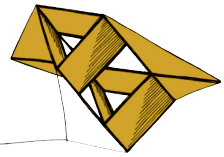


Systém pro rozesílání cvičných phishingových zpráv

Martin Šebela[1]

1 Úvod

S tím, jak se internet stal standardem běžného života dnešní společnosti, došlo k tomu, že stejné médium začali využívat i lidé, jejichž cílem je z méně pozorných uživatelů získat důvěrné informace (hesla, čísla platebních karet apod.), a ty následně zneužít ve svůj prospěch. Typickým příkladem je phishing (např. podvodné e-maily) a s ním související metody sociálního inženýrství, kterých útočník využívá.

Cílem této bakalářské práce tak bylo vytvořit systém, který umožní rozesílat cvičné phishingové zprávy (včetně odkazů na cvičné podvodné webové stránky), na základě kterých budou dobrovolně registrovaní uživatelé schopni lépe odhalovat reálný phishing. Uživatelé mohou z těchto cvičných podvodných e-mailů zjistit, na co se mají v elektronické komunikaci zaměřit, jakých metod mohou útočníci využívat, a především se v případě neúspěchu i poučit – systém uživateli poskytne zpětnou vazbu, čeho si měl na podvodném e-mailu všimnout a podle jakých indicií mohl prohlásit, že se jedná o phishing.

2 Vytvořený systém Phishingator

Systém byl vytvářen tak, aby nesloužil pouze administrátorům k rozesílání cvičného phishingu, ale i běžným uživatelům, čímž se liší od všech ostatních, existujících řešení. Existující řešení navíc neobsahují funkce požadované univerzitou, přičemž některá z nich jsou i finančně nákladná. V minulosti byl na univerzitě cvičný phishing rozesílán ve spolupráci s externí organizací *CESNET*.

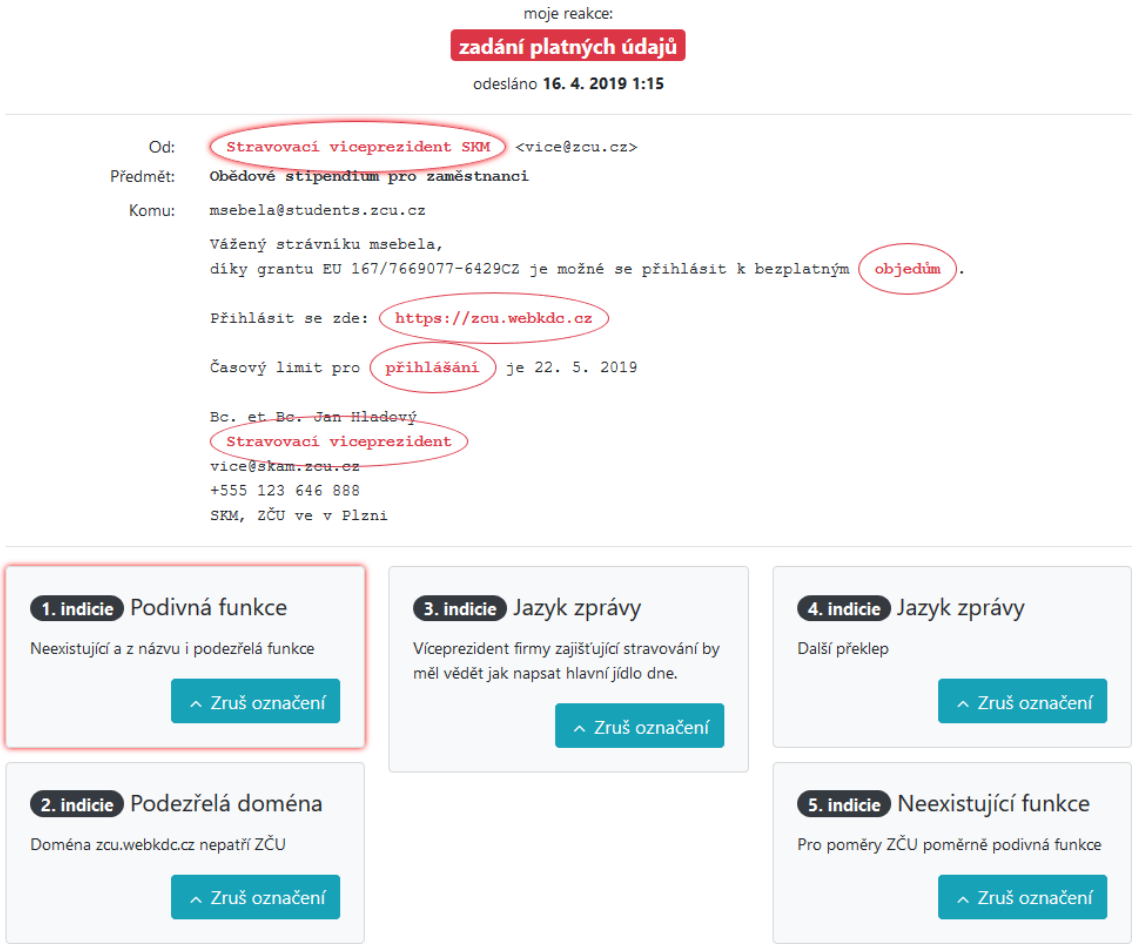
Administrátor je schopen v naprogramovaném systému během několika minut vytvořit novou phishingovou kampaň, která se skládá z rozesílaného podvodného e-mailu, podvodné webové stránky, jejíž odkaz bude v e-mailu uveden, dále pak z akce, která se stane po odeslání formuláře na podvodné stránce a konečně také ze seznamu příjemců (a dalších parametrů jako data spuštění a ukončení kampaně apod.). Všechny zmíněné fragmenty phishingové kampaně lze v systému také vytvářet a dále spravovat (tj. podvodné e-maily, indicie k rozpoznání phishingu u daného e-mailu a podvodné webové stránky).

Po spuštění phishingové kampaně dochází ke sledování příjemců, a sice tak, že jsou na podvodné stránce zaznamenávány všechny akce uživatelů (tj. zdali stránku navštívili, zdali vyplnili platné či neplatné přihlašovací údaje, nebo zdali na podvodný e-mail vůbec nereagovali). Všechna zaznamenaná data jsou systémem zpracována a přehledně zobrazena do několika grafů a tabulek, přičemž získaná data je také možné exportovat do formátu CSV *(Comma-separated values)*.

Běžní uživatelé (kdokoliv s univerzitním kontem) se do systému mohou přihlásit a zároveň se dobrovolně registrovat k odebírání cvičných phishingových zpráv (včetně možnosti nastavit

[1] student bakalářského studijního programu Inženýrská informatika, obor Informatika,
e-mail: msebela@students.zcu.cz

si případný limit). Uživatelé si mohou všechny přijaté phishingové e-maily zpětně prohlédnout, a to včetně indicií (označených pasáží v textu včetně popisu), na základě kterých bylo možné phishing rozpoznat (viz obr. 1).



Obrázek 1: Jeden ze cvičných phishingových e-mailů včetně seznamu indicií (zakroužkovaných pasáží v textu včetně souvisejícího popisu v dolní části obrázku) tak, jak si jej může uživatel zobrazit ve vytvořeném systému (tento e-mail byl zároveň zasílán vybraným uživatelům v rámci testování bakalářské práce, přičemž v horní části obrázku je uživateli zobrazeno, jak na e-mail, popř. na podvodnou webovou stránku reagoval)

Systém byl naprogramován ve skriptovacím jazyce PHP s využitím architektury MVC *(Model–View–Controller)*, data se ukládají do MySQL databáze a celý systém je propojen s univerzitním LDAP *(Lightweight Directory Access Protocol)* a autentizační službou *WebAuth*.

3 Závěr

Vytvořený systém byl v rámci bakalářské práce pilotně otestován zaměstnanci i studenty a nasazen na server *Západočeské univerzity v Plzni*. Systém je tak dostupný všem uživatelům univerzity, a to na oficiální URL adrese `https://phishingator.zcu.cz`. Systém bude dále využíván ke vzdělávání uživatelů univerzity v oblasti phishingu a dále vylepšován o nové funkce. Systém byl zároveň navržen jako modulární a mohl by tak být nasazen i na jiné univerzitě.