Západočeská univerzita v Plzni
Fakulta aplikovaných věd
Katedra informatiky a výpočetní techniky

Bakalářská práce

Systém pro rozesílání cvičných phishingových zpráv

Plzeň 2019 Martin Šebela

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta aplikovaných věd
Akademický rok: **2018/2019**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin ŠEBELA**
Osobní číslo:	**A15B0135P**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informatika**
Název tématu:	**Systém pro rozesílání cvičných phishingových zpráv**
Zadávající katedra:	**Katedra informatiky a výpočetní techniky**

Zásady pro vypracování:

1. Seznamte se s problematikou rozesílání phishingových zpráv a sociálním inženýrstvím.
2. Navrhněte systém pro automatizované rozesílání cvičných phishingových zpráv.
3. Navržený systém implementujte.
4. Systém otestujte a výsledky vyhodnoťte.

Rozsah grafických prací:	**dle potřeby**
Rozsah kvalifikační práce:	**doporuč. 30 s. původního textu**
Forma zpracování bakalářské práce:	**tištěná**
Seznam odborné literatury:	

Dodá vedoucí bakalářské práce.

Vedoucí bakalářské práce:	**Ing. Aleš Padrta, Ph.D.** Centrum informatizace a výpočetní techniky
Konzultant bakalářské práce:	**Doc. Ing. Pavel Král, Ph.D.** Katedra informatiky a výpočetní techniky

Datum zadání bakalářské práce:	**10. října 2018**
Termín odevzdání bakalářské práce:	**2. května 2019**

Doc. Dr. Ing. Vlasta Radová
děkanka

Západočeská univerzita v Plzni
Fakulta aplikovaných věd
L.S.

Doc. Ing. Přemysl Brada, MSc., Ph.D.
vedoucí katedry

V Plzni dne 15. října 2018

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů.

V Plzni dne 25. dubna 2019

Martin Šebela

Abstract

The first part of the bachelor's thesis deals with phishing and techniques of social engineering. In the second part of the thesis is created software that allows to send phishing training e-mails to selected recipients. Sent phishing e-mails contain a link to fraudulent websites created in this software. The software automatically tracks users how they respond and what they fill in a form on a fraudulent website. The software uses these data to generate statistics and charts. Users can review all received phishing training e-mails in the software together with a list of signs of phishing. Users can educate themselves based on these signs of phishing e-mails in this software.

Abstrakt

Práce se v teoretické části zabývá phishingem, sociálním inženýrstvím a jeho metodami. V rámci praktické části práce je vytvořen software, který umožňuje rozesílat vybraným uživatelům cvičné phishingové zprávy s odkazy na vlastní podvodné stránky. Uživatel je po obdržení phishingového e-mailu automaticky sledován, jakým způsobem bude reagovat a zdali na podvodné stránce vyplní platné, či neplatné přihlašovací údaje, přičemž získaná data software použije ke generování statistiky. Přidanou hodnotou softwaru je fakt, že příjemce phishingových zpráv má možnost si v systému všechny jemu doručené e-maily zpětně prohlédnout včetně seznamu indicií, na základě kterých mohl phishing rozpoznat a pomocí kterých se může řídit při odhalování reálného phishingu.

Poděkování

Chtěl bych poděkovat vedoucímu práce, panu *Ing. Aleši Padrtovi Ph.D.* za důkladné vedení bakalářské práce a za všechny připomínky s ní související. Dále pak konzultantovi práce, panu *Ing. Jiřímu Čepákovi* za připomínky týkající se vytvořeného softwaru.

Obsah

1 Úvod

Internet a informační technologie už dávno nejsou doménou omezeného množství lidí, kteří je používali výhradně k vědeckým nebo jiným specializovaným účelům. S postupným rozšířením těchto technologií a služeb do celé společnosti, již dnes prakticky nelze nalézt člověka v produktivním věku, který nemá založen vlastní e-mail nebo jiný způsob elektronické komunikace (už jen z důvodu výměny zpráv s úřady a jinými institucemi), o účtech na sociálních sítích nemluvě. Je třeba si ovšem uvědomit, že na stejné médium se přesunuli i lidé, jejichž cílem je z méně pozorných uživatelů získat důvěrné informace, a ty následně zneužít ve svůj prospěch. A i když bude systém, který chce útočník napadnout nebo z něho získat informace, sebelépe zabezpečen, zásadní roli bude hrát vždy lidský faktor a s ním související metody sociálního inženýrství. Mnoho uživatelů navíc o této hrozbě vůbec neví, nebo si ji dokonce raději nepřipouští.

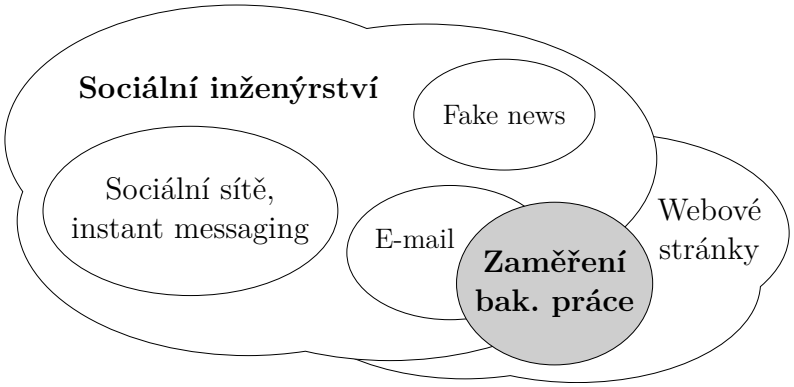
Tato práce by měla umožnit uživatelům ZČU se na dobrovolné bázi přihlásit k odebírání cvičných podvodných phishingových zpráv, na základě kterých budou uživatelé schopni lépe odhalovat reálný phishing. Uživatel bude moci z těchto cvičných podvodných e-mailů zjistit, na co se má v elektronické komunikaci 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.

V době psaní práce jsou na ZČU pravidelně pořádány teoretické i praktické semináře k phishingu bezpečnostním týmem WIRT[1]. Systém vzniklý z této práce tak může uživatelům posloužit k tomu, aby se odhalování phishingu nevěnovali pouze v průběhu semináře, ale aby jim byl do jejich e-mailových schránek jednou za čas doručován cvičný phishing a oni byli schopni reagovat kdykoliv. Pokud se totiž dostane do oběhu phishing, který zatím nebyl bezpečnostním týmem podchycen, je nutné, spolehnout se na vlastní rozum uživatele. V případě jeho oklamání může dojít ke zneužití osobních údajů nebo odcizení účtu uživatele. Účet může útočník zneužít například k rozesílání nevyžádané pošty (spamu), a poškodit tak reputaci celé instituce. Ostatní poštovní servery začnou považovat všechny e-maily pocházející z takového zdroje za spam a automaticky je odmítat. Důvěryhodnost a el. komunikace všech uživatelů instituce tak může být významně narušena.

[1] WEBnet Incident Response Team – `https://wirt.zcu.cz`

2 Sociální inženýrství

Techniky sociálního inženýrství jsou založeny na různých způsobech psychologického nátlaku na člověka [29]. Samotný phishing a problematika podvodných webových stránek (a tedy zaměření této práce) je jen malou podmnožinou celého sociálního inženýrství (viz obr. 2.1).



Obrázek 2.1: Sociální inženýrství v rámci internetu zasahuje do mnoha různých oblastí, přičemž tato práce se zaměřuje jen na vymezený rozsah

2.1 Metody sociálního inženýrství

Jedná se o postupy, kterými se útočník snaží přesvědčit svou oběť k vykonání nějaké akce [26], přičemž útočník může metody různě kombinovat, aby na oběť zapůsobil co nejsilněji. Pak existuje velká pravděpodobnost, že uživatel nebude jednat racionálně, ale zbrkle na základě svých emocí a bude povolnější k provedení akce, kterou po něm útočník požaduje. Svou chybu si navíc uživatel uvědomí až tehdy, když dojde k nějakým škodám, které jeho jednáním vznikly [17].

V případě cílení útoku na konkrétního uživatele dnes útočníkovi ve velkém pomáhají sociální sítě. Drtivá většina uživatelů na nich dobrovolně zveřejňuje nejrůznější střípky ze svého osobního i profesního života a útočník má tak možnost z veřejně dostupných dat danou osobu jednoduše profilovat. Většina uživatelů totiž nechává nastavení ochrany soukromí na hodnotách, které jim přednastavila samotná sociální síť – to jsou často položky nastavené na volbu *veřejné*, *viditelné pro všechny* apod. Na základě těchto uživatelem zveřejněných informací může například útočník zjistit odpovědi na

různé bezpečnostní otázky, které jsou vyžadovány pro změnu hesla uživatele. Konkrétně na nejznámější sociální síti *Facebook* lze navíc informace vyhledávat pomocí uživatelsky přívětivých a pochopitelných dotazů, podle kterých je dotazovanému poskytnuta požadovaná odpověď. Jedná se o vyhledávací systém *Facebook Graph Search*, který využívá zpracování přirozeného jazyka pro pochopení zadaných otázek [2]. Například zadáním výrazu `photos liked by jméno příjmení` do vyhledávacího pole na zmíněné sociální síti je možné, nechat si vypsat fotografie, které nějakým způsobem na sociální síti zvolený uživatel ohodnotil (formou tlačítka *like*, popř. jeho dalšími nabízenými alternativami), a toho využít ve svůj prospěch. Jakýkoliv dotaz je navíc možné ještě parametrizovat například zadáním časového období, kdy uživatel danou akci provedl (viz obr. 2.2). Útočník si může zmíněný nebo jiný výraz nechat automaticky sestavit pomocí webového nástroje – například na adrese `https://www.stalkscan.com`.

```
https://www.facebook.com/search/id-uzivatele/photos-liked/
            this-month/date/photos/intersect
```

Obrázek 2.2: Univerzální URL adresa vedoucí na sociální síť *Facebook*, pomocí které budou přihlášenému útočníkovi zobrazeny fotografie, které uživatel (podle parametru `id-uzivatele` na sociální síti) za poslední měsíc nějakým způsobem ohodnotil (formou tlačítka *like* apod.)

Útočník ovšem nemusí profilovat pouze jednotlivce, ale i skupinu uživatelů například v nějaké firmě. Zjistí si, jaký software a služby uživatelé ve firmě běžně používají (například k interní komunikaci [18]) a podle toho přizpůsobí svůj útok.

2.1.1 Vydávání se za autoritu

V tomto případě se jedná o oslovení uživatele jménem některé z vyšších autorit, ze které může mít ze své podstaty respekt a hlavně strach. Uživatel si je navíc vědom toho, že daná instituce nebo člověk může něco ovlivnit (resp. má nějakou moc – může například zablokovat účet) [29].

Příkladem může být phishing, který se vydával za e-mail od existujícího exekutorského úřadu a po uživateli vyžadoval splacení fiktivní pohledávky [19]. Cílem tohoto phishingu bylo donutit uživatele otevřít infikovanou přílohu, která se vydává za fakturu k fiktivní pohledávce.

2.1.2 Časová tíseň

Jde o snahu přesvědčit oběť, aby v co nejkratší možné době provedla akci, kterou útočník vyžaduje. Útočník využívá toho, že nedává uživateli čas na přemýšlení o tom, jestli se jedná o podvod. S velkou pravděpodobností tak bude uživatel své akce provádět zcela automaticky, aniž by si prověřil, na jakém webu se opravdu nachází, komu a co odpovídá apod., protože je pod časovým tlakem.

Ten samý následek ale může způsobit i přepracování uživatele. V takovém případě může uživatel na zprávy nahlížet jen zběžným pohledem, bude přehlížet řadu znaků phishingu (viz kapitola 3.2) a podvod tak nemusí odhalit.

Způsob tohoto útoku může spočívat například ve výzvě k okamžité změně hesla z důvodu napadení stránek. Pokud uživatel tuto akci neprovede do útočníkem zvoleného času, je uživateli vyhrožováno, že o účet včetně dat v něm uložených (a například ještě fotografií, které mohou mít vyšší emocionální hodnotu), přijde. Stejným případem by byla zpráva od exekutorského úřadu (v souvislosti s bodem 2.1.1), že pohledávku je nutné uhradit do následujícího dne od přečtení e-mailu, jinak budou následovat právní kroky vůči uživateli.

2.1.3 Hrozba ztrátou

Útočník se snaží v oběti vyvolat pocit, že by mohla přijít o něco, co má, nebo o něco, co by mohla získat (ztráta příležitosti).

Uživateli může být útočníkem nabízena jedinečná příležitost, která se již nemusí znovu naskytnout. Typickým příkladem může být odměna za odpověď na jednoduché otázky (například formou kvízu, ve kterém mohou být ovšem všechny odpovědi úmyslně správné [24, 27]). Za správnou odpověď a za poskytnutí osobních údajů a informací o kreditní kartě je slíbena věc o nemalé finanční hodnotě. Celý proces navíc může být umocněn ostatními uživateli (útočníkem vytvořenými a smyšlenými osobami), které budou na kvíz reagovat tak, aby byl uživatel přesvědčen o pravosti celé akce [24].

2.1.4 Vzbuzení soucitu

Dalším ze způsobů je nadměrné používaní přídavných jmen v obsahu sdělení. Ty jsou volena takovým způsobem, aby v kombinaci s ostatními slovy vzbudila v uživateli soucit (součástí bývá typicky prosba o pomoc). Pozornost uživatele je tak věnována především emoční stránce sdělení než samotné zprávě.

2.1.5 Nátlak skupinou

Útočník využívá příslušnosti uživatele k nějaké skupině (resp. kolektivu, pracovnímu oddělení) k tomu, aby přesvědčil uživatele k provedení určité akce. Uživatel je ujištěn tvrzením, že všichni ostatní ze skupiny danou akci již provedli, měl by to tedy udělat také. Tvrzení se ovšem nezakládá na pravdě a pokud si uživatel tuto informaci neprověří, je pravděpodobné, že provede akci, kterou po něm útočník vyžaduje.

2.1.6 Utajování

Cílem útočníka je přesvědčit oběť k tomu, aby veškeré detaily o jejich vzájemné komunikaci zůstaly pouze mezi nimi. Uživatel se ze snahy dodržet slovo (ale i ze strachu) neporadí s nějakou jinou, nezávislou osobou, která by mohla nekalé chování útočníka identifikovat a uživatele na něj upozornit. Mezi oběma stranami se tak může tvořit falešné pouto, kterého útočník zneužívá.

2.1.7 Pretexting

Hlavní náplní pretextingu je vzbudit v uživateli dojem, že je něco pravda, používáním kontextu typického pro danou věc [29]. K přesvědčení útočník používá s věcí související vazby, slovní spojení a informace, které by uživatel u dané věci očekával a nejsou tedy nijak podezřelé. Cílem útočníka je, získat si u uživatele tímto stylem psaní důvěru a přimět ho k určité akci (například k otevření zavirované přílohy, kterou v textu vydává za fakturu). Kontext zprávy může být založen na pravdě, ale není to podmínkou.

Jedna z forem pretextingu je založena na častém opakování některého ze slov. Pokud například útočník v e-mailu několikrát zmíní, že v příloze je faktura nebo se na ni jiným způsobem často odkazuje (třeba informací, že je nutné ji uhradit, že je v její hlavičce umístěn bankovní účet, na který má být zaslána platba apod.), může být uživatel přesvědčen, že je v příloze opravdu faktura [29].

Dalším konkrétním příkladem je e-mail s prosbou o finanční pomoc nigerijskému astronautovi, který se „ztratil“ ve vesmíru [27]. Kontext e-mailu je založen na reálných informacích (například název kosmické lodi), které mají uživatele přesvědčit o důvěryhodnosti celého sdělení. Vyjma toho útočník samozřejmě uživateli slibuje nemalé procento z celkové částky.

Útočník ale může v kontextu zprávy použít i zmíněné nepravdivé informace. Například se může ve svém sdělení odkazovat na neexistující univerzitu, aby vzbudil dojem vzdělanosti.

3 Phishing

Phishing je jeden ze způsobů, jakým z uživatele získat důvěrné informace (ať už jeho vlastní nebo někoho jiného) za pomoci metod sociálního inženýrství [3, 29]. Phishing lze v podstatě přirovnat k velkému kobercovému náletu, který sice během své cesty způsobí mnoho problémů administrátorům, ale zároveň existuje velká pravděpodobnost, že se v každé phishingové kampani najde dost obětí, které zprávě uvěří [27].

Označení phishing vychází z anglického termínu *password harvesting* [3], respektive anglického spojení *fish for password* [15]. Nemusí se ovšem jednat jen o sbírání přihlašovacích údajů, jak by se mohlo ze zmíněných termínů zdát, ale i o sbírání dalších, mnohem citlivějších údajů (osobní údaje o uživateli, jeho kreditní kartě apod.). Další pojem, se kterou má phishing souvislost, je anglický termín *phreaking* [15]. To je způsob, který se používal především dříve k napojování do telefonních systémů za účelem vedení bezplatných hovorů, odposlouchávání nebo narušování telefonních služeb [25]. Právě z termínu *phreaking* jsou převzaty první dva znaky `ph`, které nahrazují písmeno `f` ve slově *fish* [15]. Tímto nahrazením vznikne spojení *phish for password*, zkráceně *phishing* [15].

Většina phishingových útoků cílí na e-mailové schránky uživatelů, a to především z důvodu jednoduchosti takového útoku a velkého množství potenciálních obětí. S podvodnými zprávami tohoto druhu je nicméně možné se setkat i v jiných komunikačních kanálech – ve formě SMS, v instant messagingu apod. [18] Důvod, proč je phishing realizován především formou e-mailu je i ten, že je veřejně na internetu k dispozici obrovské množství sesbíraných e-mailových adres, které buď unikly z databází nebo byly automaticky posbírány například z internetových diskuzí (ověřit, zda byla e-mailová adresa součástí některého ze známých úniků, umožňuje například služba `https://haveibeenpwned.com`, popř. je možné zkusit zadat e-mail do vyhledávače a filtrovat získané výsledky pouze na záznamy pocházející ze stránek `https://pastebin.com` [31]).

3.1 Druhy phishingu

Phishing je závislý na zpětné aktivitě od uživatele, ke které je donucen metodami sociálního inženýrství. V praxi je možné se setkat se třemi základními typy phishingu [3].

3.1.1 Přímé vyžádání osobních údajů

Jedná se o nejjednodušší a nejstarší formu phishingu spočívající v tom, že oběť útočníkovi dobrovolně odešle své osobní údaje odpovědí na phishingový e-mail [19].

Uživatel může tento druh phishingu poznat na základě toho, že útočník si od uživatele přímo vyžádá zaslání konkrétních přihlašovacích nebo jiných citlivých údajů. Útočník v obsahu e-mailu samozřejmě použije ještě některé z metod sociálního inženýrství (viz kapitola 2.1), aby uživatele donutil k zaslání těchto údajů.

3.1.2 Phishing obsahující infikovanou přílohu

Útočník se v tomto typu phishingu snaží přesvědčit uživatele k otevření přiloženého infikovaného souboru. V obsahu e-mailu může na soubor navíc slovně odkazovat, a tedy uživatele donutit k tomu, aby soubor otevřel (viz kapitola 2.1.7). Uživatel může soubor otevřít i ze zvědavosti nebo v domnění toho, že se v něm nachází více podrobností (například detaily k zaplacení faktury).

Uživatel může odhalit tento způsob útoku na základě přípony souboru (viz kapitola 3.2.4). Pokud je uživateli doručen e-mail a v příloze má být jen faktura nebo jiný dokument, přičemž přiložený soubor je spustitelného typu (v operačním systému *Microsoft Windows* přípona `.exe`) nebo se jedná například o archiv (přípony `.zip`, `.rar`, `.tar` apod.) nebo dokonce o skript, je velká pravděpodobnost, že jde o phishing.

Útočník může navíc infikovanou přílohu (resp. archiv) zaheslovat a znemožnit antivirovému programu provést automatickou kontrolu. Heslo pro jeho otevření pak umístí do e-mailu a vydává ho jako „zabezpečení přenášené přílohy“.

3.1.3 Podvodná (podvržená) webová stránka

Cílem tohoto typu phishingu je přimět uživatele k návštěvě podvodné webové stránky, která ho má nějakým způsobem poškodit [19]. Uživatel se s tímto typem phishingu může nejčastěji setkat u hypertextových odkazů v e-mailové komunikaci. Na podvodné stránky se přesto může uživatel dostat i z jiných zdrojů – například z odkazu uvedeného ve vyhledávači, v komentářích (které může přidat kdokoliv včetně robota) na důvěryhodných stránkách, na sociálních sítích apod. Vzhled podvodné stránky pro důvěryhodnost zpravidla odpovídá nebo se aspoň blíží vzhledu originálních webových stránek.

Konkrétně obsah e-mailu může kopírovat typické zprávy od různých služeb – žádost o změnu hesla, žádost o zaplacení předplatného (tzv. subscription) k nějaké službě aj. Útočník spoléhá na to, že uživatel bude automaticky následovat odkazy umístěné v e-mailu (popř. ve vyhledávači nebo jinde), aniž by se nějak zabýval tím, kam opravdu vedou (více v kapitole 3.4). Uživatel se tak po kliknutí na odkaz dostane na útočníkem vytvořené podvodné stránky. Základním prvkem podvodných stránek je formulář, pomocí kterého útočník sbírá uživatelem zadané údaje, nebo závadná příloha, kterou si má uživatel stáhnout a spustit na svém zařízení. Kopírováním vzhledu pravých webových stránek (záleží na propracovanosti takového phishingu) může být navíc oběť přesvědčena o jejich pravosti.

Tento druh phishingu už ovšem vyžaduje, že útočníkem vytvořené podvodné stránky budou někde provozovány. S tím souvisí, že útočník musí pro realizaci tohoto phishingu získat doménu (nebo veřejnou IP adresu), pod kterou budou stránky přístupné – buď jejím pronájmem, nebo zneužitím již existující domény (například zjištěním přístupových údajů k DNS (*Domain Name System*) záznamům domény a jejich změnou). Útočník ale může pro provoz podvodné stránky zneužít i existující důvěryhodný web. Stačí, aby zdrojový kód důvěryhodného webu obsahoval bezpečnostní chybu, kterou útočník zneužije. Typicky se jedná o napadené redakční systémy (*WordPress*, *Joomla* apod.), které jsou nasazeny na celé řadě webových stránek. Útočník zneužije zranitelnosti v některé z verzí takového systému, zjistí si weby, na kterých běží stejná verze redakčního systému a napadne je. Útočník počítá s tím, že web se jednou nasadí a z hlediska bezpečnosti neaktualizuje. Případně se útočník do systému dostane zjištěním hesla uživatele (např. otestováním výchozí kombinace uživatelského jména a hesla nebo hrubou silou). Stejně tak může útočník vyzkoušet automaticky vkládat skripty například do komentářů pod články, fotografiemi apod. a spoléhat, že vstup není ošetřen a vložený skript se po načtení stránky komukoliv spustí (útok XSS – *Cross-site Scripting*). Útočník na takto napadeném webu může buď provést přesměrování na vlastní podvodné stránky (došlo by ale ke změně URL adresy, čehož by si mohl uživatel všimnout), nebo stačí, pokud původní obsah důvěryhodné stránky překryje vlastním obsahem po celé šířce i výšce webu (např. rámem, HTML tag `<iframe>`). Uživatel bude stále na důvěryhodné stránce i doméně (v URL adrese se nic nezmění), přičemž obsah originální stránky bude překryt obsahem dodaným od útočníka. Proti tomuto útoku se vývojáři webových stránek mohou bránit správným nastavením bezpečnostních HTTP hlaviček (např. hlavičkami `Content-Security-Policy (CSP)` a `X-Frame-Options` [13]). Pokud útočník pro umístění podvodných stránek nezneužije již existující web, musí získat jiný server, na kterém budou

podvodné stránky hostovány. Je vhodné, aby takových serverů bylo vícero.

V případě, že by podvodné stránky (IP adresu) někdo nahlásil, útočník (resp. automatický nástroj) jen vyřadí tuto IP adresu ze seznamu `A` záznamů DNS domény, protože byla kompromitována. A vzhledem k tomu, že takových záznamů (serverů) bude mít útočník u podvodné stránky několik, pravděpodobně nedojde zablokováním jedné IP adresy k odstavení celé podvodné stránky. Útočníci pro jistotu ještě využívají velmi krátké TTL (*Time To Live*) pro `A` záznam domény, aby se změna na DNS serverech projevila co nejdříve a podvodná stránka byla neustále k dispozici (tato technika se označuje jako *fast flux*) [1, 9]. V souvislosti s tím navíc tato technika ztěžuje zpětné dohledávání návštěv podvodného webu v provozních a lokalizačních údajích (z důvodu, že IP adresa je známa jen po krátkou dobu do minulosti, např. po dobu 5 minut).

3.2 Znaky phishingu

V současné době neexistuje univerzální způsob, podle kterého by se dalo strojovým zpracováním rozpoznat phishingový e-mail [29]. Člověk ale může většinu rozesílaných běžných phishingových zpráv odhalit na základě několika typických znaků, které vyplývají z obsahu takové zprávy.

3.2.1 Podezřelý odesílatel

První, co by si měl uživatel před čtením obsahu zprávy ověřit, je jméno a název e-mailu odesílatele. V běžných phishingových útocích buď tyto dvě hodnoty vůbec nesouvisí, nebo jsou přinejmenším velmi podezřelé (například volbou jména, kombinací s doménou, náhodnými znaky za jménem apod.) [29]. Případně může uživatel v poli odesílatel nalézt i svůj vlastní e-mail.

Není to ovšem kontrola, na základě které lze rozhodnout, že se nejedná o phishing. Ten může být zaslán i z pravého e-mailu z důvodu napadení dané schránky útočníkem. Případně může útočník zfalšovat hlavičku e-mailu a zprávy pod tímto e-mailem zasílat pomocí skriptu – například ve skriptovacím jazyce PHP (*Hypertext Preprocessor*) pomocí funkce `mail(·)` nebo stejnojmenným příkazem z terminálu v operačním systému *Linux* – pokud nejsou na straně e-mailového serveru implementovány technologie SPF (*Sender Policy Framework*) a DKIM (*DomainKeys Identified Mail*). Jistotu, že daný e-mail odeslal vyplněný odesílatel, tak poskytuje jen elektronický podpis [29].

3.2.2 Obsah

Dalším ze znaků, na základě kterého může uživatel označit zprávu za phishing, je obsah samotný. Ten nemusí být vůbec relevantní. Uživatel by tak měl zvážit, zdali má důvod reagovat na e-mail od neznámého člověka, na e-mail s neočekávaným druhem zprávy (například se zaslaným životopisem, který v rámci své pracovní pozice od nikoho nepožadoval [29]), nebo od služby, do které se nikdy neregistroval.

Některé z phishingových e-mailů mohou svým obsahem připomínat například seznamku s vlastnostmi ideálních partnerů a žádostí o navázání vztahu s uživatelem (resp. uživatelkou). Takový e-mail je většinou pro důvěryhodnost opatřen i odpovídající atraktivní fotografií protějšku [29]. Známy jsou nicméně i případy, kdy útočník jako důkaz své identity použil zfalšovaný řidičský průkaz či pas [27].

3.2.3 Jazyk použitý v e-mailu a jeho úroveň

Uživatel by měl brát ohled i na jazyk použitý v e-mailu. V případě, že dostane e-mail od české instituce, neočekává se, že by jeho obsah byl v angličtině nebo v jiném cizím jazyce [29].

Phishing cílící konkrétně na české uživatele navíc často obsahuje strojový překlad češtiny, což je následně znát na slovosledu, skloňování a časování, případně může obsahovat chyby v diakritice. Lze se ale setkat i s texty, které jsou naprosto bezchybné, a pro uživatele tak těžko odhalitelné [19].

3.2.4 Podezřelá příloha

Cílem infikované přílohy je nainstalovat do uživatelova počítače útočníkův program (tzv. *malware*) nebo provést v operačním systému akci, která bude uživatele poškozovat.

Chování takového programu může spočívat například v odesílání veškerých dat zadaných uživatelem na klávesnici na útočníkův server (jedná se o tzv. *keylogger*). Případně je možné zneužít zařízení k zapojení do *botnet* sítě (například pro rozesílání dalších phishingových zpráv), k těžbě kryptoměn apod. (uživatel si poklesu výkonu svého zařízení o cca 10 % nemusí vůbec všimnout [27]).

Potenciálně nebezpečnou přílohu lze odhalit na základě přípony takového souboru. Jestliže uživatel očekává v příloze textový dokument a je mu dodán spustitelný binární soubor nebo skript, lze s velkou pravděpodobností prohlásit, že se jedná phishing. V tomto směru uživatelům příliš

nepomáhá konkrétně operační systém *Microsoft Windows*, neboť ve výchozím stavu informaci o příponách souborů automaticky skrývá [10]. A právě automatického skrývání přípon souborů často zneužívají útočníci. Infikovaný spustitelný soubor například pojmenují `faktura.doc.exe`, nastaví mu odpovídající ikonu, kterou uživatel důvěrně zná a uživateli se na základě pravidla o skrývání přípon souborů zobrazí na první pohled důvěryhodný textový soubor `faktura.doc`.

Útočník ovšem může využít i uživatelům známý soubor s příponou PDF (*Portable Document Format*), který sice bude obsahovat relevantní informace, ale po svém otevření bude po uživateli vyžadovat spuštění skriptu útočníka [29]. Stejné skripty mohou být také umístěny v makrech běžně používaných dokumentů (tj. souborů vytvořených v programech kancelářského balíku *Microsoft Office* nebo *LibreOffice*).

3.2.5 Čas odeslání zprávy

Jedním z pomocných parametrů může být i čas odeslání zprávy – například u e-mailů od úředníka se typicky neočekává, že budou odesílány během hluboké noci [30] (pokud se nejedná o zprávy automaticky generované systémem).

3.2.6 Jiné informace

Uživatelům velmi nahrává fakt, že útočník s velkou pravděpodobností nebude mít tak detailní znalost uživatelova okolí. To jsou informace, které sice mohou vypadat obyčejně a nedůležitě, v kontextu zprávy ale mají při odhalování podvodu významnou roli. Uživatel je totiž ten, který nejlépe ví, s kým si dopisuje, od koho může očekávat jakou zprávu nebo dokonce zná způsob písemného vyjadřování nejbližších kontaktů. V případě firemního prostředí pak pracovní pozice některých zaměstnanců, umístění a označení významnějších místností v budově apod.

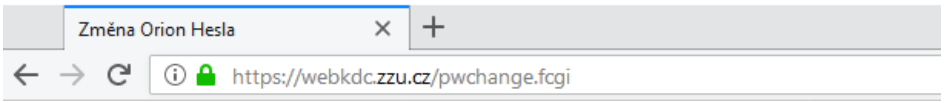
Jestliže například dosud uživatel ve firmě dostával určité e-maily od jedné kolegyně, která měla danou věc na starost a náhle dostal stejný, nebo podobný e-mail od jiné osoby, měl by si ověřit, zda nejde o podvod. Stejně tak je velmi podezřelé, pokud uživateli přijde nová žádost o změnu hesla, přičemž stejná žádost přišla relativně nedávno a heslo si uživatel úspěšně změnil.

3.3 Rozpoznání podvodného webu

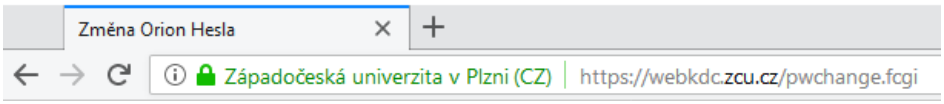
Vzhledem k tomu, že útočníci k získání citlivých údajů nepoužívají pouze zprávy zasílané přes e-mail, ale cíleně vytváří i podvodné webové stránky, na kterých se rovněž snaží uživatele nějakým způsobem poškodit, měl by si tohoto faktu být vědom i uživatel a být schopen takový web rozpoznat.

Uživatel si podvodné stránky může všimnout především pečlivou kontrolou URL (*Uniform Resource Locator*) adresy (více v kapitole 3.4). Dále by si měl uživatel ověřit, zda stránka běží na zabezpečeném protokolu HTTPS (*Hypertext Transfer Protocol Secure*), není to ovšem záruka bezpečí, viz následující odstavec. Pak už záleží jen na samotném uživateli, zdali obsah stránky odpovídá tomu, co opravdu požadoval. Pokud není některá z těchto podmínek splněna, je možné, že se jedná buď o podvod, nebo o méně důležité stránky provozované laiky (v případě absence HTTPS). Uživatelům i mírně pomáhají nejnovější verze některých webových prohlížečů, které je upozorní na případ, kdy se snaží zadat přihlašovací údaje na nezabezpečeném protokolu HTTP (*Hypertext Transfer Protocol*). Data zaslaná HTTP protokolem navíc může kdokoliv odchytit, nejen tvůrce podvodných stránek.

Nicméně ani HTTPS spojení nezaručí, že se uživatel nenachází na podvodné webové stránce. Webové stránky mohou být zabezpečeny nedůvěryhodným certifikátem (tzn. certifikátem, který si útočník mohl vydat sám a neschválila ho žádná důvěryhodná autorita). V takovém případě se uživateli ve webovém prohlížeči zobrazí varovná zpráva, podle které by na stránku neměl pokračovat. Útočník si ale může nechat zadarmo vystavit i důvěryhodný certifikát (například od certifikační autority *Let's Encrypt*) a implementovat ho na podvodný web. Uživateli je pak daná stránka ve webovém prohlížeči například zeleně zvýrazněna, čímž může uživatel nabýt falešného pocitu bezpečí (viz obr. 3.1). Jen v roce 2018 mělo cca 35 % podvodných phishingových stránek implementováno právě důvěryhodný certifikát [20]. V připravovaných nových verzích některých webových prohlížečů tak bude HTTPS bráno jako standard a důvěryhodně budou zvýrazňovány pouze weby, na kterých bude nasazen nejvyšší EV (*Extended Validation Certificate*) certifikát [4] (tj. důkladné prověření identity žadatele [23], viz obr. 3.2), zatímco weby běžící na protokolu HTTP budou označovány jako nebezpečné [14].



Obrázek 3.1: Podvodná webová stránka pro změnu hesla (URL adresa obsahuje `zzu.cz` místo `zcu.cz`) s nasazeným důvěryhodným certifikátem nižší úrovně (pozn. nejedná se o reálně šířený podvod, ale o funkční ukázku připravenou autorem práce)



Obrázek 3.2: Pravá webová stránka pro změnu hesla s nasazeným nejvyšším EV certifikátem (v adresním řádku se navíc zobrazuje jméno držitele domény, resp. certifikátu)

3.4 Manipulace s URL

Podvodné webové stránky (viz kapitola 3.1.3) jsou často umístěny na adresách, které využívají techniky záměny podobných znaků a možnosti rozkladu stromové struktury URL adresy. Cílem je, aby si uživatel myslel, že je na originální stránce. Útočník se tedy snaží, aby URL adresa připadala uživateli věrohodná, protože právě na základě ní může uživatel zjistit, zda se jedná o podvod (záleží na propracovanosti útoku, některé adresy se mohou absolutně lišit od originálních URL adres).

Uživatelé tak často chybují v tom, že originální název domény (např. `zcu.cz`) očekávají kdekoliv v URL adrese. Slepě tak důvěřují například náhodně generovaným doménám jako `http://zcu.cz.oiefwe2w4eff.com`, i přesto, že doména 2. řádu cílí na úplně jinou webovou stránku a s doménou `zcu.cz` nemá společného vůbec nic. Správným rozborem a vizuální kontrolou URL adresy by uživatelé vyloučili velké množství těchto podvodných stránek [19] (podvržené DNS servery nebo například pozměněný `hosts` soubor běžný uživatel již těžko odhalí, a navíc by útočník musel svůj útok konkretizovat na daného uživatele, což není primárním cílem phishingu). Rozbor jednotlivých částí pro konkrétní URL adresu (viz obr. 3.3) je popsán v tab. 3.1.

```
https://webkdc.zcu.cz/pass/pwchange.fcgi?action=cp&a=256
```

Obrázek 3.3: Typická URL adresa včetně parametrů (rozbor URL adresy je uveden v tab. 3.1)

Část URL adresy	Význam řetězce
`https`	protokol
`webkdc`	doména 3. řádu (subdoména)
`zcu`	doména 2. řádu
`cz`	doména 1. řádu – TLD (*Top Level Domain*) doména
`pass`	cesta (adresář)
`pwchange.fcgi`	soubor
`?action=cp&a=256`	parametry skriptu

Tabulka 3.1: Význam jednotlivých částí URL adresy uvedené na obr. 3.3

Jedna z technik pro rozpoznání podvodných URL stránek ve phishingových e-mailech je založena na počtu zanoření v adrese. Čím více částí (tzv. *labels* – domén jednotlivých řádů) oddělených tečkou adresa obsahuje, tím je pravděpodobnější, že se útočník snaží v hlubokém zanoření stromové struktury něco skrýt [28]. Většina webových prohlížečů navíc automaticky testuje (popř. v rámci nějakého doplňku), zdali je navštívená stránka na některém z blacklistů (tj. seznamu podvodných a nebezpečných stránek) a varuje uživatele před její případnou návštěvou. Některé uživatele nicméně nezastaví ani tato případná upozornění [27], zvlášť, když jim takový e-mail přijde od blízké osoby nebo vyšší autority.

3.4.1 Záměna znaků v doméně

V případě, že se útočník snaží co nejvíce přiblížit originální URL adrese, aby zmátl i pozorného uživatele, využije nejčastěji záměny podobných znaků v doméně webu.

Typickým příkladem je náhrada l (malého písmena L) za 1 (jedničku), nebo I (velké písmeno i). Dalším příkladem může být i kombinace dvou znaků, které v některém z fontů mohou při vykreslení vypadat jako jeden znak [21]. Například v adrese `seznarn.cz` tak bylo písmeno m vyměněno za písmena rn. Méně pozorný uživatel si této změny nemusí všimnout (zvlášť u proporcionálního písma a na displejích s vysokým rozlišením na malé úhlopříčce v kombinaci s nastavením hodnoty DPI (*Dots Per Inch*) na 100 %).

3.4.2 IDN homograph attack

Jako IDN (*Internationalized Domain Names*) je označována doména, která obsahuje znaky některé národní abecedy (v případě češtiny háčky a čárky) [5]. Bylo by tak možné si například zaregistrovat doménu `zču.cz`, jejíž IDN tvar

(tzv. *punycode* [22]) by byl `xn-zu-ema.cz`. V adresním řádku webového prohlížeče se ovšem uživateli zobrazí pouze `zču.cz`. V době psaní práce ale nejsou při registraci české národní domény `.cz` tyto možnosti povoleny [5]. U některých jiných národních domén to ale možné je.

Útočníci v tomto útoku zneužívají některé znaky z jiných národních abeced, které po vykreslení vypadají téměř podobně, nebo dokonce stejně, jako znaky v latince (záleží na použitém písmu a jeho řezu). Doména tak může obsahovat například některý ze znaků cyrilice, který v adresním řádku webového prohlížeče bude vypadat stejně jako příslušný znak z latinky. Uživatel tak prakticky nemá možnost vizuální kontrolou z adresního řádku zjistit, zdali se nachází na podvodné nebo pravé webové stránce. Stejné to je i s některými speciálními netisknutelnými znaky, které sice v URL adrese formálně jsou, ale font je nevykreslí [21]. Přehled potenciálně zneužitelných homomorfismů ukazuje dokument [6].

Příkladem může být doména `zcu.cz`, kde je ale původní znak `c` (z latinky) nahrazen jiným malým znakem `c`, ovšem z cyrilice. Pokud by si uživatel zjistil IDN tvar této domény, dostal byl `xn-zu-omc.cz`, který s pravou doménou `zcu.cz` nemá vůbec nic společného.

4 Existující řešení pro zasílání cvičných phishingových zpráv

Vzhledem k tomu, že phishing je v dnešní době velkou hrozbou nejen pro jednotlivce, ale i pro instituce (jak bylo zmíněno v úvodu práce), existuje několik softwarových řešení pro zasílání cvičných phishingových zpráv.

Je třeba zmínit, že ale ani jedno z existujících řešení nesplňuje požadavky nebo nemá funkce, které vyžaduje bezpečnostní tým WIRT na ZČU. Některá existující řešení jsou navíc poměrně finančně nákladná, protože cenu za produkt stanovují podle počtu uživatelů v organizaci, což v případě počtu uživatelů na ZČU není zanedbatelná částka.

Dosud rozesílání cvičných podvodných zpráv probíhalo tak, že nejprve došlo k manuálnímu importu zvolených příjemců do programu, který zabezpečoval samotné rozeslání e-mailů. Dalším programem pak bylo nutné provést analýzu a zhodnocení získaných dat. Systém vzniklý z této práce by měl tyto kroky integrovat a automatizovat do jednoho řešení, které bude navíc obsahovat i další dodatečné funkce požadované prostředím univerzity.

V následujících podkapitolách budou stručně popsány dvě existující řešení, které se v rámci základních funkcí podobají výslednému systému vzešlého z této práce.

4.1 GoPhish

Jedná o *open-source* řešení, které administrátorovi umožňuje v jednoduchém webovém rozhraní vytvářet cvičné phishingové kampaně. *GoPhish* je vyvíjen pro operační systémy *Linux*, *Microsoft Windows* a *macOS* (ve všech třech případech jak v 32bitové, tak 64bitové verzi). Instalace je velmi jednoduchá a v podstatě jen stačí spustit stažený binární soubor, který spustí server (popřípadě je předtím možné upravit konfigurační soubor).

V rámci softwaru je možné založit podvodné stránky, na které se uživatel může dostat skrz zaslané e-maily, přičemž je sledováno, zdali byl e-mail úspěšně odeslán, jestli jej uživatel otevřel (na základě zobrazení sledovacího obrázku), kliknul na uvedený odkaz, případně zdali vyplnil nějaká data do formuláře na podvodné stránce. Software rovněž umožňuje do zasílaných

e-mailů vkládat i přílohy.

Registraci příjemců cvičných podvodných zpráv musí provádět administrátor, který v každé založené kampani specifikuje skupinu příjemců. Příjemci zpráv nemají žádnou zpětnou vazbu o tom, jestli byli součástí nějakého testu nebo jaký je jejich výsledek v rámci kampaní, do kterých byli registrováni (pokud jim to sám administrátor nesdělí jiným způsobem).

Získaná data z provedených phishingových kampaní je možné exportovat do formátu CSV (*Comma-separated Values*).

Další detaily včetně dokumentace jsou uvedeny na webových stránkách programu `https://getgophish.com`.

4.2 Phishing Frenzy

Phishing Frenzy šířený pod licencí *open-source* je software, který administrátorovi poskytuje, stejně jako *GoPhish* popsaný v bodě 4.1, webové rozhraní k vytváření cvičných phishingových kampaní. Program je dostupný pro operační systém *Linux* a jeho instalace není tak triviální jako v případě *GoPhish*.

Webové rozhraní umožňuje používat předpřipravené šablony podvodných webových stránek (například formulář k přihlášení do *Microsoft Office 365*, do sociální sítě *LinkedIn* apod.), ale vytvářet i šablony zcela nové, ke kterým se uživatel dostane z rozesílaných e-mailů. Software na podvodných stránkách vyjma zadávaných údajů navíc zaznamenává IP adresu uživatele (pro následnou geolokaci ve statistice) a otisk použitého webového prohlížeče (tzv. *browser fingerprint*). Zároveň je možné do podvodné stránky umístit i kód frameworku BeEF (*The Browser Exploitation Framework*), který umožňuje útočníkovi řízeně ze serveru provádět na klientském zařízení řadu možných útoků, resp. zneužívat známé zranitelnosti použitého webového prohlížeče [11].

Každá z kampaní obsahuje statistiku s nasbíranými údaji o uživatelích (viz předchozí odstavec) a datech, která uživatelé vyplnili do formuláře. Data získaná z těchto kampaní lze exportovat do formátu XML (*Extensible Markup Language*) a PDF.

Registraci příjemců cvičného phishingu musí stejně jako v případě *GoPhish* provádět administrátor. Rovněž nejsou uživatelé žádným způsobem informováni o tom, že byli součástí testu nebo informací o jeho výsledku.

Další podrobnosti o programu je možné společně s dokumentací nalézt na webových stránkách `https://www.phishingfrenzy.com`.

5 Implementace aplikace

Protože ani jedno z existujících řešení popisovaných v předešlé 4. kapitole nesplňuje požadavky a nemá funkce požadované univerzitou, bylo přistoupeno k návrhu nového systému.

Cílem bylo, aby systém usnadnil práci administrátorům, kteří tak budou schopni během několika minut vytvořit novou cvičnou phishingovou kampaň, v níž si jednoduše zvolí, jaký phishingový e-mail bude rozesílán, jaká podvodná stránka bude z e-mailu přístupná a jakým příjemcům e-mail dorazí, přičemž o vše ostatní se již postará vytvořená aplikace.

Do aplikace ale budou mít přístup i běžní uživatelé, kterým nabídne možnost se dobrovolně přihlásit k odebírání cvičných phishingových zpráv, díky které se budou moci v problematice phishingu vzdělávat (viz dále v podkapitole 5.4).

5.1 Architektura aplikace

Aplikace byla navržena v třívrstvé *model–view–controller* (MVC) architektuře, jejíž základní myšlenkou je oddělit logiku aplikace od výstupu, a to rozdělením aplikace do následujících vrstev (informace a popis vrstev vychází ze zdroje [7]):

- `Models` – třídy obsahující logiku aplikace, práci s daty, databází apod.
- `Controllers` – třídy, které obsluhují příchozí požadavky uživatele a fungují jako prostředník, se kterým komunikuje uživatel a ostatní vrstvy
- `Views` – šablony pro výstup aplikace, které vypisují obsah uživateli

Zvolená architektura webové aplikace byla implementována ve skriptovacím jazyce PHP.

Výjimku, kde není využito výhod architektury MVC, tvoří úvodní stránka projektu, která je až na detaily statická a slouží jen k zobrazení informací o projektu a navedení uživatele na přihlašovací stránku do systému.

Druhou výjimkou jsou podvodné stránky, které se obvykle skládají z jednoho vstupního souboru (resp. `index.php`) s HTML kódem formuláře a CSS souboru, popř. obrázků zobrazovaných na stránce. Protože bylo cílem, aby přidání podvodných stránek bylo co nejjednodušší a nebylo nutné důkladně znát architekturu aplikace, rozdělení jednoho vstupního souboru do několika vrstev by nedávalo smysl.

5.2 Použité technologie

Aplikace ke svému běhu používá následující knihovny třetích stran, které jsou nutné pro její správné vykreslení a bezproblémový běh:

- *Bootstrap 4.1.3* (společně s *Popper.js*) – front-end framework (viz kapitola 7)
- *jQuery 3.3.1 (slim build)* – nadstavba pro *JavaScript*, kterou vyžadují ostatní použité knihovny
- *Feather v4.21.0* – knihovna obsahující grafické SVG (*Scalable Vector Graphics*) ikonky
- *Chart.js v2.8.0* – knihovna pro vykreslování grafů
- *jQuery highlightTextarea 3.1.3* – knihovna pro zvýrazňování vlastní syntaxe v HTML tagu `<textarea>` a tagu `<input>` (v aplikaci použito pro vyznačování proměnných u phishingových e-mailů)

Všechny knihovny jsou umístěny v adresáři `public/extensions`, aby nebylo nutné odkazovat na externí zdroje, u kterých není zaručena jistota dostupnosti.

Z hlediska serverových technologií, které jsou nutné pro běh aplikace, se jedná o následující seznam:

- *PHP* – interpret jazyka PHP s následujícími moduly, které nemusí být součástí původní instalace: `php-mysql`, `php-mbstring` (pro multibyte funkce PHP, resp. pro potřeby diakritiky českého jazyka)
- *PHPMailer 6.0.7* – knihovna pro zasílání e-mailů v jazyce PHP s pokročilými možnostmi, které standardní funkce `mail(·)` v PHP nenabízí
- *MySQL (MariaDB)* – databázový systém
- *Apache* – webový server
- *WebAuth* – systém sloužící k autentizaci uživatelů při přihlašování do aplikace (v rámci modulu `mod_webauth` pro *Apache*)
- *Kerberos* – systém pro ověřování správnosti přihlašovacích údajů zadaných uživateli na podvodných webových stránkách
- *e-mailový server* – nutno nastavit v případě, že požadavky na odesílání cvičných phishingových zpráv nebude odbavovat jiný, nadřazený poštovní server (v rámci této práce požadavky zpracovával poštovní server ZČU)

- *Certbot* – software, který umožňuje automaticky vydávat a prodlužovat certifikáty podepsané důvěryhodnou certifikační autoritou *Let's Encrypt* určené pro webové stránky (není povinné, pokud není vyžadován důvěryhodný certifikát na podvodných stránkách, popř. lze nahradit jiným existujícím řešením)

5.3 Podstatné části aplikace

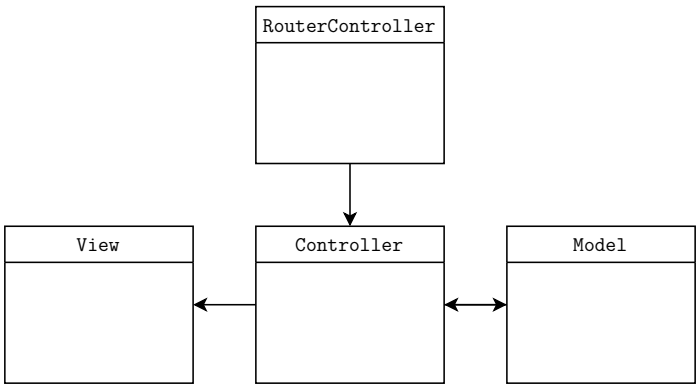
V následujících podkapitolách budou zmíněny významné třídy a soubory, které jsou používány napříč celou aplikací a které lze považovat za jádro celého systému.

5.3.1 Třída `RouterController`

Třída řeší zpracování požadavků ze strany uživatele, na základě kterých aplikaci informuje o tom, jaký konkrétní `Controller` má načíst (viz podkapitola 5.3.2). Požadavky pak přesměruje na vybraný `Controller` (pokud existuje).

5.3.2 Třída `Controller`

Třída `Controller` poskytuje všem svým potomkům atributy a metody, které by jinak bylo nutné po každé znovu implementovat. V podstatě každá ze sekcí systému představuje jeden `Controller`, který přijímá požadavky od uživatelů předaných ze třídy `RouterController` (viz podkapitola 5.3.1).



Obrázek 5.1: Navržená komunikace mezi jednotlivými vrstvami vytvořené webové aplikace

Po vytvoření nové instance této třídy v `RouterController` je jako první volána abstraktní metoda `process(·)`, které jsou předány požadavky ze

strany uživatele (tuto metodu je nutné v každém z potomků třídy implementovat). Zmíněná metoda obvykle analyzuje uživatelské argumenty a v případě očekávaných dat vytvoří novou instanci odpovídající třídy `Model`, která nejčastěji dědí své vlastnosti a metody ze třídy `FormModel` (viz podkapitola 5.3.4). Třídu `Model` poté žádá o odpovědi na otázky (resp. argumenty) uživatele a předává je dále do šablony, tzn. do `View` (viz obr. 5.1).

5.3.3 Třída pro obsluhu databáze

Požadavky na databázi zpracovává třída `Database`. Pro spuštění SQL (*Structured Query Language*) dotazů nad databází není nutné psát v ostatních třídách opakující se kód (volání metody pro vykonání dotazu, dodání parametrů pro *prepared statements* apod.), ale stačí jen volat konkrétní metodu z této třídy v závislosti na tom, co je třeba v databázi provést a předat jí požadované parametry.

Aplikace se do databáze připojuje v rámci vrstvy PDO (*PHP Data Objects*).

5.3.4 Třída pro obsluhu formuláře

Všechny třídy aplikace, které zpracovávají data z formuláře, dědí atributy a metody od abstraktní třídy `FormModel`. Ta svým potomkům poskytuje metody, které by bylo nutné v každé z těchto tříd implementovat. Spolu s tím třída obsahuje abstraktní metodu `validateData()`, kterou je nutné v každé ze tříd implementovat a jejímž cílem je ověřit správnost uživatelského vstupu voláním dalších, jednoduchých (a tak snadno testovatelných) metod.

Třída řeší inicializaci formuláře, tedy např. zjištění maximálního počtu znaků, který lze do každého ze vstupních polí vložit (na základě atributů v databázi). Třída také obsahuje metodu `getInputsValues()`, která pro každé ze vstupních polí formuláře vrátí jeho ošetřený obsah (je-li nějaký k dispozici), a to buď ten uložený v HTTP POST, nebo z databáze (v závislosti na prováděné akci). Stejně tak obsahuje i metodu `load()`, která se pokusí vložit do atributů potomka třídy data zadaná ve formuláři pro další zpracování. V rámci této metody je prováděna i kontrola proti útoku CSRF (*Cross-site Request Forgery*, viz kapitola 8.4).

5.3.5 Obecné funkce

V rámci souboru `globalFunctions.php` je k dispozici řada funkcí, které jsou využívány napříč zdrojovým kódem aplikace a nemají tak příslušnost k nějaké konkrétní třídě.

5.3.6 Konfigurační soubor

Aplikace obsahuje v kořenovém adresáři soubor `config.php`, který shromažďuje konstanty a nastavení používaná v aplikaci.

Rámcově lze nastavit základní konfiguraci aplikace (tj. připojení k databázi, LDAP), úroveň logování systémových zpráv a další nastavení s logováním související, ale také výchozí možnosti uživatelů po registraci do systému (zda budou automaticky dobrovolně odběrateli cvičných phishingových zpráv a s jakým limitem), úroveň anonymizace hesel na podvodných stránkách nebo například názvy proměnných používaných ve phishingových e-mailech, seznam skupin uživatelů z LDAP, který bude k dispozici při vytváření/úpravě kampaně apod.

Popis každé z konstant je detailně uveden v komentářích ve zmíněném souboru.

5.4 Části aplikace

Uživatel má po přihlášení do aplikace k dispozici několik sekcí, a to podle toho, jaké je jeho oprávnění, přičemž oprávnění v systému mohou být následující:

- *administrátor* – nejvyšší oprávnění, na základě kterého má uživatel přístup do všech sekcí v systému (určeno pro členy bezpečnostního týmu WIRT)
- *správce testů* – umožňuje uživateli vytvářet vlastní kampaně či spravovat kampaně ostatních uživatelů, kteří jsou ve stejné skupině jako uživatel
  - každý *správce testů* je parametrizovatelný – *administrátor* může definovat, že daný *správce testů* bude moci vytvářet kampaně jen pro určitou množinu příjemců (oprávnění je určeno pro lokální správce IT na jednotlivých fakultách a pracovištích ZČU)
- *uživatel* – nejnižší oprávnění v systému, které je uživateli ve výchozím stavu přiděleno

Uživatelé s vyšším oprávněním (minimálně *správce testů*) navíc mohou přepínat mezi svým a všemi ostatními, nižšími oprávněními.

V následujících podkapitolách bude stručně popsáno, co podstatného je v dostupných sekcích řešeno a jaké minimální oprávnění je nutné pro vstup do dané sekce.

5.4.1 Úvodní stránka

Jedná se o první stránku, na kterou bude uživatel po úspěšném přihlášení přesměrován. Cílem je uživateli poskytnout souhrnné statistiky a grafy, které se ho týkají, a to v závislosti na jeho oprávnění.

Statistika se společně s legendou a daty pro grafy získává z metod dostupných ve třídě `StatsModel`.

5.4.2 Moje účast v programu

V této sekci má uživatel možnost se dobrovolně přihlásit k odebírání cvičných phishingových zpráv s volbou maximálního počtu e-mailů, které mu budou v budoucnu ještě odeslány (po každém odeslání e-mailu se tato hodnota dekrementuje, než dosáhne nuly). Limit a to, zdali chce uživatel dobrovolně zasílat cvičné podvodné e-maily je *administrátorovi* zobrazeno v seznamu uživatelů a v seznamu příjemců u kampaní.

Je třeba ovšem podotknout, že toto nastavení nemá vliv na to, pokud se *správce testů* nebo *administrátor* rozhodne uživateli e-mail poslat i tak (to je především z důvodu možnosti provést bezpečnostní audit či uživatele prověřit kvůli jeho podezřelým aktivitám).

Třída řešící správu tohoto nastavení se nazývá `ParticipationModel`.

5.4.3 Přijaté phishingové e-maily

Přihlášení uživatelé mají kromě své osobní statistiky dostupné na úvodní stránce (viz podkapitola 5.4.1) k dispozici i seznam všech phishingových e-mailů, které jim byly v minulosti zaslány. U každého e-mailu je uživateli poskytnut interaktivní seznam indicií včetně jejich označení v samotném e-mailu, a i informace o tom, jak na daný e-mail (popř. podvodnou stránku) reagoval, přičemž reakce uživatele mohou být následující:

1. *bez reakce* – e-mail byl uživateli doručen, ale na odkaz v něm uvedený a vedoucí na podvodnou stránku, neklikl
2. *návštěva stránky* – uživatel navštívil podvodnou stránku přístupnou z phishingového e-mailu, ale nic zde nevyplňoval
3. *zadání neplatných údajů* – uživatel do formuláře na podvodné stránce zadal neplatné přihlašovací údaje
4. *zadání platných údajů* – uživatel do formuláře na podvodné stránce zadal platné přihlašovací údaje

5.4.4 Kampaně

Cílem této sekce je vytvářet nové a upravovat stávající kampaně nebo umožnit nahlížet na statistiky a grafy právě běžících či už proběhlých kampaní. Oprávněný uživatel si tak u každé kampaně zvolí, jaký podvodný e-mail bude rozesílán, jaká podvodná webová stránka bude přístupná z rozesílaného e-mailu, co se stane po odeslání formuláře na podvodné stránce (k dispozici je pět různých možností), datum a čas startu a konce kampaně a konečně i seznam příjemců.

Do dané sekce mají přístup *správci testů* a *administrátoři*, přičemž *správce testů* má přístup jen ke kampaním, které vytvořil on sám nebo někdo ze stejné uživatelské skupiny.

Všechny operace týkající se správy kampaní zajišťuje třída `CampaignModel`.

Interaktivní výběr příjemců

Výběr příjemců kampaně je realizován pomocí dialogového okna, ve kterém jsou zobrazeni všichni potenciální příjemci včetně těch, které systém získal dotazem do univerzitní databáze LDAP (*Lightweight Directory Access Protocol*). Uživatel má možnost zaškrtnout pouze konkrétní příjemce a svůj výběr potvrdit, případně příjemce manuálně zadávat do vstupního pole (pokud se například nevyskytují v interaktivním seznamu příjemců z důvodu nadměrného počtu uživatelů univerzitní sítě). U *správců testů* může systém limitovat výběr jen na ty příjemce, kteří splňují požadavky skupiny uživatele (viz podkapitola 5.4.9).

Samotné přihlášení či odhlášení příjemců do kampaně nemá vliv na to, zdali se odebírání cvičných phishingových zpráv účastní dobrovolně či nikoliv. Dobrovolně registrovaní příjemci jsou pouze odlišeni jiným názvem kategorie v interaktivním seznamu potenciálních příjemců.

Přihlášení a odhlášení uživatelů do vybrané kampaně řeší metody třídy `CampaignModel`, totiž `insertRecipient(·)` a `unsignRecipient(·)`. Zatímco odhlášení uživatele do databáze pouze zapíše záznam o tom, že uživatel od zvoleného data již není příjemcem v dané kampani (viz podkapitola B.3), přihlášení příjemců je složitější v tom, že systém nejprve musí ověřit, zdali je daný uživatel zanesen v systému a pokud ne, provést jeho registraci na základě dat získaných z LDAP a teprve poté jej svázat s konkrétní kampaní.

Export zaznamenaných dat

Aby mohla být data zaznamenaná na podvodných stránkách dále zpracovávána mimo systém, umožňuje aplikace jejich export. Export zajišťují metody

umístěné ve třídě `StatsExportModel`.

Všechna zaznamenaná data lze u každé kampaně exportovat do formátu CSV ve dvou různých variantách. Obě varianty lze také exportovat zabalené v ZIP archivu (v takovém případě nejprve dojde k vytvoření CSV souborů v dočasném `temp` adresáři aplikace a poté k vytvoření archivu a smazání původních CSV souborů).

5.4.5 Podvodné e-maily

Sekce má na starost správu všech evidovaných phishingových zpráv. Uživatel systému (resp. pouze *administrátor*) může jednoduše vytvářet nové podvodné e-maily (či upravovat a mazat ty stávající), přičemž postupuje v podstatě úplně stejně, jako kdyby stejný e-mail vyplňoval v některém z e-mailových klientů. Před jakoukoliv úpravou má navíc uživatel možnost si e-mail prohlédnout v náhledu.

Všechny akce související s těmito podvodnými zprávami obstarává třída `PhishingEmailModel`. Tato třída obsahuje vyjma operací pro přidání, úpravu a smazání podvodného e-mailu i několik dalších, pomocných metod, které slouží například k personalizaci e-mailu, úpravě jeho formátování, označení indicií apod.

Personalizace podvodného e-mailu

Aby byl e-mail pro příjemce co nejvíce důvěryhodný, je umožněno v jeho těle používat několik proměnných, které jsou při odeslání e-mailu nahrazeny skutečným obsahem. Hlavní metoda, která personalizaci e-mailu řeší, se nazývá `personalizeEmailBody(·)`. Zmíněné proměnné jsou zároveň uvedeny i v konfiguračním souboru, kde je možné je případně upravit.

Seznam dostupných proměnných s informací o tom, za co budou nahrazeny, je následující:

- `%recipient_username%` – uživatelské jméno příjemce
- `%recipient_email%` – e-mail příjemce
- `%date_cz%` – datum, ve kterém dochází k odeslání e-mailu ve formátu `D. M. YYYY`
- `%date_en%` – datum, ve kterém dochází k odeslání e-mailu ve formátu `YYYY-MM-DD`

- `%url%` – povinná proměnná pro každý z e-mailů, která bude nahrazena za URL podvodné stránky svázané s e-mailem (metoda umožňuje specifikovat buď přesnou URL adresu, přes kterou může uživatel na podvodnou stránku přistoupit, nebo URL adresu bez sledovacího parametru určenou pro náhled e-mailu)

Proměnnou `%recipient_email%` lze používat i místo e-mailu odesílatele (e-mail příjemce i odesílatele bude poté identický), přičemž tuto personalizaci řeší metoda `personalizeEmailSender(·)`.

Označování indicií

Zvýrazňování indicií, na základě kterých lze rozpoznat phishing u konkrétního podvodného e-mailu řeší metoda `insertHTMLIndications(·)`. Metoda projde všechny části phishingového e-mailu (včetně odesílatele a předmětu) a vybrané pasáže zvýrazní a nastaví tak, aby mohly být provázány se seznamem všech indicií u daného e-mailu. To uživateli poskytuje možnost si každou z indicií v e-mailu zvýraznit či její zvýraznění deaktivovat. Metoda také aktivuje i případné kliknutí na konkrétní indicii, které uživatele navede na detailní popis indicie.

Rozesílání e-mailů

Rozeslání phishingových e-mailů řeší třída `EmailSenderModel`, resp. metoda `startSendingEmails()`.

Metoda zjistí, jaké kampaně jsou stále aktivní, dále zdali aktuální čas odpovídá času, kdy se mají v rámci této kampaně odesílat e-maily a teprve poté metoda projde všechny příjemce, kterým se má podvodný e-mail rozeslat. U každého příjemce navíc dojde k ověření, zdali už mu nebyl e-mail odeslán někdy v minulosti. Pokud tomu tak nebylo, dojde k nahrazení proměnných v e-mailu za skutečné hodnoty (případně k personalizaci) a k jeho odeslání pomocí externí třídy `PHPMailer`. V případě, že má příjemce nastaven limit zpráv, které si přeje do budoucna obdržet, tak dojde k jeho snížení.

Ve vytvořené aplikaci jsou e-maily rozesílány každých 5 minut, a to pomocí programu `cron`, který spouští soubor `mailSender.php`.

5.4.6 Indicie k rozpoznání phishingu

Cílem této sekce je, aby ke každému cvičnému podvodnému e-mailu existoval seznam indicií, na základě kterých mohl uživatel rozpoznat, že se jednalo o phishing.

Indicie k podvodným e-mailům přidává *administrátor* s tím, že uživatel si jejich seznam může u každého e-mailu, který obdržel, prohlédnout. *Administrátor* může v e-mailu označovat libovolné pasáže včetně jména a e-mailu odesílatele či předmětu e-mailu (na základě proměnných `%sender_name%`, `%sender_email%` a `%subject%` upravitelných v konf. souboru aplikace) a upozornit tak uživatele například na fakt, že pokud je v poli odesílatel uvedena osoba s vyšší autoritou, tak to ještě neznamená, že je daná osoba opravdu odesílatelem e-mailu (viz podkapitola 3.2.1 v teoretické části práce).

Správu indicií řeší třída `EmailIndicationsModel`.

5.4.7 Podvodné stránky

Podvodné stránky jsou samotnou zásadní kapitolou celého systému, a to především z toho důvodu, že je třeba provést zásah v konfiguraci webového serveru (už z tohoto hlediska má do sekce přístup jen *administrátor*). Vytvořená aplikace nicméně tuto konfiguraci uživateli dopředu automaticky připraví a jeho jediným úkolem je tak pouze nastavit rutinní kroky, jako směrování DNS záznamů podvodné domény na IP adresu vytvořené aplikace a uvést podvodnou stránku do provozu aktivováním příslušného konfiguračního souboru pro webový server.

Operace, které se musí při přidání nové podvodné stránky provést, jsou tedy následující:

1. nastavit odpovídající `A` záznam v DNS záznamech podvodné domény (popř. subdomény), na které bude provozována podvodná stránka tak, aby byl směrován na IP adresu, kde běží vytvořená webová aplikace pro rozesílání cvičných phishingových zpráv

2. přidat podvodnou stránku v sekci *Podvodné stránky*, která v umístění nastaveném v konfiguračním souboru aplikace vytvoří nový konfigurační soubor pro podvodnou stránku určený pro webový server (ten dané podvodné stránce nastavuje konkrétní `DocumentRoot`, tedy adresář, kde je umístěna šablona (vzhled) podvodné stránky a další parametry požadované pro svázání stránky s vytvořenou aplikací)

3. v konfiguraci webového serveru *Apache* aktivovat nový konfigurační soubor, resp. `VirtualHost`, který bude zachytávat požadavky na danou doménu/subdoménu

4. dle požadavků vydat důvěryhodný či nedůvěryhodný certifikát pro podvodnou stránku, nebo ji nechat běžet pouze na protokolu HTTP (v rámci aplikace řešeno programem *Certbot*, který automaticky vydá

důvěryhodný certifikát podepsaný certifikační autoritou *Let's Encrypt*) a tuto skutečnost nastavit v konfiguračním souboru daného `VirtualHost`

5. restartovat (resp. stačí volat příkaz `reload`) webový server *Apache* pro aplikování provedených změn

Po těchto krocích systém automaticky nad podvodnou stránkou (resp. konkrétní doménou/subdoménou) převezme kontrolu, a to pomocí speciální třídy `WebsitePrependerModel`.

Správu podvodných stránek včetně vytváření konfiguračních souborů pro webový server *Apache* řeší třída `PhishingWebsiteModel`.

Obsluha podvodné stránky

Přístupnost a obsluhu podvodné stránky řeší třída `WebsitePrependerModel`, která zabezpečuje, že daná podvodná stránka bude dostupná jen pro aktivní kampaň (těch může být vícero) a jen pro uživatele, kteří jsou příjemci dané kampaně. Ostatní nepovolené přístupy jsou směrovány na úvodní stránky systému. Spolu s tím třída zaznamenává jakoukoliv aktivitu na podvodné stránce, kterou následně ukládá do databáze (viz podkapitola B.4).

Třída také řeší to, jakým způsobem má podvodná stránka reagovat na vstup ze strany uživatele – tedy na to, co se stane po odeslání formuláře (tuto možnost si tvůrce kampaně zvolí při jejím vytváření). Možnosti jsou následující:

- *bez reakce* – po odeslání formuláře se bude stránka tvářit, že se nic nestalo
- *informace, že jde o test* – přesměrování na úvodní stránku aplikace s informací o tom, že uživatel právě absolvoval praktický phishingový test
- *přesměrování na skutečný WebAuth* – po odeslání formuláře bude uživatel přesměrován na pravou univerzitní stránku s přihlášením
- *zobrazit chybovou hlášku o nesprávných přihlašovacích údajích* – po odeslání formuláře se bude neustále zobrazovat hláška o nesprávně zadaných přihlašovacích údajích (i když byly zadány správně)
- *nechat uživatele dvakrát zadat přihlašovací údaje a po druhém zadání přesměrovat na pravý WebAuth* – kombinace předchozích možností

Podvodná stránka je navíc přístupná jen přes konkrétní odkaz, který je jedinečný pro každého příjemce kampaně a který je zároveň jedinečný i pro každou kampaň. Odkaz obsahuje parametr (tj. část za otazníkem, viz obr. 5.2), ze kterého aplikace dekóduje identifikátor kampaně a identifikátor příjemce. Stejný mechanismus s parametrem v URL adrese používají i reálné phishingové e-maily, ve kterých jsou uvedeny odkazy na podvodné stránky. Aby navíc identifikátor nebyl tak jasně dekódovatelný, je rozdělen na tři části, jak uvádí tab. 5.1.

```
https://webkdc.zzu.cz/?2fv3as3
```

Obrázek 5.2: URL adresa jedné z podvodných stránek včetně parametru, v němž je skryt identifikátor kampaně a uživatele (viz tab. 5.1)

parametr	**1. část ID uživatele**	**ID kampaně**	**2. část ID uživatele**
`2fv3as3`	`2fv`	`3`	`as3`

Tabulka 5.1: Dekódování identifikátoru kampaně a uživatele (pozn. identifikátor uživatele má vždy pevně stanovou délku) z parametru v URL adrese podvodné stránky uvedené na obr. 5.2

5.4.8 Uživatelé

Operace s uživateli lze provádět v sekci *Uživatelé*, do níž má přístup pouze uživatel s oprávněním *administrátor* (nejvyšší oprávnění).

Záznam o uživateli se v této sekci zobrazí tehdy, pokud platí některá z následujících podmínek:

- uživatel se do systému sám přihlásil přes přihlašovací formulář (resp. pomocí autentizační služby *WebAuth*)
- uživatel byl zařazen mezi příjemce v některé z kampaních jiným uživatelem (resp. uživatelem s oprávněním *správce testů* nebo *administrátorem*)
- uživatel byl přidán *administrátorem* v rámci této sekce (dává smysl pouze tehdy, pokud mu chce *administrátor* udělit vyšší oprávnění dříve, než se do systému uživatel sám přihlásí)

Uživateli je při každé z těchto možností přidělen i URL parametr, což je jedinečný řetězec vkládaný za URL adresu podvodné stránky, který slouží

k identifikaci uživatele právě na dané podvodné webové stránce. Tento parametr je ve výchozím stavu 6 znaků dlouhý (délku je možné změnit v konfiguračním souboru) a obsahuje znaky anglické abecedy a čísla. Parametr navíc zaručuje to, že se na konkrétní podvodnou stránku vždy dostane pouze uživatel, který na ni má mít opravdu přístup (konkrétní příklad je uveden v podkapitole 5.4.7).

Všechny operace týkající se uživatelů zpracovávají metody umístěné ve třídě `UsersModel`. E-mail svázaný s uživatelem je získáván na základě uživatelského jména uživatele z databáze LDAP v rámci třídy `LdapModel` (připojení k danému LDAP serveru lze nastavit v konfiguračním souboru aplikace). Pokud se e-mail uživatele v této databázi nepodaří nalézt, k registraci nedojde.

5.4.9 Skupiny

V rámci třídy `UserGroupsModel` je k dispozici několik metod, které slouží k vytváření nových či úpravě stávajících uživatelských skupin. Přístup do sekce má pouze uživatel s oprávněním *administrátor*.

Uživatelské skupiny slouží v systému ke sdružování uživatelů se stejným oprávněním (více informací o oprávněních uživatelů v systému poskytuje podkapitola 5.4), přičemž interní značení dostupných oprávnění v systému je následující:

- *administrátor* – nejvyšší oprávnění, které je v systému značeno `0`
- *správce testů* – v systému značeno `1`
- *uživatel* – nejnižší oprávnění, které je v systému značeno `2`

U každé uživatelské skupiny s oprávněním *správce testů* lze nastavit, jakým příjemcům bude moci zasílat uživatel s tímto oprávněním cvičné phishingové zprávy. *Administrátor* pouze u dané skupiny výčtem určí, jaké konkrétní domény nižšího řádu jsou povoleny (např. vstupem `@fav.zcu.cz;@civ.zcu.cz` je řečeno, že *správce testů* s tímto oprávněním bude mít k dispozici pouze příjemce z FAV ZČU a CIV ZČU).

Správu oprávnění a ověření toho, zdali si přihlášený uživatel může změnit během své relace oprávnění, řeší třída `PermissionModel`.

6 Struktura databáze

Pro ukládání dat aplikace využívá databázi navrženou v databázovém systému *MySQL*, přičemž všechny tabulky používají úložiště *InnoDB*.

Parametry pro připojení k databázi lze nastavit v konfiguračním souboru `config.php` vytvořené aplikace (viz podkapitola 5.3.6).

6.1 Tabulky

Aplikace obsahuje celkem 15 databázových tabulek. Všechny tabulky mají ve svém názvu prefix `phg_` (několik písmen z názvu systému *Phishingator*) pro případ, že by se nalézaly ve stejné databázi s dalšími tabulkami z jiných aplikací.

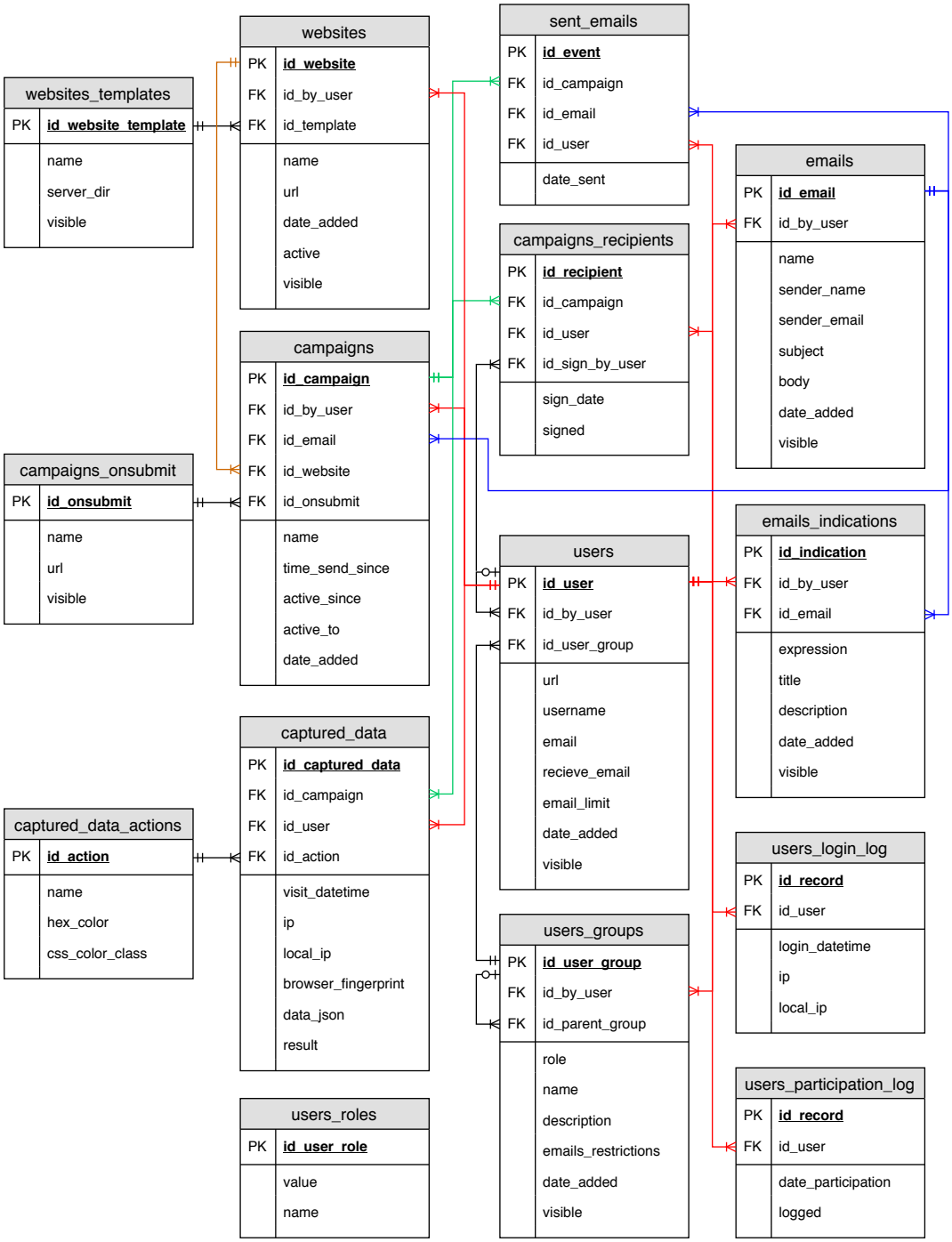
V několika databázových tabulkách je mezi atributy obsažen cizí klíč `id_by_user`, který slouží k uchování informace o tom, kdo daný záznam do databáze přidal nebo například jakým uživatelem (resp. *administrátorem* či *správcem testů*) byl příjemce přihlášen nebo odhlášen z kampaně (atribut `id_sign_by_user` v tabulce `phg_campaigns_recipients`).

Některé z tabulek také obsahují atribut s názvem `visible`, který slouží ke smazání (resp. deaktivaci) záznamu v aplikaci. Atribut nabývá buď hodnoty `1` (záznam je viditelný, výchozí stav), nebo `0` (záznam je smazán a není tedy v aplikaci nikde vidět).

Detailnější popis každé z tabulek včetně podstatných atributů je z důvodu většího rozsahu uveden v příloze B.

6.2 ERA diagram

Vztahy mezi databázovými tabulkami ukazuje ERA diagram na obr. 6.1 (pozn. názvy tabulek pro ušetření místa neobsahují prefix `phg_`).



Obrázek 6.1: ERA diagram navržené databáze

7 Grafické rozhraní

Při návrhu a realizaci grafického rozhraní vytvořené webové aplikace byl použit front-end framework *Bootstrap 4.1.3*. Zmíněný framework ve svých zdrojových kódech obsahuje předpřipravené komponenty a styly a zajišťuje i základní responzivnost webové aplikace [8] (vhodné zobrazení aplikace na různých zařízeních, ovšem pouze při vhodně použitých komponentách).

7.1 Vzhled

Vzhled vytvořené webové aplikace je založen na volně dostupných příkladech v dokumentaci frameworku *Bootstrap*, a to konkrétně na šablonách *Jumbotron* a *Dashboard*, které svým rozvržením obsahu splňují požadavky této aplikace.

Šablony bylo třeba dále upravit, aby byla zajištěna responzivnost pro všechna zařízení a navrhnout, jakým způsobem pracovat s obsahem určeným pro uživatele (formuláře, výpisy záznamů apod.). Z původních šablon tak prakticky zbyla pouze kostra a základní barevné rozvržení.

Cílem bylo vytvořit především přehledný a minimalistický vzhled, který nebude uživateli znesnadňovat práci v systému a kvůli kterému by musel při každé operaci nahlížet do externí nápovědy. U vstupních polí formuláře je uživateli např. nabízena šedě podbarvená krátká nápověda, kterou může časem ignorovat, ale zároveň ho neruší při jakýchkoliv akcích v systému a má případně šanci se vždy ihned přesvědčit, zdali postupuje správně.

7.2 Responzivní design

Vytvořená webová aplikace je plně responzivní na všech zařízeních (tzn. od mobilních telefonů a tabletů, po notebooky s nižším rozlišením až po širokoúhlé monitory s vysokým rozlišením), čímž uživateli usnadňuje její používání i na zařízeních s nestandardním rozlišením bez nutnosti např. přibližování a oddalování stránky.

Z hlediska administrátora aplikace je vhodnější aplikaci používat na širokoúhlých monitorech z důvodu přehlednějšího výpisu tabulek (kvůli velkému počtu sloupců v tabulkách a množství dat v nich vypisovaných), nicméně s určitým uživatelským diskomfortem lze téhož docílit i na zmíněných menších rozlišeních.

8 Zabezpečení aplikace

Aplikace vyjma zabezpečení obvyklého pro většinu webových aplikací (jako například běh aplikace pouze pod HTTPS s certifikátem vydaným důvěryhodnou certifikační autoritou) obsahuje i některé nadstandardní bezpečnostní funkce. Soupis všech těchto bezpečnostních opatření je popsán v následujících podkapitolách.

8.1 WebAuth a režimy oprávnění

Uživatel se pro vstup do aplikace musí autentizovat prostřednictvím autentizační služby *WebAuth* používané univerzitou, přičemž jeho výchozí oprávnění jsou na úrovni *uživatel* (nejnižší úroveň). Při jakékoliv akci, ke které má z hlediska návrhu aplikace přístup jen uživatel s vyšším oprávněním (*správce testů* nebo *administrátor*), dochází k ověřování tohoto oprávnění.

8.2 Ošetření výstupu, obrana proti XSS

Veškeré výstupy v aplikaci jsou ošetřovány proti útoku XSS. Pokud by se útočníkovi přeci jen podařilo vnést do systému externí *JavaScript*, nemělo by k vykonání skriptu dojít na základě implementovaných bezpečnostních HTTP hlaviček, viz kapitola 8.6.

8.3 Ošetření uživatelského vstupu

Jakýkoliv uživatelský vstup je nejprve validován na straně uživatele ve webovém prohlížeči. Vstupní pole formuláře jsou opatřena parametry, které webovému prohlížeči sdělí, jaký je v daném vstupním poli očekáván datový typ (datum, e-mail apod.), maximální počet znaků korespondující s maximálním počtem znaků daného atributu v databázi (pokud dojde ke změně max. počtu znaků v databázi, automaticky se to projeví i v daném formuláři a všech kontrolách) a zdali je nutné vstupní pole vyplnit.

Po odeslání formuláře a kontrole na straně uživatele dochází ke stejným kontrolám i na straně serveru. Ten navíc kontroluje i existenci jakékoliv vybrané hodnoty např. v HTML tagu `<select>`, aby databázi nebyla podstrčena hodnota, která se v ní nenalézá (nebo byla např. v minulosti smazána).

Data budou navíc zpracována jen tehdy, pokud byl součástí formuláře validní *CSRF token*, viz podkapitola 8.4.

Po úspěšném průchodu všemi zmíněnými kontrolami dojde před uložením/úpravou dat v databázi ještě k ošetření uživatelského vstupu pomocí *prepared statements* pro zabránění útoku typu *SQL injection*.

8.4 Obrana proti CSRF

Libovolná akce, která má dopad na konkrétní záznam v databázi (přidání, úprava, smazání), je ověřována na základě jedinečného otisku (pro každého uživatele) generovaného při přihlášení uživatele do systému. Tento otisk (tzv. *CSRF token*) je platný po dobu uživatelova přihlášení a nepřenáší se metodou HTTP GET.

Pokud by chtěl útočník vykonat akci bez vědomí přihlášeného uživatele, ovšem jeho jménem (například podstrčením odkazu pro smazání určitého záznamu do atributu `src` HTML tagu `<img>`), musel by nejprve nějakým způsobem odposlechnout (v kombinaci s nasazeným HTTPS) právě zmíněný *CSRF token* a ten poté připojovat k jakékoliv vykonávané operaci, aby ji aplikace schválila.

8.5 Obrana proti brute force

Protože jedním z cílů aplikace je zaznamenávat uživatelskou aktivitu na podvodných webových stránkách, která se zapisuje do databáze, je každá z těchto podvodných stránek opatřena mechanismem pro zablokování nadměrného počtu požadavků ze strany konkrétního uživatele.

V případě, že uživatel provede na podvodné stránce minimálně 10 požadavků, přičemž doba mezi prvním a posledním požadavkem nepřesáhne 20 sekund, dojde k dočasnému přesměrování konkrétního uživatele na úvodní stránku projektu bez možnosti návratu na podvodnou stránku (dočasné přesměrování je aktivní po dobu 60 sekund od poslední aktivity uživatele). Databáze tak nebude muset zpracovávat další příchozí a nepodstatné záznamy ze strany tohoto uživatele.

Zvýšenou aktivitu lze navíc zpětně identifikovat ve zmiňovaných záznamech z podvodných stránek, protože na podvodné stránky má vždy přístup jen uživatel zapojený mezi příjemce dané kampaně přes odkaz, který je jedinečný pro každého uživatele. Varování o nadměrné aktivitě je zároveň zapisováno do protokolu systému v rámci logování pod úrovní `WARN`.

Stejně tak nelze například opakovaně odesílat tentýž formulář znovu stisknutím klávesy `F5` nebo jiným, nuceným obnovením stránky (po úspěšném přidání záznamu do databáze dochází k přesměrování).

8.6 Secure HTTP headers

Pro zvýšení zabezpečení aplikace došlo k implementaci několika bezpečnostních hlaviček, které webový prohlížeč informují o tom, jak nakládat s potenciálně nebezpečným obsahem na stránce a jinými zranitelnostmi týkajících se webových aplikací [12].

Seznam použitých HTTP hlaviček je následující (popis hlaviček vychází ze zdroje [12]):

- `X-Frame-Options: DENY` – zablokuje vykreslení stránky v HTML tagu `<iframe>` (resp. v rámu) na jiné webové stránce
- `X-XSS-Protection: 1; mode=block` – zablokuje vykreslení stránky, pokud webový prohlížeč na stránce detekuje potenciální XSS útok
- `HTTP Strict Transport Security (HSTS)` – informuje webový prohlížeč o tom, že komunikace mezi serverem a klientem bude na doméně i všech subdoménách probíhat pouze po protokolu HTTPS
- `X-Content-Type-Options: nosniff` – informuje webový prohlížeč o nutnosti kontrolovat MIME (*Multipurpose Internet Mail Extensions*) typ souborů
- `Referrer-Policy: strict-origin-when-cross-origin` – určuje, jaký obsah bude předáván v hlavičce `Referrer` a kam dále bude povoleno tyto požadavky předávat (nastaveno pouze po HTTPS a pouze v rámci stejné domény, mimo doménu bude odeslán pouze název domény)
- `Feature-Policy` – informuje webový prohlížeč o povolených či zakázaných vlastnostech API (*Application Programming Interface*) webového prohlížeče, které může webová stránka využívat (např. umožnit používání mikrofonu, vibrace zařízení apod.; vše nastaveno na zakázáno)
- `Content-Security-Policy` – zablokuje vkládání obsahu z jiných než autorem aplikace specifikovaných zdrojů a navíc jen pod protokolem HTTPS

8.7 Zabezpečení cookies

HTTP cookies, v nichž je uloženo `PHPSESSID` identifikující konkrétní `session` uložené na serveru, ve které jsou uloženy informace o přihlášeném uživateli, jsou zabezpečeny následujícím způsobem:

- `session.cookie_secure: true` – cookie je přenášeno pouze po protokolu HTTPS
- `session.cookie_httponly: true` – cookie nebude možné přečíst (a případně odcizit) na straně klienta pomocí jazyka *JavaScript*

8.8 Odstínění jádra aplikace

Aby potenciální útočník neměl šanci odhalit adresářovou strukturu aplikace a aby neměl přístup k souborům jádra vytvořené aplikace, konfiguračním souborům apod., je aplikace navržena tak, že uživateli (tj. veřejnosti) jsou přístupny jen nezbytné soubory (CSS, *JavaScript* soubory, hlavní PHP přístupový soubor apod.).

Odstínění je docíleno rozvrstvením aplikace a nastavením `DocumentRoot` (v konfiguraci `VirtualHost` webového serveru *Apache*) na konkrétní veřejný adresář – `public`, přičemž do souborů jádra aplikace má přístup jen webový server, nikoliv uživatel přes konkrétní URL adresu.

Stejně tak je ve všech veřejných adresářích aplikováno pravidlo `Options -Indexes`, které zablokuje uživateli zobrazení výpisu souborů v daném adresáři.

8.9 security.txt

Soubor `security.txt` slouží k uvedení kontaktů na autora aplikace v případě, že by se někomu podařilo v aplikaci nalézt bezpečnostní zranitelnost či jinou chybu podobného charakteru a chtěl by ji nahlásit kompetentní osobě [16].

Soubor je dostupný v očekávaném umístění `https://phishingator.zcu.cz/.well-known/security.txt`, přičemž na základě přepisovacího pravidla v souboru `.htaccess` je přístupný i z kořenového adresáře webu.

9 Testování

Aplikace byla v průběhu vývoje a před samotným nasazením na server ZČU testována vybranými uživateli a případné problémy byly evidovány v seznamu chyb a námětů a postupně opravovány.

9.1 Testování pomocí Selenium IDE

Pomocí pluginu *Selenium IDE* do webového prohlížeče *Mozilla Firefox* bylo vytvořeno několik desítek testů ověřující různé scénáře, které mohou nastat ve formulářích aplikace. Soubor s testy je součástí přiloženého média.

9.2 Logování

Aplikace zaznamenává veškeré aktivity dle požadované úrovně do zvoleného protokolu (na základě nastavení v konfiguračním souboru) a některé záznamy ukládá i do databáze.

9.3 Testování bezpečnosti

Aplikace byla autorem práce několikrát testována na nevalidní, neexistující a jiné neočekávané vstupy, na základě kterých docházelo k implementaci dalších ověřovacích a bezpečnostních mechanismů (viz kapitola 8).

Na serveru `https://securityheaders.com`, který ověřuje správnost nastavení bezpečnostních HTTP hlaviček (viz podkapitola 8.6), dostala aplikace v době psaní práce hodnocení *A*, tedy druhé nejvyšší možné hned po *A+* (nejhorší hodnocení je *F*, mezi které spadala většina webových stránek tou dobou uživateli testovaných).

9.4 Testované webové prohlížeče

Aplikace byla testována ve webových prohlížečích (v době psaní práce nejnovější verze) *Mozilla Firefox 66*, *Google Chrome 73*, *Opera 58*, *Microsoft Edge 44* a *Internet Explorer 11*, přičemž ve všech těchto zmíněných webových prohlížečích byla aplikace funkční a zobrazena tak, jak bylo původně navrženo.

10 Pilotní provoz

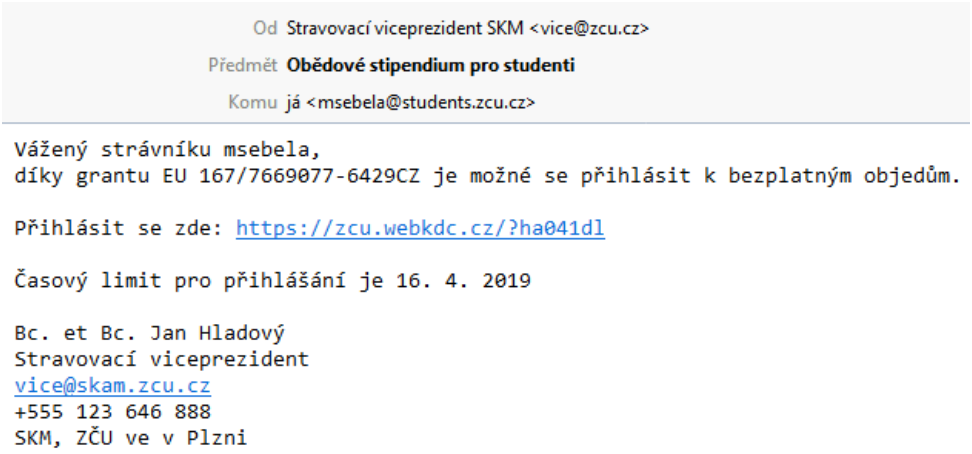
Aplikace byla po nasazení na veřejné adrese `https://phishingator.zcu.cz` serveru ZČU vyzkoušena v omezeném kruhu vybraných uživatelů z řad zaměstnanců a studentů univerzity.

Vybraným uživatelům bylo řečeno, že se stanou součástí testování, nebyl jim ovšem sdělen datum a čas, kdy mohou očekávat cvičný phishingový e-mail. Do kampaně bylo zapojeno 41 vybraných uživatelů.

Parametry kampaně, v rámci které testování probíhalo, jsou popsány v následujících podkapitolách.

10.1 Rozesílaný phishingový e-mail

Vybraným uživatelům byl rozeslán shodný cvičný podvodný e-mail (s minimální úpravou v předmětu e-mailu, který obsahoval buď „*Obědové stipendium pro zaměstnanci*“, nebo „*Obědové stipendium pro studenti*“). Jeho originální znění, které bylo doručeno do e-mailových schránek daných uživatelů, je vyobrazeno na obr. 10.1. V rámci tohoto e-mailu mohl uživatel pokračovat na podvodnou webovou stránku (viz podkapitola 10.2).


Od Stravovací viceprezident SKM <vice@zcu.cz>
Předmět **Obědové stipendium pro studenti**
Komu já <msebela@students.zcu.cz>

Vážený strávníku msebela,
díky grantu EU 167/7669077-6429CZ je možné se přihlásit k bezplatným objedům.

Přihlásit se zde: https://zcu.webkdc.cz/?ha041dl

Časový limit pro přihlášání je 16. 4. 2019

Bc. et Bc. Jan Hladový
Stravovací viceprezident
vice@skam.zcu.cz
+555 123 646 888
SKM, ZČU ve v Plzni

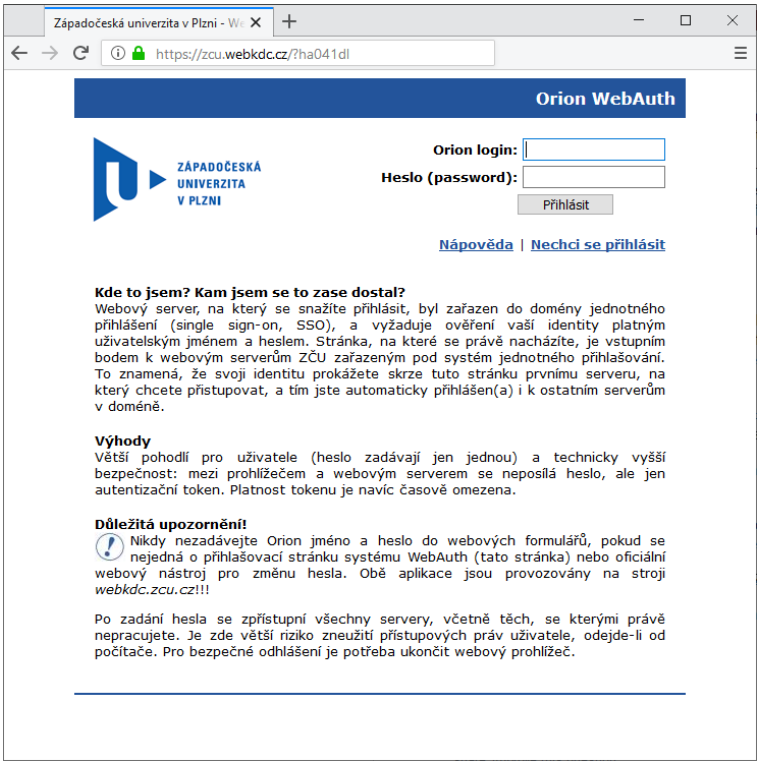
Obrázek 10.1: Cvičný podvodný e-mail obsahující znaky phishingu (překlepy, pravopisné chyby apod., viz teoretická část bakalářské práce) a sociálního inženýrství, který byl pro větší důvěryhodnost automaticky personalizován vůči příjemcům e-mailu (screenshot z aplikace *Mozilla Thunderbird*)

10.2 Dostupná podvodná webová stránka

Ze zaslaného phishingového e-mailu se mohli uživatelé dostat na podvodnou webovou stránku (viz obr. 10.2), jejímž cílem bylo získat jejich přihlašovací údaje používané v prostředí univerzity výměnou za „stipendium na obědy“.

Stránka graficky přesně imitovala pravou webovou stránku, přičemž snaha útočníka (resp. autora práce) bylo vymyslet URL adresu, která se co nejvíce podobá té originální. Zatímco pravý formulář pro přihlašování uživatelů do univerzitního systému je dostupný na adrese `https://webkdc.zcu.cz`, ten falešný na adrese `https://zcu.webkdc.cz` (doménu `webkdc.cz` bylo nutné zakoupit).

Samozřejmostí podvodné stránky bylo i HTTPS s nasazeným důvěryhodným certifikátem (pro uživatele spíše známém ve formě „zeleného zámečku/nákupní tašky“ v adresním řádku webového prohlížeče), který ovšem uživateli nemusí zaručit bezpečí, viz podkapitola 3.3, případně článek [24]).



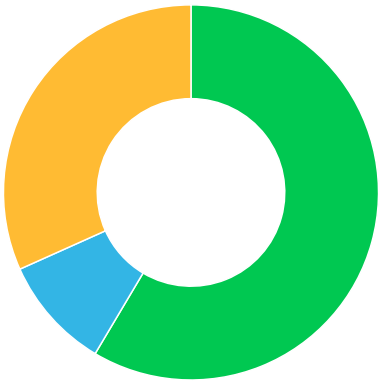
Obrázek 10.2: Podvodná webová stránka, na kterou se mohli uživatelé dostat z odkazu ve cvičném phishingovém e-mailu a jejímž cílem bylo získat přihlašovací údaje uživatelů (screenshot z aplikace *Mozilla Firefox*)

10.3 Výsledky kampaně

Celkové výsledky kampaně (tzn. nejvážnější akce, kterou mohl uživatel v kampani provést) ukazuje graf a tab. 10.3 (v celkových výsledcích je zahrnuto všech 41 uživatelů).

Doba trvání kampaně (a tedy doba, po kterou byla dostupná podvodná stránka ze zasílaného e-mailu) byly tři pracovní dny.

	akce	**počet uživatelů**	
	bez reakce	24	58,5 %
	pouze návštěva podvodné stránky	4	9,8 %
	zadání neplatných přihlašovacích údajů	13	31,7 %
	zadání platných přihlašovacích údajů	0	0 %



Obrázek 10.3: Konečné akce všech uživatelů v testované kampani

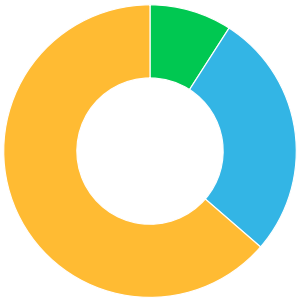
Výsledky odpovídají předpokladu – příjemci byli o zasílaném phishingu dopředu informováni, ale především byli všichni z nich technicky zdatní uživatelé a něco podobného by je nemělo překvapit.

Uživatelé tak do vstupních polí místo přihlašovacích údajů vyplňovali například nestandardní uživatelské vstupy jako příkazy a úryvky zdrojových kódů, které představovaly útoky na aplikaci, a proti kterým je aplikace chráněna, viz kapitola 8 (k prolomení bezpečnosti tedy nedošlo).

Co je třeba poznamenat a co není na žádném z grafů vidět, je fakt, že někteří uživatelé po obdržení e-mailu nejprve začali pátrat, o jakou doménu jde, aniž by následovali odkaz v podvodném e-mailu (zjištěno na základě přístupových logů webového serveru u podvodné domény `zcu.webkdc.cz`).

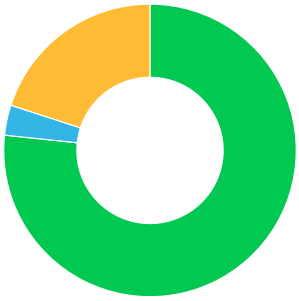
Rozdělení výsledků pro studenty je uvedeno na obr. 10.4 a pro zaměstnance pak na obr. 10.5.

	akce	**počet uživatelů**	
	bez reakce	1	9,1 %
	pouze návštěva podvodné stránky	3	27,3 %
	zadání neplatných přihlašovacích údajů	7	63,6 %
	zadání platných přihlašovacích údajů	0	0 %



Obrázek 10.4: Konečné akce studentů (celkem 11 uživatelů) v testované kampani

	akce	**počet uživatelů**	
	bez reakce	23	76,7 %
	pouze návštěva podvodné stránky	1	3,3 %
	zadání neplatných přihlašovacích údajů	6	20,0 %
	zadání platných přihlašovacích údajů	0	0 %



Obrázek 10.5: Konečné akce zaměstnanců (celkem 30 uživatelů) v testované kampani

11 Závěr

Cílem práce bylo seznámit se phishingem, sociálním inženýrstvím a jeho metodami a na základě výsledků analýzy existujících softwarových řešení navrhnout a implementovat software, který umožní jednoduše vytvářet a odesílat cvičné phishingové zprávy konkrétním uživatelům a který na rozdíl od existujících aplikací bude splňovat požadavky ZČU.

Vytvořená aplikace do odeslaných cvičných phishingových e-mailů na předem určená místa vkládá odkazy na podvodné webové stránky, které je možné stejně tak vytvářet a provádí automatické vyhodnocení získaných dat. Všem uživatelům navíc systém umožňuje si všechny přijaté podvodné e-maily zpětně prohlédnout včetně seznamu indicií (označených pasáží v e-mailu s popisem), na základě kterých mohl uživatel phishing rozpoznat a podle kterých se může v budoucnu řídit při odhalování reálného phishingu. Uživatelé se zároveň mohou ve vytvořené aplikaci dobrovolně přihlásit k odebírání cvičných phishingových zpráv s možností volby maximálního počtu e-mailů, který jim bude v budoucnu doručen. Všechny cíle bakalářské práce tak byly splněny.

V rámci bakalářské práce došlo k otestování vytvořeného systému mezi vybranými uživateli a k nasazení aplikace na server ZČU s tím, že do aplikace má možnost se přihlásit kdokoliv z uživatelů ZČU pomocí svého univerzitního konta. Spolu s tím došlo k rozhodnutí, že aplikace bude nadále vylepšována a rozšiřována o nové funkce.

Univerzita tak bude mít nástroj určený ke vzdělávání uživatelů pro odhalování phishingu, který naváže na semináře zabývající se phishingem. Aktivní vzdělávání uživatelů v této problematice je navíc jeden z požadavků zákona o kybernetické bezpečnosti.

Vyvinutou aplikaci pojmenovanou *Phishingator* lze navíc po určitých úpravách nasadit i v jiných institucích včetně dalších vysokých škol, čímž může aplikace získat i komerční potenciál a globální data o chování uživatelů na phishingových stránkách.

Na základě výzkumu souvisejícího s teoretickou částí bakalářské práce také vznikl odborný článek „*Kam vás dovede dotazník z podvodné stránky?*“ popisující postupy používané při manipulaci uživatelů internetu pomocí sociálního inženýrství a odhalující část infrastruktury útočníka [24].

Přehled zkratek

API	Application Programming Interface
BeEF	The Browser Exploitation Framework
CSP	Content Security Policy
CSRF	Cross-site Request Forgery
CSS	Cascading Style Sheets
CSV	Comma-separated Values
DKIM	DomainKeys Identified Mail
DNS	Domain Name System
DPI	Dots Per Inch
EV	Extended Validation Certificate
HSTS	HTTP Strict Transport Security
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDE	Integrated Development Environment
IDN	Internationalized Domain Name
IP	Internet Protocol address
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extensions
MVC	Model–view–controller
PDF	Portable Document Format
PDO	PHP Data Objects
PHP	Hypertext Preprocessor
SMS	Short Message Service
SPF	Sender Policy Framework
SQL	Structured Query Language
SVG	Scalable Vector Graphics
TLD	Top Level Domain
TTL	Time To Live
URL	Uniform Resource Locator
WIRT	WEBnet Incident Response Team
XML	Extensible Markup Language
XSS	Cross-site Scripting

Literatura

[1] *SSAC Advisory on Fast Flux Hosting and DNS* [online]. 2008. [cit. 2018-12-12]. Dostupné z: https://www.icann.org/en/system/files/files/sac-025-en.pdf.

[2] *Facebook Announces Its Third Pillar "Graph Search" That Gives You Answers, Not Links Like Google* [online]. 2013. [cit. 2018-11-21]. Dostupné z: https://techcrunch.com/2013/01/15/facebook-announces-its-third-pillar-graph-search/.

[3] *Phishing* [online]. 2017. [cit. 2018-10-27]. Dostupné z: https://support.zcu.cz/index.php/Phishing.

[4] *Chrome removes secure notification* [online]. 2018. [cit. 2018-11-19]. Dostupné z: https://www.xolphin.com/news/Chrome_removes_secure_notification.

[5] *CZ.NIC - IDN - Internationalized domain names* [online]. c2018. [cit. 2018-11-03]. Dostupné z: https://www.háčkyčárky.cz.

[6] *Unicode Security Mechanisms for UTS #39* [online]. 2018. [cit. 2018-11-16]. Dostupné z: https://www.unicode.org/Public/security/latest/confusables.txt.

[7] *MVC architektura* [online]. 2018. [cit. 2019-04-20]. Dostupné z: https://www.itnetwork.cz/navrh/mvc-architektura-navrhovy-vzor.

[8] *Bootstrap* [online]. [cit. 2019-04-20]. Dostupné z: https://getbootstrap.com/.

[9] *Fast flux* [online]. 2015. [cit. 2018-12-12]. Dostupné z: http://timehosting.cz/fast-flux/.

[10] *How to modify your folder view settings or to customize a folder* [online]. 2018. [cit. 2018-11-05]. Dostupné z: https://support.microsoft.com/en-ph/help/812003/how-to-modify-your-folder-view-settings-or-to-customize-a-folder.

[11] *BeEF - The Browser Exploitation Framework Project* [online]. [cit. 2018-12-08]. Dostupné z: https://beefproject.com/.

[12] *OWASP Secure Headers Project* [online]. 2019. [cit. 2019-04-14]. Dostupné z: https://www.owasp.org/index.php/OWASP_Secure_Headers_Project.

[13] *Clickjacking Defense Cheat Sheet* [online]. 2017. [cit. 2018-11-19]. Dostupné z: https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet.

[14] *Marking HTTP As Non-Secure* [online]. 2018. [cit. 2018-11-19]. Dostupné z: https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure.

[15] *Origins of the Word "Phishing"* [online]. [cit. 2018-11-16]. Dostupné z: https://docs.apwg.org/word_phish.html.

[16] *A Method for Web Security Policies draft-foudil-securitytxt-06* [online]. 2019. [cit. 2019-04-10]. Dostupné z: https://tools.ietf.org/html/draft-foudil-securitytxt-06.

[17] *Sociální inženýrství* [online]. [cit. 2018-11-07]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/.

[18] *Phishing: Jak jej včas rozpoznat a „nenaletět“ - CSIRT* [online]. 2015. [cit. 2018-11-05]. Dostupné z: https://csirt.cz/page/2940/phishing--jak-jej-vcas-rozpoznat-a-nenaletet/.

[19] *Phishing - příklady* [online]. 2017. [cit. 2018-10-29]. Dostupné z: https://support.zcu.cz/index.php/Phishing_-_příklady.

[20] *Phishing Activity Trends Report, 2nd Quarter 2018* [online]. 2018. [cit. 2018-11-17]. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q2_2018.pdf.

[21] *IDN homograph attack* [online]. Wikimedia Foundation, 2001-2018. [cit. 2018-11-03]. Dostupné z: https://en.wikipedia.org/wiki/IDN_homograph_attack.

[22] *Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)* [online]. 2003. [cit. 2018-11-05]. Dostupné z: https://www.ietf.org/rfc/rfc3492.txt.

[23] Caletka, O. *Co musíte vědět o šifrování* [online]. 2017. [cit. 2018-11-05]. Dostupné z: https://ondřej.caletka.cz/dl/slidy/20171129-ZCU-Co_musite_vedet_o_sifrovani.pdf.

[24] Šebela, M. *Kam vás dovede dotazník z podvodné stránky?* [online]. 2019. [cit. 2019-02-11]. Dostupné z: https://www.root.cz/clanky/kam-vas-dovede-dotaznik-z-podvodne-stranky/.

[25] Šimek, R. *Sociotechnika (sociální inženýrství)* [online]. 2003. [cit. 2018-11-09]. Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm.

[26] Kolouch, J. *CyberCrime*. CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.

[27] Kolouch, J. *Phishing včera, dnes a zítra* [online]. 2018. [cit. 2018-10-27]. Dostupné z: https://www.youtube.com/watch?v=ugF-1cLUKYw&index=2&list=PLvwguJ6ySH1eEol6yw1_8DgSEixndlaw8.

[28] Mudruněk, F. Detekce phishingu, 2016. Dostupné z: https://dspace.cvut.cz/bitstream/handle/10467/65080/F8-DP-2016-Mudrunek-Filip-thesis.pdf.

[29] Padrta, A. – Čepák, J. *IT bezpečnost - Phishing* [online]. 2018. [cit. 2018-10-27]. Dostupné z: https://www.download.zcu.cz/public/Prezentace/seminare_CIV_2018/Skoleni_ZCU_Phishing_v5.5.pdf.

[30] Padrta, A. – Orkáč, R. Cvičné phishingové e-maily ZČU/2017. Dostupné z: https://www.download.zcu.cz/secure/Prezentace/2017-12-13-phish_zcu2017-prezentace.pdf. 2017.

[31] Špaček, M. *Vyhledávejte na netu jako MacGyver* [online]. 2018. [cit. 2018-10-30]. Dostupné z: https://www.michalspacek.cz/prednasky/vyhledavejte-na-netu-jako-macgyver-linuxdays.

Přílohy

A Uživatelská dokumentace

V následujících podkapitolách jsou informace pro používání vytvořené aplikace *Phishingator*.

Stejná dokumentace je také k dispozici online na oficiální URL adrese `https://support.zcu.cz/index.php/LPS:Phishingator`, kde je také uveden rozcestník na jednotlivé stránky (tedy podkapitoly této přílohy).

A.1 O aplikaci Phishingator

Phishingator je systém pro rozesílání cvičných phishingových zpráv dostupný na URL adrese `https://phishingator.zcu.cz`.

Administrátorům systému umožňuje jednoduše vytvářet cvičné phishingové e-maily, označovat v nich indicie, na základě kterých je možné daný podvodný e-mail rozpoznat a samotné e-maily pak v rámci tzv. kampaní automaticky rozesílat zvoleným uživatelům.

Každý z podvodných e-mailů navíc ve svém těle odkazuje na konkrétní podvodnou stránku (napodobující například přihlášení do STAG), kterou administrátor vytváří v rámci tohoto systému. Cílem této podvodné stránky je od uživatelů získat jejich přihlašovací údaje, přičemž veškerá aktivita ze strany uživatele (návštěva podvodné stránky, zadání platných či neplatných údajů do formuláře na podvodné stránce anebo nereagování) se zaznamenává a projevuje v souhrnu a grafech u každé kampaně a v celkových statistikách.

Uživatelé ZČU se mohou do systému přihlásit svým *Orion* kontem a zároveň si nechat dobrovolně zasílat cvičné phishingové zprávy (s možností nastavení limitu, tedy maximálního počtu e-mailů, které si uživatel ještě přeje obdržet). Spolu s tím má uživatel možnost si v systému detailně prohlédnout každý ze cvičných phishingových e-mailů, který mu byl v minulosti zaslán a na základě administrátorem přidaných indicií tak zjistit, čeho si měl na konkrétním e-mailu všimnout, a především všímat do budoucna. Uživatel má zároveň k dispozici i osobní statistiku znázorňující jeho úspěšnost v odhalování phishingu.

Vznik aplikace proběhl v ak. roce 2018/2019 na FAV ZČU v rámci bakalářské práce *Systém pro rozesílání cvičných phishingových zpráv (Martin Šebela)* pod vedením *Ing. Aleše Padrty, Ph.D.* V textu bakalářské práce jsou detailně uvedeny další podrobnosti týkající se tohoto systému.

A.2 Návod pro uživatele

Pro přihlášení do systému *Phishingator* stačí přejít na adresu `https://phishingator.zcu.cz` a kliknout na tlačítko *Přihlásit se*. Přihlašovací údaje jsou stejné jako pro přihlášení do jiných systémů na ZČU (jako např. do STAG), tedy *Orion* kontem uživatele.

Úvodní stránka

Obsahuje osobní statistiku uživatele znázorňující počet cvičných phishingových zpráv, které byly uživateli odeslány a stejně tak osobní úspěšnost v odhalování phishingu, kterou si lze prohlédnout i na příslušném grafu (jestliže jsou již k dispozici nějaká relevantní data).

Moje účast v programu

Uživatel si po přihlášení do systému může zvolit, zdali chce dobrovolně přijímat cvičné phishingové e-maily, které připravuje bezpečnostní tým WIRT. Spolu s tím si může nastavit limit (resp. maximální počet) cvičných phishingových e-mailů, které chce ještě do budoucna přijmout.

Při přihlášení k dobrovolnému odebírání cvičných phishingových zpráv může uživatel takové e-maily očekávat párkrát do roka (tedy v minimálním počtu) a svou účast v programu má možnost kdykoliv zrušit.

Přijaté phishingové e-maily

V této sekci má uživatel možnost si detailně prohlédnout seznam všech cvičných phishingových e-mailů, které mu byly v minulosti doručeny. U každého e-mailu navíc vidí i svou reakci, tedy to, jakým způsobem na konkrétní e-mail reagoval (například zdali navštívil podvodnou stránku přístupnou z tohoto e-mailu a zadal do formuláře platné přihlašovací údaje apod.) či nereagoval. U podvodného e-mailu je vždy vytvořen i seznam indicií (zakroužkované pasáže v textu s popisem, co konkrétně vyvolává podezření), na základě kterých může uživatel zpětně zjistit, zdali postupoval správně nebo čeho by si měl do budoucna všímat.

A.3 Návod pro správce testů

Správce testů je jedno z oprávnění dostupných v systému *Phishingator*, které danému uživateli umožňuje vytvářet a spravovat kampaně spadající do stejné uživatelské skupiny.

Pro přihlášení do systému *Phishingator* stačí přejít na adresu `https://phishingator.zcu.cz` a kliknout na tlačítko *Přihlásit se*. Přihlašovací údaje jsou stejné jako pro přihlášení do jiných systémů na ZČU (jako např. do STAG), tedy *Orion* kontem uživatele.

Pokud má uživatel oprávnění správce testů (přiděluje jej administrátor, resp. člen týmu WIRT), uvidí po přihlášení do systému tento název role v pravé horní části obrazovky vedle svého uživatelského jména. Na stejném místě může přihlášený uživatel měnit svou roli a přepnout se tak na úroveň oprávnění uživatele (viz podkapitola A.2) a naopak.

Úvodní stránka

Obsahuje graf znázorňující průběžnou úspěšnost všech kampaní, které byly vytvořeny přihlášeným uživatelem, nebo jiným správcem testů ve stejné uživatelské skupině.

Kampaně

Umožňuje přihlášenému uživateli přidávat nové a upravovat existující kampaně, ke kterým má oprávnění (byly tedy vytvořeny jím, nebo někým, kdo je ve stejné uživatelské skupině jako on). U stejných kampaní má stejně tak možnost si prohlédnout statistiku a průběžné výsledky konkrétní kampaně.

Seznam kampaní

Obsahuje stručný přehled o všech kampaních, ke kterým má správce testů přístup (viz předchozí odstavec). Data (sloupec *Aktivní od* a *Aktivní do*) svým barevným podbarvením znázorňují, zdali datum již proběhlo či nikoliv, a to následujícím způsobem:

- *zelené podbarvení* – datum ještě nenastalo (tzn. start kampaně ještě neproběhl nebo kampaň stále běží)
- *šedé podbarvení* – datum již nastalo (tzn. start kampaně již proběhl nebo byla kampaň již ukončena)
- *žluté podbarvení* – poslední den, během kterého bude kampaň aktivní

Přidání nebo úprava kampaně

Pro vytvoření kampaně je třeba vyplnit všechna vstupní pole formuláře a stisknout tlačítko *Přidat*, které v případě nesprávných nebo chybějících dat vyzve uživatele k nápravě. Vstupní pole, která se musí vyplnit, jsou následující:

- *název* – slouží k identifikaci v systému, resp. v seznamu přidaných kampaní
- *rozesílaný podvodný e-mail* – cvičný phishingový e-mail, který bude zvoleným příjemcům kampaně doručen do jejich e-mailových schránek; z tohoto e-mailu se budou moci dostat na podvodnou webovou stránku (viz následující bod)
- *podvodná webová stránka přístupná z e-mailu* – stránka, která bude přístupná z odkazu umístěného ve cvičném podvodném e-mailu a na které je umístěn formulář pro sbírání dat v něm zadaných
- *akce po odeslání formuláře* – akce, která nastane na straně uživatele po odeslání formuláře na podvodné webové stránce
- *spustit rozesílání e-mailů v čase* – čas, ve kterém se začnou v den startu kampaně rozesílat cvičné phishingové e-maily
- *start kampaně* – datum spuštění kampaně (den, kdy se začnou rozesílat cvičné phishingové e-maily a den, od kterého začne být vybraným příjemcům dostupná podvodná webová stránka)
- *ukončení kampaně* – datum ukončení kampaně (den, kdy přestanou fungovat odkazy vedoucí na podvodnou stránku přístupnou z cvičných phishingových e-mailů a tedy den, kdy skončí zaznamenávání jakékoliv aktivity na této podvodné stránce)
- *seznam účastníků kampaně* – příjemci zasílaného cvičného podvodného e-mailu a zároveň jediní uživatelé, kteří budou mít přes vlastní a jedinečný odkaz přístup na zvolenou podvodnou webovou stránku
  - výběr příjemců probíhá buď manuálně vypsáním e-mailových adres, nebo po otevření dialogového okna stisknutím tlačítka *Vybrat příjemce* (pod vstupním polem se seznamem příjemců), které umožňuje vybrat příjemce, ke kterým má správce testů oprávnění

A.4 Návod pro administrátory

Administrátor je nejvyšší oprávnění, které je v systému *Phishingator* k dispozici. Obvykle má toto oprávnění člen týmu WIRT.

Pro přihlášení do systému *Phishingator* stačí přejít na adresu `https://phishingator.zcu.cz` a kliknout na tlačítko *Přihlásit se*. Přihlašovací údaje jsou stejné jako pro přihlášení do jiných systémů na ZČU (jako např. do STAG), tedy *Orion* kontem uživatele.

Změna role

Systém umožňuje uživatelům s vyšším oprávněním (tedy minimálně s oprávněním správce testů) přepínat mezi všemi ostatními, nižšími rolemi. Pro změnu role stačí v systému kliknout na tlačítko *Změnit roli* (příp. *Role*) v pravé horní části obrazovky.

Úvodní stránka

Obsahuje grafy znázorňující průběžnou úspěšnost všech přidaných kampaní. Spolu s tím je k dispozici i další graf, který stejná data převádí do podoby sloupců symbolizujících skupinu, do které uživatelé (resp. příjemci) spadají (na základě jejich e-mailu).

Kampaně

Umožňuje administrátorovi přidávat nové a upravovat jakékoliv existující kampaně. U běžících a ukončených kampaní je možnost si prohlédnout statistiku nebo průběžné výsledky a seznam všech akcí, které uživatelé provedli na podvodných webových stránkách.

Seznam kampaní

Obsahuje stručný přehled o všech přidaných kampaních. Data (sloupec *Aktivní od* a *Aktivní do*) svým barevným podbarvením znázorňují, zdali datum již proběhlo či nikoliv, a to následujícím způsobem:

- *zelené podbarvení* – datum ještě nenastalo (tzn. start kampaně ještě neproběhl nebo kampaň stále běží)
- *šedé podbarvení* – datum již nastalo (tzn. start kampaně již proběhl nebo byla kampaň již ukončena)
- *žluté podbarvení* – poslední den, během kterého bude kampaň aktivní

Přidání nebo úprava kampaně

Pro vytvoření kampaně je třeba vyplnit všechna vstupní pole formuláře a stisknout tlačítko *Přidat*, které v případě nesprávných nebo chybějících dat vyzve uživatele k nápravě. Vstupní pole, která se musí vyplnit, jsou následující:

- *název* – slouží k identifikaci v systému, resp. v seznamu přidaných kampaní
- *rozesílaný podvodný e-mail* – cvičný phishingový e-mail, který bude zvoleným příjemcům kampaně doručen do jejich e-mailových schránek; z tohoto e-mailu se budou moci dostat na podvodnou webovou stránku (viz následující bod)
- *podvodná webová stránka přístupná z e-mailu* – stránka, která bude přístupná z odkazu umístěného ve cvičném podvodném e-mailu a na které je umístěn formulář pro sbírání dat v něm zadaných
- *akce po odeslání formuláře* – akce, která nastane na straně uživatele po odeslání formuláře na podvodné webové stránce
- *spustit rozesílání e-mailů v čase* – čas, ve kterém se začnou v den startu kampaně rozesílat cvičné phishingové e-maily
- *start kampaně* – datum spuštění kampaně (den, kdy se začnou rozesílat cvičné phishingové e-maily a den, od kterého začne být vybraným příjemcům dostupná podvodná webová stránka)
- *ukončení kampaně* – datum ukončení kampaně (den, kdy přestanou fungovat odkazy vedoucí na podvodnou stránku přístupnou z cvičných phishingových e-mailů a tedy den, kdy skončí zaznamenávání jakékoliv aktivity na této podvodné stránce)
- *seznam účastníků kampaně* – příjemci zasílaného cvičného podvodného e-mailu a zároveň jediní uživatelé, kteří budou mít přes vlastní a jedinečný odkaz přístup na zvolenou podvodnou webovou stránku
  - výběr příjemců probíhá buď manuálně vypsáním e-mailových adres, nebo po otevření dialogového okna stisknutím tlačítka *Vybrat příjemce* (pod vstupním polem se seznamem příjemců)

Podvodné e-maily a indicie

Obsahuje seznam všech přidaných podvodných e-mailů. Ke každému podvodnému e-mailu lze po jeho přidání vložit indicie, na základě kterých mohl uživatel phishingový e-mail rozpoznat.

Přidání nebo úprava podvodného e-mailu

Vstupní pole při vytváření nebo úpravě podvodného e-mailu jsou následující:

- *název* – slouží k identifikaci v systému
- *jméno odesílatele* – nepovinný údaj, který v e-mailových klientech doplňuje e-mail odesílatele; při jeho nevyplnění bude v odeslaném podvodném e-mailu vidět pouze e-mail odesílatele
- *e-mail odesílatele* – umožňuje definovat e-mail, ze kterého budou odesílány podvodné e-maily, případně použít proměnnou `%recipient_email%`, místo které dojde ke vložení e-mailu příjemce (tzn. e-mail odesílatele i příjemce bude stejný)
- *předmět*
- *tělo* – v těle e-mailu je možné použít několik proměnných, které budou při odeslání podvodného e-mailu nahrazeny reálným (případně personalizovaným) obsahem (pro vložení proměnné do těla e-mailu stačí kliknout na její název vedle vstupního pole):
  - `%recipient_username%` – uživatelské jméno příjemce
  - `%recipient_email%` – e-mail příjemce
  - `%date_cz%` – datum, ve kterém dochází k odeslání e-mailu v českém formátu (např. 7. 4. 2019)
  - `%date_en%` – datum, ve kterém dochází k odeslání e-mailu ve formátu `YYYY-MM-DD` (např. 2019-04-07)
  - `%url%` – URL podvodné stránky svázané s e-mailem

Přidání nebo úprava indicií u podvodného e-mailu

Pro přidání indicií k phishingovému e-mailu stačí v souhrnném seznamu všech e-mailů kliknout na tlačítko *Nastavit indicie*. Následuje zobrazení náhledu přidaného podvodného e-mailu a formuláře pro přidání nových či úpravu dosud přidaných indicií. Vstupní pole jsou následující:

- *indicie (podezřelý řetězec)* – konkrétní pasáž v textu, která má být systémem označena (resp. zakroužkována) a se kterou má být svázán popis indicie; pokud není cílem odkázat na text v těle e-mailu, ale na jinou část e-mailu, je možné použít následující proměnné:
  - `%sender_name%` – pro označení jména odesílatele e-mailu
  - `%sender_email%` – pro označení e-mailu odesílatele
  - `%subject%` – pro označení předmětu e-mailu
- *nadpis* – stručný nadpis indicie nebo název kategorie (např. podezřelé oslovení, překlepy apod.)
- *popis* – nepovinný údaj obsahující podrobnější popis indicie

Po přidání či úpravě indicie je ihned v horní části obrazovky uveden náhled zvýrazněné pasáže. Tlačítkem *Náhled včetně indicií* je možné si e-mail prohlédnout včetně seznamu indicií a včetně personalizovaných proměnných vůči aktuálně přihlášenému uživateli.

Podvodné stránky

Sekce obsahuje seznam všech podvodných stránek, na které se mohou uživatelé dostat skrz odkazy v rozesílaných podvodných e-mailech.

Přidání nebo úprava podvodné stránky

Vstup na podvodné stránky je limitován systémem, který je nechává přístupné pouze po dobu běhu kampaně a zároveň jen přes jedinečné odkazy, jež jsou dostupné pouze pro příjemce dané kampaně (všichni ostatní příchozí budou bez znalosti konkrétního odkazu automaticky přesměrováni na úvodní stránku projektu *Phishingator*).

Postup pro založení nové podvodné stránky je následující:

1. nastavit odpovídající `A` záznam v DNS záznamech podvodné domény (popř. subdomény), na které bude provozována podvodná stránka tak, aby byl směrován na IP adresu, kde běží aplikace *Phishingator*
2. přidat podvodnou stránku v sekci *Podvodné stránky*, která v lokaci nastavené v konfiguračním souboru aplikace (konstanta `PHISHING_WEBSITE_APACHE_SITES_DIR`) vytvoří nový konfigurační soubor pro podvodnou stránku určený pro webový server (ten dané podvodné stránce nastavuje konkrétní `DocumentRoot`, tedy adresář, kde je umístěna šablona (vzhled) podvodné stránky a další parametry požadované

pro svázání stránky s aplikací *Phishingator*), přičemž vstupní pole formuláře jsou následující:

- *název* – slouží k identifikaci v systému
- *URL* – URL adresa, která bude doplňována do podvodných e-mailů místo proměnné `%url%` a tedy URL adresa, jejíž konkrétní `A` záznam musí být v DNS směrován na IP adresu webového serveru, kde běží systém *Phishingator*
- *šablona* – vzhled, který bude na dané podvodné stránce (další lze definovat v databázové tabulce `phg_websites_templates`, kde u nového záznamu stačí pouze upřesnit, v jakém adresáři (výchozí je `/templates/websites`) se nacházejí zdrojové soubory dané šablony, viz dále)
- *stránka je připravena (. . .)* – nastavení, zdali má být podvodná stránka viditelná pro ostatní uživatele (tzn. především pro správce testů) v seznamu dostupných podvodných stránek v kampaních

3. v konfiguraci webového serveru *Apache* aktivovat nový konfigurační soubor, resp. `VirtualHost`, který bude zachytávat požadavky na danou doménu/subdoménu, a to příkazem `a2ensite konfiguracni_soubor` (pozn. aplikace konfigurační soubor vytváří v adresáři nastaveném v konstantě `PHISHING_WEBSITE_APACHE_SITES_DIR` v konf. souboru aplikace, vygenerovaný soubor je tedy vhodné zkopírovat do adresáře `/etc/apache2/sites-available/` a v tomto adresáři zadat zmíněný příkaz)

4. dle požadavků vydat důvěryhodný či nedůvěryhodný certifikát pro podvodnou stránku, nebo ji nechat běžet pouze na protokolu HTTP (v rámci aplikace řešeno programem *Certbot*, který automaticky vydá důvěryhodný certifikát podepsaný certifikační autoritou *Let's Encrypt*) a tuto skutečnost nastavit v konfiguračním souboru daného `VirtualHost`

5. restartovat (resp. stačí volat příkaz `reload`) webový server *Apache* pro aplikování provedených změn

Po těchto krocích systém automaticky nad podvodnou stránkou (resp. konkrétní doménou/subdoménou) převezme kontrolu.

Požadavky na šablonu podvodné stránky

Aby systém zachytával data zadaná do formuláře na podvodné stránce, je nutné, aby formulář splňoval následující podmínky:

- formulář musí mít jako metodu odesílání nastaveno `method="post"` (povoleny jsou pouze POST požadavky)
- vstupní pole pro zadání uživatelského jména musí obsahovat atribut `name="username"`
- vstupní pole pro zadání hesla musí obsahovat atribut `name="password"`
- ve formuláři musí existovat tlačítko obsahující atribut `type="submit"` sloužící pro odeslání formuláře (obvykle v rámci HTML tagu `<input>` nebo `<button>`)

Informace o nové šabloně (především lokaci zdrojových souborů na webovém serveru) je poté nutné manuálně přidat do databázové tabulky `phg_websites_templates` a všechny její soubory umístit do nového adresáře v lokaci nastavené v `PHISHING_WEBSITE_APACHE_SITES_DIR` (ve výchozím stavu `/templates/websites`).

Uživatelé

Umožňuje prohlížet seznam všech uživatelů evidovaných v systému.

Uživatelé se do systému mohou přihlásit buď dobrovolně v rámci služby *WebAuth*, případně tím, že je zaregistruje administrátor anebo tím, že budou uvedeni mezi příjemci v některé z kampaní.

Mezi všemi uživateli lze vyhledávat (pozn. vyhledává se ve sloupci e-mail) a dále filtrovat. Seznam dále administrátorovi zobrazuje, kolik cvičných phishingových e-mailů každý z uživatelů obdržel, jeho případný limit a také to, zdali se přihlásil k odebírání cvičných phishingových zpráv a kdy konkrétně.

Přidání nebo úprava uživatele

Pro registraci uživatele do systému není třeba jej předem vytvářet na základě tohoto postupu. Využití tohoto postupu pro přidání nového uživatele dává smysl jen tehdy, pokud chce administrátor přidělit vyšší práva konkrétnímu uživateli dříve, než se do systému sám přihlásí, všechny ostatní případy řeší systém automaticky (například registrace příjemců do kampaně, kteří zatím nemají žádný záznam v systému). Vstupní pole pro přidání nebo úpravu uživatele jsou následující:

- *e-mail* – e-mail uživatele, na který budou zasílány cvičné phishingové e-maily a zároveň e-mail, který je uveden u daného uživatele v databázi LDAP

- *skupina* – uživatelská skupina, na základě které uživatel získá oprávnění v systému, a to buď oprávnění uživatel, správce testů nebo administrátor

Uživatelské skupiny

Obsahuje seznam všech uživatelských skupin, na základě kterých uživatelé získávají oprávnění v systému. Tři základní (rodičovské) skupiny nelze smazat a slouží jako záloha pro uživatele, kterým bude smazána jejich původní skupina (tzn. pokud bude uživatel členem skupiny, jejíž oprávnění je uživatel a administrátor tuto skupinu smaže, dojde k přesunu všech uživatelů mazané skupiny do rodičovské skupiny se stejným oprávněním).

Přidání nebo úprava uživatelské skupiny

Formulář pro přidání nebo úpravu skupiny obsahuje následující vstupní pole:

- *název* – slouží k identifikaci v systému
- *popis* – nepovinný popis skupiny
- *oprávnění* – oprávnění, které budou mít všichni uživatelé této skupiny (výběr mezi *uživatel*, *správce testů*, přičemž možnosti, které každá z těchto skupin nabízí, lze zjistit na základě přepnutí role (viz podkapitola A.4), případně na základě návodů pro ostatní skupiny oprávnění z předchozích kapitol)
- *omezení skupiny na konkrétní sadu e-mailů* – vstupní pole vztahující se pouze na uživatele s oprávněním *správce testů*, které udává seznam domén, případně domén nižších řádů, na které může uživatel této skupiny zasílat cvičné phishingové e-maily (při vytváření kampaně nebude moci vybrat jiné příjemce) a to ve tvaru: `@civ.zcu.cz;fav.zcu.cz` (tedy vždy s uvedeným znakem `@` a záznamy oddělenými znakem `;`, pokud nebylo v konfiguraci aplikace definováno jinak)

Konfigurace systému

Řadu možností systému (jako např. parametry pro připojení k databázi, LDAP, výchozí nastavení uživatelů k dobrovolnému odebírání cvičných phishingových zpráv apod.) lze konfigurovat v rámci souboru `config.php`. Vzhledem k tomu, že je detailně komentován, stejně jako zdrojový kód aplikace, nebudou zde jednotlivé možnosti popisovány.

A.5 Instalace systému

Aplikaci *Phishingator* lze nainstalovat následujícím postupem, po kterém by měla být plně funkční (předpokladem je mít na serveru nainstalované potřebné technologie a moduly popisované v kapitole 5.2 a HTTPS):

- nastavit v konkrétní konfiguraci `VirtualHost` webového serveru *Apache*:
  - `DocumentRoot` na adresář `public` v aplikaci *Phishingator*
  - adresář `public/portal` tak, aby byl přístupný pouze po úspěšném přihlášení do služby *WebAuth*
- umístit na webový server všechny potřebné soubory aplikace
- vytvořit databázi a importovat do ní všech 15 databázových tabulek a parametry pro připojení k databázi poté upravit v souboru `config.php`
- nastavit parametry pro připojení k databázi LDAP v souboru `config.php`
- nastavit práva pro zápis do souboru `log.log`
- alespoň překontrolovat a případně upravit nastavení následujících konstant (obvykle obsahují absolutní adresu či název domény) v souboru `config.php` (popis konstant je uveden ve stejném souboru):
  - `LOGGER_FILEPATH`
  - `WEB_URL`
  - `CORE_DOCUMENT_ROOT`
  - `PHISHING_EMAIL_HEADER_VALUE`
  - `PHISHING_WEBSITE_APACHE_SITES_DIR`
  - `PHISHING_WEBSITE_TEMPLATE_CONF_FILE`
  - `PHISHING_WEBSITE_SERVER_ADMIN`
  - `PHISHING_WEBSITE_PREPENDER`
  - `EMAILS_ALLOWED_DOMAIN`
  - `LDAP_GROUPS_RECIPIENTS`
- nastavit práva `777` pro adresář `temp`
- nastavit, aby byl soubor `verifyCredentials.sh` ověřující správnost přihlašovacích údajů uživatele (na podvodných stránkách) spustitelný
- nastavit `cron`, aby v určitý čas spouštěl PHP skript `mailSender.php`

Pozn.: veškeré uvedené relativní cesty a soubory se vztahují k adresářové struktuře a zdrojovým souborům aplikace *Phishingator*

B Popis databázových tabulek

Protože vytvořená aplikace *Phishingator* obsahuje několik databázových tabulek, na kterých je její běh závislý, je účel všech těchto tabulek a jejich významnější atributy popsán v následujících podkapitolách (v abecedním pořadí).

B.1 phg_campaigns

Sdružuje informace o každé vytvořené kampani (název, datum spuštění a ukončení kampaně apod.) a obsahuje řadu cizích klíčů, a sice:

- `id_by_user` – uživatel, který kampaň vytvořil (viz podkapitola B.9)
- `id_email` – podvodný e-mail, který bude v rámci kampaně rozeslán zvoleným příjemcům (viz podkapitola B.6)
- `id_website` – podvodná webová stránka, která bude dostupná z vybraného podvodného e-mailu (viz podkapitola B.14)
- `id_onsubmit` – akce, která se stane po odeslání formuláře na podvodné stránce (viz podkapitola B.2)

Všechny atributy této tabulky musí být vyplněny a nemohou obsahovat hodnotu `NULL`.

B.2 phg_campaigns_onsubmit

Obsahuje seznam akcí, které se stanou po odeslání formuláře na podvodné stránce a ze kterých si tvůrce kampaně (buď uživatel s oprávněním *správce testů* nebo *administrátor*) může vybrat při jejím vytváření. Tvůrce kampaně si tak může zvolit, zdali se při odeslání formuláře např. nic nestane, nebo zdali dojde k přesměrování na konkrétní webovou stránku (např. na pravé webové stránky pro zmatení uživatele) apod.

Tabulka obsahuje 5 různých předpřipravených možností, které mohou po odeslání zmíněného formuláře nastat.

B.3 phg_campaigns_recipients

Tabulka shromažďuje přihlášení a odhlášení uživatelů (resp. příjemců podvodných e-mailů) ke všem vytvořeným kampaním.

Každý záznam vyjma vlastního identifikátoru obsahuje následující atributy:

- `id_campaign` – kampaň, do které je uživatel přihlašován/odhlašován
- `id_user` – uživatel, který má být do kampaně přihlášen/odhlášen
- `id_sign_by_user` – uživatel (buď *správce testů*, nebo *administrátor*), který konkrétního příjemce (viz atribut `id_user`) do kampaně přihlašuje, nebo ho z ní odhlašuje
- `sign_date` – datum a čas přihlášení, nebo odhlášení uživatele z kampaně
- `signed` – nabývá hodnoty buď `1`, pokud je uživatel do kampaně přihlašován, nebo hodnoty `0`, pokud je z ní naopak odhlašován

B.4 phg_captured_data

Tabulka slouží pro uložení všech zaznamenaných akcí provedených na podvodných stránkách.

Obsahuje řadu informací o uživateli (jako jeho IP adresu, informace o použitém webovém prohlížeči a konfiguraci operačního systému – pozn. tato data lze podvrhnout odborným zásahem na straně uživatele), dále pak HTTP POST data ve formátu JSON obsahující data zadaná ve formuláři na podvodné stránce (vyplněná hesla jsou ve výchozím režimu jsou anonymizována) a stejně tak informaci o tom, zdali přihlašovací údaje zadané do formuláře byly platné (atribut `result`) a kdy k dané akci došlo (`visit_datetime`).

V tabulce se dále nacházejí následující cizí klíče:

- `id_campaign` – kampaň, pod kterou zaznamenaná aktivita spadá (pro generování statistiky)
- `id_user` – uživatel, který danou aktivitu provedl
- `id_action` – akce, kterou uživatel na podvodné stránce provedl (viz podkapitola B.5)

B.5 phg_captured_data_actions

Tabulka obsahuje seznam možností, jak může uživatel (resp. účastník kampaně) reagovat na zaslaný e-mail, popř. na podvodnou stránku přístupnou z tohoto e-mailu. Seznam akcí (a tedy obsah tabulky) je následující:

1. *bez reakce* – e-mail byl uživateli doručen, ale na odkaz v něm uvedený a vedoucí na podvodnou stránku, neklikl

2. *návštěva stránky* – uživatel navštívil podvodnou stránku přístupnou z phishingového e-mailu, ale nic zde nevyplňoval

3. *zadání neplatných údajů* – uživatel do formuláře na podvodné stránce zadal neplatné přihlašovací údaje

4. *zadání platných údajů* – uživatel do formuláře na podvodné stránce zadal platné přihlašovací údaje

U každé této akce je i uvedena barva v hexadecimálním tvaru (atribut `hex_color`) a název CSS třídy (`css_color_class`), na základě které jsou odlišeny výpisy a statistika ve vytvořené webové aplikaci.

B.6 phg_emails

Zahrnuje všechny vytvořené cvičné phishingové e-maily.

U každého záznamu je v cizím klíči `id_by_user` uvedeno, jakým uživatelem byl záznam přidán do databáze. Dále jsou součástí tabulky atributy týkající se samotného e-mailu – předmět, tělo e-mailu, e-mail odesílatele a nepovinně pak jméno odesílatele e-mailu.

B.7 phg_emails_indications

Tabulka obsahuje seznam indicií k rozpoznání phishingu a sociálního inženýrství u již přidaných cvičných phishingových e-mailů (viz podkapitola B.6).

U každého záznamu je uveden cizí klíč na uživatele, který danou indicii přidal (`id_by_user`) a dále pak cizí klíč na podvodný e-mail (`id_email`), kterého se daná indicie týká. Ostatní atributy slouží pro definování obsahu indicie.

B.8 phg_sent_emails

Tabulka obsahuje záznamy o již zaslaných podvodných e-mailech v následující podobě:

- `id_campaign` – kampaň, se kterou je podvodný e-mail svázán
- `id_email` – konkrétní e-mail, který byl uživateli odeslán
- `id_user` – uživatel, kterému se phishingový e-mail odeslal
- `date_sent` – datum a čas odeslání e-mailu

V podstatě se tedy jedná o seznam již odeslaných e-mailů, pomocí kterého se řídí systém při odesílání dosud neposlaných e-mailů.

B.9 phg_users

V této tabulce se nachází seznam všech uživatelů, kteří měli někdy něco společného s vytvořenou aplikací.

Uživatelé se do aplikace mohou buď sami dobrovolně přihlásit, nebo je přidá *administrátor*, či je do aplikace automaticky zaeviduje systém na základě účasti v některé z kampaní (opět buď způsobeno činností *administrátora* nebo *správcem testů*). Tento stav je rovněž zohledněn v atributu `id_by_user`.

Mezi podstatnější atributy tabulky patří:

- `id_by_user` – obsahuje buď ID uživatele, který uživatele do systému přidal, nebo hodnotu `NULL`, která označuje uživatele, jenž se do systému přihlásil dobrovolně
- `id_user_group` – uživatelská skupina, do které je uživatel zařazen, a na základě které získává v systému konkrétní oprávnění (viz podkapitola B.10)
- `url` – jedinečný řetězec pro každého uživatele složený ze znaků anglické abecedy a čísel (ve výchozím stavu o celkové délce 6 znaků – lze změnit v konfiguračním souboru aplikace), který slouží k přístupu a identifikaci uživatele na podvodných stránkách
- `username` – uživatelské jméno pro přístup do systému
- `email` – e-mail uživatele, na který budou zasílány cvičné phishingové e-maily
- `recieve_email` – obsahuje hodnotu `1`, pokud si uživatel přeje dobrovolně přijímat cvičné phishingové e-maily, nebo `0`, pokud nikoliv
- `email_limit` – limit počtu cvičných phishingových e-mailů, které si uživatel ještě přeje obdržet (hodnota je při každém odeslání e-mailu dekrementována), popř. hodnota `NULL`, pokud limit není stanoven

B.10 phg_users_groups

Shromažďuje informace o uživatelských skupinách, do kterých jsou uživatelé v rámci systému zařazeni. Na základě těchto skupin pak uživatelé získávají

oprávnění v systému, přičemž jeden uživatel může být zařazen pouze v jedné skupině. Významnějšími atributy jsou:

- `id_by_user` – uživatel, který skupinu v systému vytvořil
- `id_parent_group` – rodičovská skupina, do které se uživatelé skupiny přesunou tehdy, pokud *administrátor* danou skupinu odstraní; příp. obsahuje hodnotu `NULL`, jestliže se jedná o rodičovskou, a tedy zároveň neodstranitelnou skupinu
- `role` – oprávnění všech uživatelů ve skupině (viz podkapitola B.13)
- `emails_restrictions` – seznam domén a domén nižších řádů (resp. části e-mailové adresy za znakem `@` včetně tohoto znaku), na které mohou uživatelé skupiny zasílat podvodné e-maily (týká se pouze uživatelů s oprávněním *správce testů*)

B.11 phg_users_login_log

Obsahuje záznamy o datu a čase přihlášení uživatelů do systému včetně použité IP adresy.

B.12 phg_users_participation_log

Slouží k vedení záznamů o dobrovolných přihlášeních a odhlášeních uživatelů k odebírání cvičných phishingových zpráv, a to následujícím způsobem:

- `id_user` – uživatel, který se přihlašuje/odhlašuje k odebírání
- `date_participation` – datum a čas, kdy se uživatel přihlašuje/odhlašuje
- `logged` – nabývá hodnoty `1`, pokud se uživatel k odebírání přihlašuje, případně hodnoty `0`, pokud se z odebírání cvičných phishingových zpráv odhlašuje

B.13 phg_users_roles

Tabulka obsahuje seznam rolí (oprávnění) dostupných v systému.

Tyto role jsou přidělovány uživatelským skupinám (podkapitola B.10), na základě kterých uživatelé získávají konkrétní oprávnění v systému.

B.14 phg_websites

Obsahuje záznamy o všech podvodných webových stránkách, které jsou dále využívány v kampaních (viz podkapitola B.1).

Mezi významné atributy patří atribut `url`, který určuje, na jaké URL adrese bude podvodná stránka dostupná. Tato URL adresa se při odeslání podvodných e-mailů doplňuje do jejich těla na zvolené místo (resp. místo proměnné `%url%`).

Atributem `id_template` je specifikováno, jaký vzhled (resp. šablonu) bude podvodná webová stránka používat (viz podkapitola B.15).

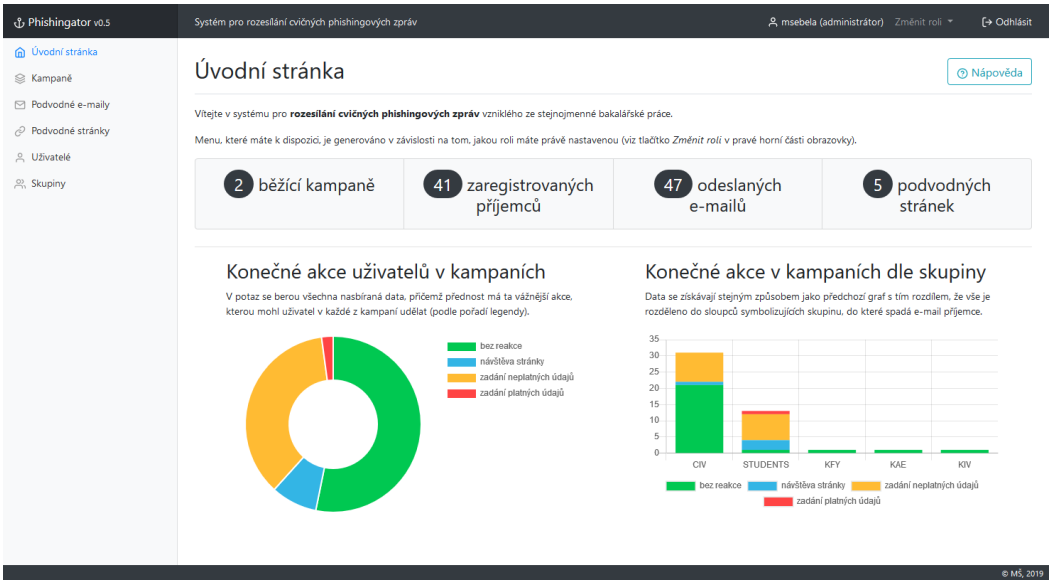
B.15 phg_websites_templates

V tabulce jsou umístěny záznamy o šablonách dostupných na webovém serveru. Šablony jsou určeny k zobrazení na podvodných webových stránkách (viz podkapitola B.14).

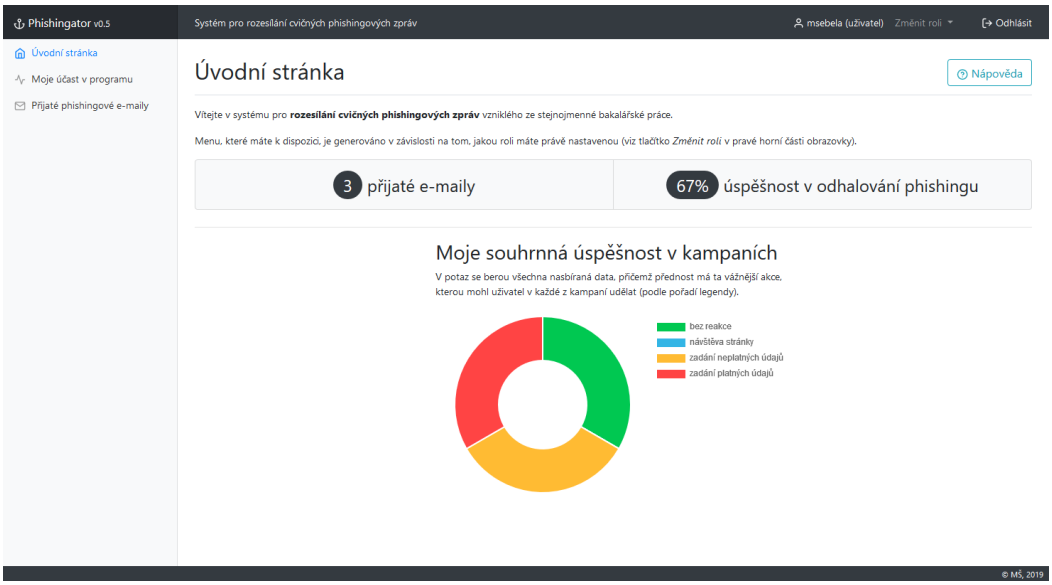
C Obrazová příloha

Na následujících stránkách jsou vybrané screenshoty vytvořené aplikace.

C.1 Úvodní stránka systému

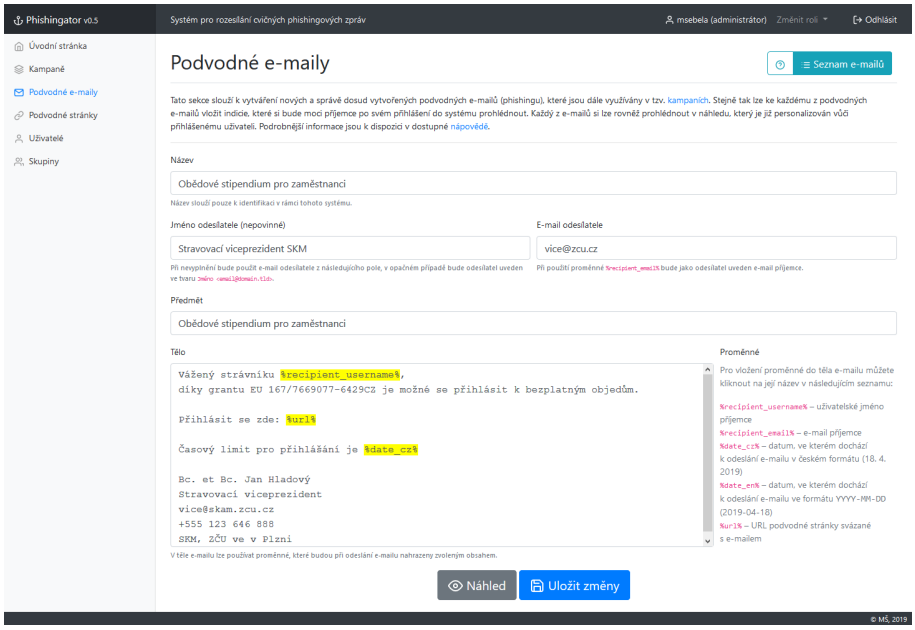


Obrázek 11.1: Úvodní stránka s globální statistikou celého systému určená pro uživatele s oprávněním *administrátor*

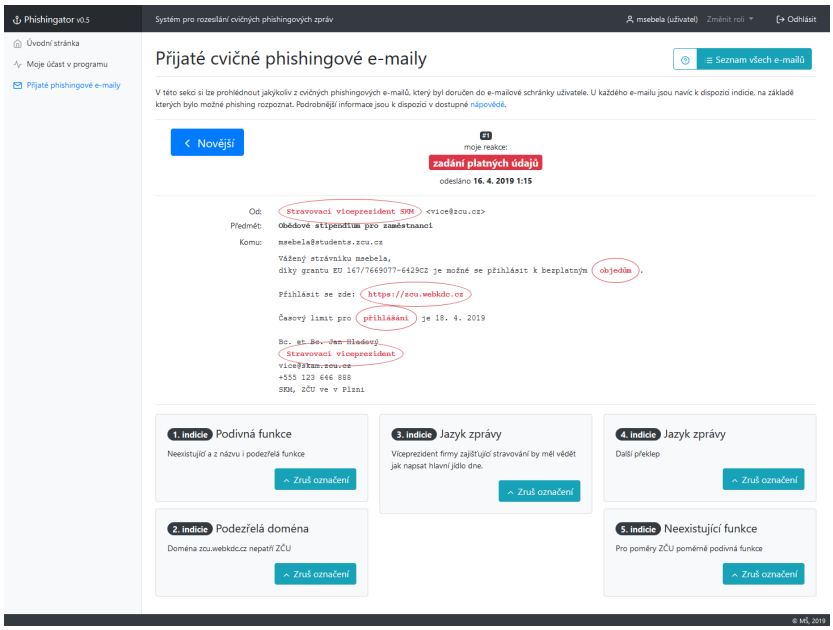


Obrázek 11.2: Úvodní stránka s osobní statistikou uživatele

C.2 Phishingové e-maily a indicie

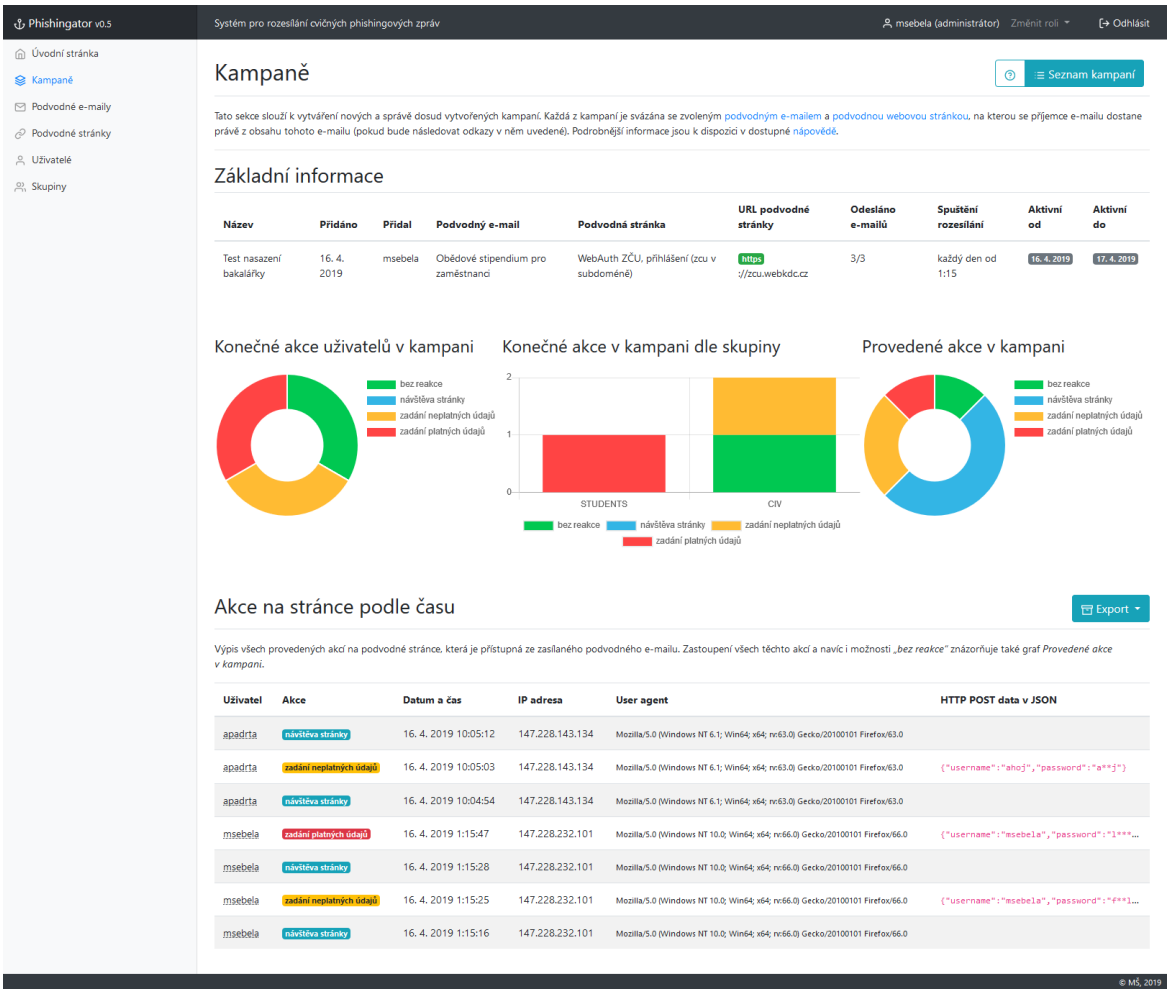


Obrázek 11.3: Úprava podvodného e-mailu s automatickým vyznačením proměnných, které budou při odeslání e-mailu nahrazeny skutečným obsahem



Obrázek 11.4: Jeden z phishingových e-mailů, který uživatel obdržel, vyobrazený společně se seznamem zakroužkovaných indicií, na základě kterých bylo možné phishing rozpoznat a s informací o tom, jak uživatel reagoval

C.3 Statistika pro konkrétní kampaň



Obrázek 11.5: Podrobná statistika pro konkrétní kampaň včetně seznamu všech akcí, které příjemci provedli na podvodné stránce