere il livello di consapevolezza del personale sui livelli di sofisticazione delle email di phishing.
- Lo staff IT e la dirigenza devono essere consapevoli di quali tipi di mansioni e quali periodi nell'arco della giornata lavorativa possono influenzare le risposte alle email di phishing.
- Valutazioni del phishing basate sui dati relativi a chi clicca e quando, possono indicare in modo più efficace dei pattern di vulnerabilità al phishing all'interno dell'organizzazione, rispetto al tasso globale di click.
- Una comunicazione chiara all'interno dell'azienda circa gli aggiornamenti IT o I processi delle Risorse Umane può giocare un ruolo fondamentale nell'evitare fraintendimenti e nel bloccare attacchi di phishing basati su temi genericamente legati all'azienda.
-

Questo Whitepaper

Questo whitepaper riporta i risultati di uno studio sperimentale della durata di 6 mesi per valutare l'efficiacia a breve e lungo termine del programma di formazione di KnowBe4 "Kevin Mitnick Security Awareness Training" (modulo da 40 minuti). L'ambito della sperimentazione era costituito da normali email di phishing su aziende medio-piccole. Questo whitepaper è sponsorizzato da KnowBe4.

"È vero l'adagio che dice che I sistemi di sicurezza devono vincere sempre, un attaccante basta che abbia successo una sola volta.

—Dustin Dykes, CISSP
Founder Wirefall Consulting

Phishing: lo Stato dell'Arte

Il costo annuale stimato del crimine informatico sull'economia mondiale è stato nel 2015 di 450 miliardi di dollari.[1] Una somma davvero notevole. L'aspetto più preoccupante è che il 90-95% di tutti gli attacchi informatici che hanno successo parte da un'email di phishing.[2] Si è stimato che circa 156 milioni di email vengono inviate ogni giorno, 16 milioni oltrepassano i filtri di sicurezza, e 800.000 di queste vengono non solo aperte ma anche cliccate. Infine, si stima che circa 80.000 delle persone che hanno cliccato su un link ha inconsapevolmente fornito agli attaccanti informazioni riservate.[3] Oltre a ciò, ogni tre mesi vengono identificate qualcosa come 250.000 nuove URL di phishing.[4]

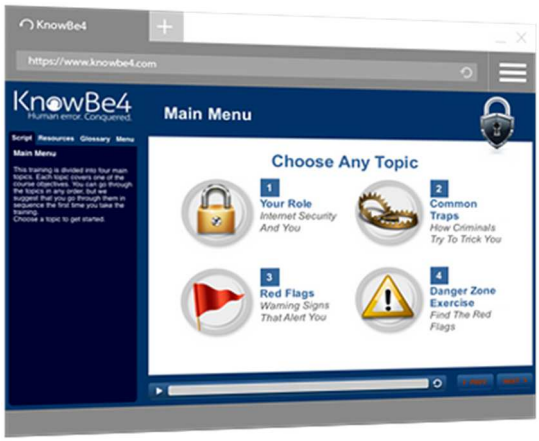
Sebbene si possano effettuare campagne automatizzate e massive di phishing, le campagne che hanno più successo sono quelle costruite su misura attorno ad un'organizzaazzione o una persona, il cosiddetto spear phishing. Tuttavia, una significativa quantità di email massive che sembrano essere inviate da un indirizzo falso o contraffatto hanno anch'esse successo.

Riuscire a non soccombere ad una campagna di phishing massiva è un punto di svolta nel livello di consapevolezza di un individuo o di un'organizzazione. Come per l'apprendimento di un nuovo linguaggio, il punto di svolta[5] è dato quando la struttura della lingua comincia ad acquisire un senso e tutto da quell momento in poi diviene più facile da imparare.

Nel phishing, similmente, un punto di svolta si ha quando si diviene chiaramente consapevoli dei segnali, e si possono apprendere facilmente le nuove tecniche del phishing. Una volta che abbia raggiunto questo punto di svolta, l'utente sarà in grado di non cliccare sui link di phishing in regolarmente e sistematicamente per un lungo periodo di tempo.

Testare il Punto di Svolta in un Esperimento di Phishing:

Quanto è efficace la formazione alla consapevolezza del phishing?



E' stata testata l'efficacia del programma di KnowBe4 "Kevin Mitnick Security Awareness Training" in un esperimento della durata di 6 mesi. Il campione era costituito da utenti rappresentativi di cinque differenti compagnie medio-piccole di settori critici dell'industria, per un totale di 1090 partecipanti.

La formazione comprendeva un'interfaccia web ad una piattaforma di apprendimento interattivo. Utilizzando questo tipo di formazione, i partecipanti al corso potevano cliccare sugli argomenti, guardare dei video e testare la propria conoscenza. Il tempo medio di completamento in media è di 40 minuti.

Nel corso dell'esperimento sono state testate le più comuni email aziendali provenienti da Risorse Umane e IT. Prima dell'inizio del training, a tutti i partecipanti è stata inviata una email di phishing per costituire una baseline. Nell'email veniva richiesto di modificare immediatamente la propria password e, nel caso in cui il link di phishing fosse stato cliccato, si apriva una pagina '404 Not Found'.

Successivamente, i partecipanti avevano un mese per completare la formazione online di 40 minuti e, al termine, sono state inviate quattro campagne di phishin su base mensile. Se cliccate, si apriva una landing page che notificava il fatto che si era trattato di un'email di phishing e forniva un breve riassunto delle cose cui è necessario prestare attenzione.

Consapevolezza, Riduzione del Tasso di Click, e Comprensione del Fattore Umano dei Cliccatori Recidivi

Quattro sono stati i principali risultati dello studio:

(1) Grazie al corso "Kevin Mitnick Security Awareness", è stato possibile arrivare ad un punto di svolta nella consapevolezza del phishing che è continuato per tutta la durata dello studio;

(2) Analizzando i tassi di click, si possono identificare dei pattern relative a coloro che cliccano: in questo studio ci sono stati molti che hanno cliccato dopo l'orario di lavoro;

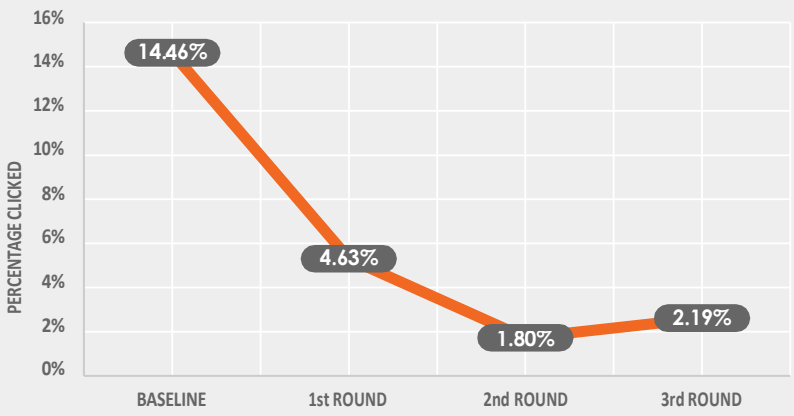
(3) Cultura aziendale e professione possono giocare un ruolo nella suscettibilità al phishing;

(4) Le email di phishing in questo esperimento avrebbero potuto essere facilmente identificate se ci fosse stata una comunicazione chiara sulle procedure delle Risorse Umane e le questioni IT rilevanti per il personale.

Tasso di Click Perdurante. I risultati, come evidenziato dal grafico, mostrano un basso tasso di click costante e duraturo con un grande abbassamento dopo la formazione ed un leggero calo nei mesi successivi. Il fatto che questo abbassamento sia continuato nei mesi dopo la formazione indica che chi prima era indotto a cliccare sui link di phishing, poi non lo era più.

Una volta ottenuta e mantenuta nel tempo la riduzione del tasso di click nel campione globale, la sfida successiva è comprendere i fattori umani di coloro che sono cliccatori persistenti.

Punto di Svolta nel Tasso dei Click di Phishing



Cliccatori "After-hour". Lo studio ha esaminato una piccola percentuale di coloro che cliccavano nonostante avessero eseguito la formazione, ed ha messo insieme indizi contestuali e meta-dati nello sforzo di comprendere i fattori umani dei click persistenti. Risulta che, a seconda delle organizzazioni, dal 25% fino al 70% di chi clicca lo fa dopo l'orario di lavoro, alla sera o a tarda notte. La percentuale totale aggregata di coloro che cliccano dopo l'orario di lavoro è del 57%. Ci sono molti fattori che possono essere implicati in questa tempistica, comunque potrebbe essere dovuta a turni serali o notturni. Sebbene la comprensione di questo elemento va al di là dell'ambito di questo esperimento, è tuttavia interessante notare che un significativo 2-4% di coloro che cliccano lo fa subito dopo l'orario d'ufficio tradizionale (8am - 5pm).

Cultura Aziendale. Riconoscendo che ciascun ufficio o dipartimento all'interno di un'organizzazione ha una propria cultura, l'esperimento ha volute controllarne le differenze. Per esempio, quasi sempre la descrizione stessa del lavoro di receptionist, risorse umane, assistenza client e PR richiede di relazionarsi con gli altri, costruire rapporti e venire in aiuto sia ai membri della propria organizzazione che con quelli al di fuori.[6]

“Puoi spendere una fortuna acquistando tecnologia e servizi, ma la tua infrastruttura di rete rimarrà sempre vulnerabile rispetto alle manipolazioni vecchio stile"

-Kevin Mitnick

Le persone in questi ruoli tendono ad essere target dell’ingegneria sociale a causa del loro atteggiamento collaborativo verso gli estranei maggiormente rispetto a coloro che lavorano nell’IT, nella sicurezza, nell’ufficio legale i quali tendono ad essere più circospetti e, più frequentemente, integrano la sicurezza operativa nella vita di ogni giorno. Lo studio ha rilevato che coloro le cui mansioni richiedano l’interazione con estranei sono più predisposti a cliccare sui link di phishing rispetto agli altri.

Comunicazione Chiara. Le email usate nello studio simulavano email generiche relative ad argomenti HR o IT. Alcune delle email di phishing sarebbero state facilmente evitate tramite una chiara comunicazione al personale relativamente a queste tematiche. Nell’ambito Risorse Umane, i processi avrebbero dovuto essere comunicati chiaramente in modo da evitare possibili fraintendimenti così come il successo dei tentativi di phishing basati su generici temi aziendali. Canali aperti di comunicazione efficace per gestire in modo trasparente le aspettative del personale relative a temi tecnici dell’IT o processi HR, possono fare molto per evitare i click su email generiche di phishing sull’aggiornamento delle password o le procedure HR. Un buon esempio? L’IT non ti chiederà mai la tua password.

Combinare l’Analisi del Phishing Guidata dai Dati ed il Fattore Umano

Che sia per motivi legali, di audit, di istruzione o di sicurezza, molte organizzazioni hanno ingaggiato delle compagnie che fanno formazione sulla security awareness per essere aiutate a ridurre i rischi degli attacchi di phishing. Tuttavia, qualche volta il consiglio di amministrazione e gli auditor sono interessati soltanto ad un basso numero di click, senza investigare più a fondo negli aspetti umani di coloro che cliccano, e ciò un buco nero nell’ingegneria sociale dell’azienda. Come si dice nei circoli della sicurezza informatica, i difensori devono essere capaci di evitare il 100% degli attacchi, mentre agli attaccanti basta avere successo con un solo attacco. Con centinaia di milioni di email di phishing inviate ogni giorno, per i difensori ciò costituisce uno sforzo titanico. Gli impiegati possono costituire una linea difensiva efficace se istruiti adeguatamente e quando l’analisi dei dati può servire ad indirizzare la giusta formazione alla giusta audience.

Raggiungere un punto di svolta nell’azienda con un basso numero di click che dura nel tempo è il primo passo. Quello successivo è comprendere i pochi che continuano a cliccare e i fattori sottostanti a questo comportamento. Se un’organizzazione sta tentando di ridurre il rischio del phishing, deve andare al di là del tasso di click e comprendere l’elemento umano per costruire un atteggiamento anti-phishing più robusto.

Abbiamo raggiunto un punto di svolta relativamente al phishing. E ora?

Che cosa accade quando un individuo o un’organizzazione raggiungono il punto di svolta? È il momento di alzare il livello.

Il punto di svolta è una rampa di lancio per il proseguimento dell’istruzione in modo più sofisticato e strategico. Così come non possiamo aspettarci che chi ha appena imparato a leggere sia in grado di leggere la letteratura classica, non possiamo neppure attenderci che coloro che sono stati appena istruiti sulla consapevolezza del phishing siano capaci di rispondere ad APT costituite da email di spear-phishing. Sin dall’infanzia, l’acquisizione della conoscenza è un processo graduale e fortunatamente può essere migliorata ed accresciuta grazie ad istruzione ed esperienza.

Il passo successive è fare ripetute modifiche ai livelli di phishing. Durante questo periodo è importante avere dei canali di comunicazione aperti con fornitori interni od esterni di servizi di phishing simulato. Questi ultimi sarebbe auspicabile che integrassero l'affiancamento del cliente tra i servizi offerti, in modo da aiutare le organizzazioni a capire come accrescere la propria consapevolezza su questi temi in un modo che meglio si adatti alla specifica cultura aziendale, ai settori, ed al personale.

La Cultura della Sicurezza supporta la Prima Linea di Difensori Umani

In sostanza, tutto si reduce a consapevolezza ed istruzione. La ragione per cui molte persone sono esperte in merito alle truffe del "Principe Nigeriano" è l'essere stata illustrata innumerevoli volte sulla stampa,[7] ed un numero significativo di persone ne hanno avuto esperienza diretta o tramite qualche loro conoscente, oppure ancora tramite qualche storiella che è uno dei migliori modi per diffondere la consapevolezza. La morale è che più sono le persone consapevoli di come si presenta un'email di phishing e più sono le probabilità di evitarlo.

Le abitudini richiedono del tempo per formarsi ed entrare a far parte della vita di ogni giorno; lo stesso si applica al divenire "cyber street-smart" ed alla prevenzione del phishing. Portare un'intera organizzazione dal livello zero alla prima linea di difesa contro criminali informatici, spionaggio industriale e hacker navigate richiede un'istruzione graduale e la pazienza di comprendere il panorama umano di quella organizzazione.

Sull'Autore

Lydia Kostopoulos (@LKCYBER) ha ottenuto il PhD in Security Policy ed è un pentester certificate di ingegneria sociale. Collabora attivamente nella comunità cyber statunitense ed internazionale su diversi fronti per promuovere la collaborazione ed aumentare la consapevolezza al fine di mitigare la vulnerabilità umana ai rischi della sicurezza informatica. Partecipa al programma NATO Science for Peace (SPS), tiene corsi universitari su intelligence e politiche cyber, ed è membro dell'InfraGard Alliance dell'FBI.

Su KnowBe4

KnowBe4 offre la più popolare piattaforma integrate di Security Awareness Training e Phishing Simulato. Migliaia di imprese la utilizzano con notevoli risultati. Basata sulla trentennale ed unica esperienza di hacking di Kevin Mitnick's, è uno strumento che ti aiuta a gestire meglio gli urgenti problemi di sicurezza IT relative ad ingegneria sociale e phishing, permettendoti di creare il tuo "firewall umano".

Questo valido programma interattivo basato su web, combinato con frequenti simulazioni di attacchi di phishing, utilizza studi di casi, video live dimostrativi e brevi test di comprensione. Il Kevin Mitnick Security Awareness Training da la possibilità di accertarsi che gli impiegati capiscano i meccanismi di spam, phishing, spear phishing, malware ed ingegneria sociale e siano in grado di applicare questa conoscenza nel loro lavoro di ogni giorno. È possibile inviare illimitati attacchi di phishing simulato ai propri impiegati nel corso dell'anno sfruttando l'ampia libreria di template di phishing. Per maggiori informazioni, visita il sito www.digiTree.it

RIFERIMENTI:

1. CSIS McAVee Report - http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
2. TrendMicro Research - http://www.techworld.com/news/security/91-of-cyberattacks-begin-with-spear-phishing-email-3413574/
3. Get Cyber Safe - http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx
4. McAfee - http://www.mcafee.com/es/resources/misc/infographic-phishing-quiz.pdf
5. Neil Jones (2014). Studies in Language Testing: Multilingual Frameworks – The construction and use of multilingual proficiency frameworks. Cambridge University Press
6. Christopher Hadnagy (2010). Social Engineering: The Art of Human Hacking. Wiley.
7. Blake Ellis. (2013). CNN Money. 5 most common financial scams - http://money.cnn.com/2013/09/12/pf/financial-scams/

DigiTree | Trieste (Italia), via di Romagna 9/1 | M: +39 366 8948545 | www.digiTree.it | E: Sales@digiTree.it