

# **Etický hacking v kontextu subjektů ochrany obyvatelstva**

Bc. Vít Michálek

---

Diplomová práce  
2023



Univerzita Tomáše Bati ve Zlíně  
Fakulta logistiky a krizového řízení

---

Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav ochrany obyvatelstva

Akademický rok: 2022/2023

## ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Bc. Vít Michálek  
Osobní číslo: L21158  
Studijní program: N1032A020002 Bezpečnost společnosti  
Specializace: Ochrana obyvatelstva  
Forma studia: Kombinovaná  
Téma práce: Etický hacking v kontextu subjektů ochrany obyvatelstva

### Zásady pro vypracování

1. Zpracujte teoretický vstup do problematiky etického hackingu.
2. Analyzujte oblasti etického hackingu a jejich vhodnost pro testování odolnosti subjektů ochrany obyvatelstva.
3. Navrhněte scénář útoku na subjekt ochrany obyvatelstva.
4. Navrhněte doporučení pro zvýšení odolnosti subjektů ochrany obyvatelstva před vybraným útokem.

Forma zpracování diplomové práce: **tištěná/elektronická**

**Seznam doporučené literatury:**

1. COFFEY, Brain. *The Black Book: Ethical Hacking + Reference Book*. Blurb, 2016. ISBN 1367590493.
2. BROOKS, Charles J., Christopher GROW, Philip CRAIG a Donald SHORT. *Cybersecurity essentials*. Indianapolis, Indiana: Sybex, John Wiley, 2018. ISBN 978-1-119-36239-5.
3. HADNAGY, Christopher. *Social Engineering: The Science of Human Hacking*. 2nd Edition. Indianapolis: Wiley, 2018. ISBN 978-1-119-43372-5.

Další odborná literatura dle doporučení vedoucího diplomové práce

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**  
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2022**

Termín odevzdání diplomové práce: **28. dubna 2023**

L.S.

---

**doc. Ing. Zuzana Tučková, Ph.D.**  
děkanka

---

**prof. Ing. Dušan Vičar, CSc.**  
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

## PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užit své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

### Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 28.4.2023

Jméno a příjmení studenta: Bc. Vít Michálek

.....  
podpis studenta

## **ABSTRAKT**

Práce se zabývá konceptem etického hackingu jako nástroje pro zvýšení kybernetické bezpečnosti u subjektů ochrany obyvatelstva. Teoretická část zkoumá současný stav kybernetické bezpečnosti, uvádí základní teoretická východiska problematiky, a dokumenty nezbytné k vymezení kybernetické bezpečnosti.

Praktická část identifikuje phishing jako riziko, kterému čelí nejenom subjekty veřejné ochrany, vymezuje phishingové kampaně jako příklad phishingových útoků a představuje scénář phishingového útoku na nemocniční zařízení. Zjištěné skutečnosti budou aplikovány při tvorbě vlastní phishingové kampaně.

Klíčová slova: etický hacking, kybernetická bezpečnost, ochrany obyvatelstva, phishing

## **ABSTRACT**

This thesis explores the concept of ethical hacking as a tool for enhancing cyber security in public protection entities. The theoretical part examines the current state of cybersecurity, presents the basic theoretical background of the issue, and documents necessary to define cybersecurity.

The practical part identifies phishing as a risk faced not only by public protection entities, defines phishing campaigns as an example of phishing attacks and presents a scenario of a phishing attack on a hospital facility. The findings will be applied to the development of a custom phishing campaign.

Keywords: Cyber security, Ethical Hacking, Phishing, Population Defense

Rád bych touto cestou poděkoval vedoucímu práce Ing. Petru Svobodovi, Ph.D za jeho odbornou pomoc a cenné rady, které mi poskytl během psaní této diplomové práce. Poděkování patří též mojí přítelkyni za podporu a trpělivost v průběhu celého studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

# OBSAH

<b>ÚVOD.....</b>	<b>9</b>
<b>I TEORETICKÁ ČÁST .....</b>	<b>11</b>
1.2 PRÁVNÍ ÚPRAVA KYBERNETICKÉ BEZPEČNOSTI.....	14
1.3 PRÁVNÍ ÚPRAVA KYBERNETICKÉ BEZPEČNOSTI NA EVROPSKÉ ÚROVNI.....	16
<b>2 ETICKÝ HACKING.....</b>	<b>17</b>
2.1 ZÁKLADNÍ POJMY .....	17
2.2 TYPY HACKERŮ .....	19
2.3 NÁSTROJE HACKERŮ .....	22
2.3.1 Password crackers .....	22
2.3.2 Backdoors.....	23
2.3.3 Skenery.....	24
2.4 KALI LINUX .....	25
2.5 KYBERNETICKÉ ÚTOKY .....	25
2.5.1 Rootkity.....	25
2.5.2 Trojské koně.....	26
2.5.3 Počítačové viry.....	27
2.5.4 Počítačovní červi.....	27
2.5.5 Spyware.....	28
2.6 SÍŤOVÉ ÚTOKY .....	28
2.6.1 Zero-Days Vulnerability .....	28
2.6.2 Sniffing.....	29
2.6.3 Man-In-the-Middle.....	29
2.6.4 DoS – Denial of service .....	29
2.7 ÚTOKY NA WEBOVÉ APLIKACE .....	31
2.7.1 Cross-Site Scripting .....	31
2.7.2 SQL injection .....	31
2.7.3 HTTP response splitting.....	32
2.7.4 Penetrační testování .....	32
2.8 SOCIÁLNÍ INŽENÝRSTVÍ.....	33
2.8.1 Phishing.....	34
2.8.2 Typy Phishingu .....	35
2.8.3 Pharming .....	37
<b>3 ORGÁNY OCHRANY OBYVATELSTVA JAKO SUBJEKTY KYBERNETICKÉ BEZPEČNOSTI.....</b>	<b>38</b>
3.1 SUBJEKTY OCHRANY OBYVATELSTVA .....	38
3.2 VÝZNAMNÉ INFORMAČNÍ SYSTÉMY.....	39
3.3 PROVOZOVATELÉ INFORMAČNÍCH SYSTÉMŮ .....	39
3.4 PRVKY KRITICKÉ INFORMAČNÍ INFRASTRUKTURY .....	40

<b>II PRAKTICKÁ ČÁST</b> .....	<b>42</b>
<b>5 PHISHINGOVÁ KAMPAŇ ETICKÉHO HACKERA</b> .....	<b>43</b>
5.1 PŘEDSTAVENÍ SPOLEČNOSTI.....	43
5.2 NÁSTROJ PHISHME .....	43
5.3 TERMINOLOGIE NÁSTROJE PHISHME.....	44
5.4 PREVENTIVNÍ PHISHINGOVÉ ŠKOLENÍ ZAMĚSTANANCŮ .....	45
5.5 PHISHINGOVÉ EMAILY .....	47
5.8 PHISHINGOVÁ KAMPAŇ .....	52
Výsledek phishingové kampaně.....	55
5.9 VYHODNOCENÍ.....	56
<b>6 NÁVRH SCÉNÁŘE PHISHINGOVÉHO ÚTOKU NA SUBJEKT OCHRANY OBYVATELSTVA</b> .....	<b>57</b>
6.2 TVORBA PHISHINGOVÉHO ÚTOKU .....	59
6.2.1 Analýza funkcionality nástroje SET .....	60
6.2.2 Vytvoření spear-phishingového emailu .....	67
6.4 NÁVRH OPATŘENÍ.....	72
<b>ZÁVĚR</b> .....	<b>77</b>
<b>SEZNAM POUŽITÉ LITERATURY</b> .....	<b>78</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK</b> .....	<b>84</b>
<b>SEZNAM OBRÁZKŮ</b> .....	<b>86</b>
<b>SEZNAM GRAFŮ</b> .....	<b>87</b>



## ÚVOD

Kybernetická bezpečnost je v dnešní době velmi důležitým tématem, protože digitální technologie jsou stále více integrovány do našich každodenních životů. S rozvojem technologií a rostoucí závislostí na informačních systémech se kybernetické útoky staly hlavní hrozbou pro bezpečnost a stabilitu nejen subjektů veřejné ochrany. Tyto subjekty jsou zodpovědné mimo jiné i za ochranu kritické infrastruktury, citlivých informací a zachování veřejné bezpečnosti. Proto je nezbytné zavést účinná opatření kybernetické bezpečnosti, pro předcházení kybernetickým útokům a zmírnění jejich dopadu.

Útoky na tyto subjekty mohou mít závažné následky, jak pro občany, tak i národní bezpečnost jako takovou. Proto je nezbytné, aby tyto organizace měly kvalitní bezpečnostní opatření a systémy, které je chrání před kybernetickými útoky a zabezpečují, že jsou důvěrné a citlivé informace uchovávány v bezpečí.

Kybernetická bezpečnost se stává stále důležitějším v kontextu ochrany obyvatelstva, kdy jsou kritické infrastruktury, jako jsou například finanční systémy, elektrické sítě, telekomunikační sítě a zdravotnické zařízení, často cílem kybernetických útoků. Z tohoto důvodu je důležité, aby byly tyto kritické infrastruktury co nejlépe zabezpečeny, a etický hacking může být užitečným nástrojem pro dosažení tohoto cíle.

Etický hacker může pomoci identifikovat a odstranit bezpečnostní problémy a slabiny v informačních systémech a aplikacích, díky čemuž lze zvýšit úroveň bezpečnosti a ochrany. Důležitost zkoumání etického hackingu na subjektech ochrany obyvatelstva tkví v tom, že tyto subjekty jsou náchylnější k útokům a jsou zároveň odpovědné za ochranu obyvatelstva. Vyhodnocení a vylepšení bezpečnostních opatření prostřednictvím etického hackingu může tedy přispět k ochraně obyvatelstva a národní bezpečnosti jako celku

Etický hacking je poměrně nová disciplína v oblasti kybernetické bezpečnosti, která zahrnuje využívání technik a metodologii, které se používají pro hacking, kdy se testuje bezpečnost informačních systémů a aplikací, ale tento proces je prováděn s povolením a za účelem zlepšení bezpečnosti, nikoli za účelem zneužití. Etický hacking může poskytnout cenné poznatky o zranitelnostech a slabinách, které by mohli zneužít hackeři.

Tato diplomová práce se zabývá analýzou využití etického hackingu v kontextu ochrany obyvatelstva a navrhuje konkrétní postupy a metody pro jeho využití.

## CÍLE A METODY

Tato práce si klade za cíl navrhnout scénář útoku etického hacker na subjekt ochrany obyvatelstva a na základě zjištěných skutečností zhodnotit jeho využitelnost v kontextu subjektů ochrany obyvatelstva.

Pro splnění tohoto cíle bude potřebné splnit dílčí cíle:

- Rešerše související problematiky.
- Analyzovat proces kybernetické bezpečnosti na dostupné subjektu podobného rozsahu.
- Navrhnout scénář kybernetického útoku na subjekt ochrany obyvatelstva.
- Navrhnout opatření pro zvýšení kybernetické odolnosti subjektu ochrany obyvatelstva vůči navrženému útoku.

### Použité vědecké metody

- Rešerše – systematické hledání informací a zdrojů k danému tématu, je využita v deskriptivní části práce k definování pojmů.
- Popis – představení zkoumaného subjektu praktické části.
- Analýza – posouzení pravděpodobnosti vzniku jednotlivých kybernetických útoků na vybraný subjekt, užita v praktické části.
- Syntéza – spojení všech jednotlivých částí do konečného celku.
- Pozorování – neboli observace, je vědecká metoda, využívaná k získání dat o sledovaném objektu nebo jevu, využita v praktické části.
- Komparace – je proces porovnávání a hodnocení rozdílů a podobností mezi různými prvky. V rámci návrhu a opatření je využito ke zhodnocení možností a doporučení nejvhodnějšího řešení.
- Dedukce – je logický postup, při kterém se ze všeobecných výroků a pravidel vychází k závěru o konkrétních situacích nebo faktech. V praktické části je využita k formulaci doporučení.
- Indukce – je způsob získávání nových znalostí na základě pozorování a zobecňování z nich, využita je v praktické části.

## **I. TEORETICKÁ ČÁST**

## 1 ÚVOD DO PROBLEMATIKY

S rozmachem moderních technologií, sociálních sítí a všeobecnou dostupností internetu se pojí i potřeba zajišťovat dostatečnou bezpečnost všech osobních informací, které mohou být o uživatelích zveřejněny. Takovéto informace se často dostávají do koloběhu datového provozu i bez přičinění samotných obyvatel – neustále se digitalizují všemožné služby, které lidé využívají často na denní bázi, od poštovních služeb až po zdravotnická zařízení. Proto představuje obrovské riziko jakýkoli únik těchto dat, i přes snahu správců systémů nebo IT bezpečnostních techniků těmto únikům zabránit. V následující kapitole bude rozebrána legislativa, které je nutno věnovat patřičnou pozornost pro pochopení problematiky.

### 1.1 Legislativa

Z pohledu legislativy je nutno rozlišit obecné pojetí kybernetické bezpečnosti, od toho, jak jej může chápat podniková praxe. *„Z hlediska platného práva je totiž nutno odlišovat ochranu kybernetické bezpečnosti státu od dalších forem individuální informační bezpečnosti, tj. od ochrany dat včetně osobních údajů, ochrany obchodního tajemství, ochrany před běžnou trestnou činností zaměřenou k informacím (informační kriminalitou) apod. Bezpečnostní manažer tedy musí pracovat vedle legislativy týkající se přímo kybernetické bezpečnosti též s rozsáhlou trestní, správní a civilní legislativou upravující právní povinnosti, které souvisejí s nejrůznějšími formami získávání, zpracovávání, ukládání a komunikace informací.“* (CyberSecurity.CZ, 2017)

Pro správnou interpretaci kybernetické kriminality je nezbytné vhodné legislativní opatření upravené tak, aby proti ní zajišťovalo účinný boj v preventivní i represivní rovině. Trestní zákoník má dvojí úlohu v oblasti kybernetické bezpečnosti; zajišťuje zpracování, ukládání a komunikaci informací a reaguje na kybernetickou kriminalitu prostřednictvím definice jednotlivých kybernetických trestných činů a ukládáním přísnějších trestů v případě závažných trestných činů. I přestože je legislativní proces často pomalý, jsou legislativní opatření stále jeden z nejučinnějších prostředků v potírání kybernetické kriminality (CyberSecurity.CZ, 2017).

V důsledku rychlého rozvoje kybernetické kriminality mohou vznikat určité komplikace ohledně legislativní úpravy, protože některé nové typy útoků nemohou být podřazeny pod existující trestný čin.

Ačkoliv se trestní právo řídí zásadou analogie v neprospěch pachatele, co můžeme chápat jako situaci, při které není možné posuzovat jako trestný čin takový skutek, který není přímo upraven v zákoně, lze však některé kybernetické útoky podřadit pod zákonem definovaný trestný čin, původně zaměřený na trestné činy spáchané tradičními prostředky.

Nově však vznikají i takové typy útoky, které nelze přiřadit k žádnému trestnému činu, který je ukotven v zákoně. Tyto případy řeší vnitrostátní právní předpisy, které mají za cíl vyplnit tyto právní mezery, čímž ale vzniká značná roztržitost příslušných právních předpisů. V mezinárodním měřítku vzniká snaha o sjednocení vnitrostátních právních úprav v oblasti kyberkriminality, což pomáhá bojovat proti této trestné činnosti (Rauter, 2017).

Po určení správné aplikace zákonných opatření je nutno nejprve identifikovat veškeré subjekty těchto právních vztahů. Internet je jeden ze základních prvků, bez kterého by nemohla vznikat většina kybernetických útoků, proto je potřebné určit nejprve právní subjektivitu tohoto prvku. Dle Koloucha (2016) nemá internet právní subjektivitu. Internet definuje jako systém informačních a telekomunikačních prvků skládajících se ze subjektů práva, tedy účastníků právních vztahů ve formě fyzických a právnických osob. Těmito účastníky mohou být například uživatelé, poskytovatelé služeb apod. Vlastníkem samotného internetu tedy není možné nikoho určit.

Internet je tvořený vzájemně propojenými počítačovými sítěmi. Menší celky jsou zpravidla majetkem nějaké fyzické či právnické osoby, nejčastěji se jedná o poskytovatele internetového připojení, tzv. ISP (Internet Service Provider). Jako vlastník může být kromě fyzických a právnických osob určen i stát. V tomto smyslu lze podle občanského zákoníku považovat internet za věc. Občanský zákoník též stanovuje, že nelze internet považovat za věc hmotnou, jelikož neplní její podstatu.

Souhrnně lze konstatovat, že se nejedná o právo ani nelze říct, že se jedná o věc bez hmotné podstaty, neboť věci hmotné podstaty, tedy informační a komunikační technologie jsou základem internetu, bez kterých nemůže existovat.

Ve zkratce se tedy informační a komunikační technologie nejsou právo a ani věci bez hmotné podstaty, ale hmotné věci, jež utváří základy internetu, nezbytné pro jeho existenci. K této problematice se vyjádřil Smejkal (2015) následovně: „*Věc v právním slova smyslu profiluje její ovladatelnost. Internet jako celek si nelze přivlastnit, ani jej ovládat.*“ Internet je tedy pevně spojen s hmotnou podstatou, tedy s nějakou hmotnou věcí, která má svého vlastníka (Kolouch, 2016).

### **Non-disclosure agreement (NDA)**

Ve spojení s etickým hackingem je nezbytné, aby v této kapitole bylo zmíněno tzv. Non-disclosure agreement (NDA). Přestože se nejedná přímo o legislativní ukotvení hackingu či kybernetické bezpečnosti, má tato smlouva právní základy. Jedná se o písemnou dohodu mezi dvěma nebo více stranami, v níž se vzájemně zavazují nezveřejňovat citlivé informace, které si mezi sebou vyměňují. V podstatě se jedná pojistku firmy, která si najme etického hackera, aby tak ochránil své know-how, obchodní tajemství, technické informace nebo jiná citlivá data, ke kterým tomuto etickému hackerovi mohou umožnit přístup, v případě nutnosti v rámci vykonání jeho služby. Podpisem NDA se obě strany zavazují, že nebudou tuto důvěrnou informaci sdělovat jiným lidem bez předchozího souhlasu druhé strany a že budou přijímat adekvátní opatření k zajištění ochrany této informace. Pokud by došlo k porušení této dohody, může to vést k právním následkům.

## **1.2 Právní úprava kybernetické bezpečnosti**

Kybernetická bezpečnost se stává stále důležitější oblastí zabezpečení moderních informačních a komunikačních technologií. S rostoucími hrozbami kybernetických útoků se také zvyšuje potřeba účinného právního rámce, který by tyto hrozby minimalizoval a poskytoval ochranu jak jednotlivcům, tak celé společnosti.

Tato část se bude věnovat přehledu právního rámce oblasti kybernetické bezpečnosti v rámci České republiky. Budou zde uvedeny hlavní zákony a dokumenty týkající se této oblasti, a detailněji se zaměří na ty, které jsou klíčové pro právní úpravu kybernetické bezpečnosti.

### **Strategie kybernetické bezpečnosti České republiky na období 2021-2025**

V dokumentu jsou uvedeny základní principy kybernetické bezpečnosti České republiky a je zde stanoveno její strategické směřování v této oblasti. Dále dokument uvádí základní vize týkající se kybernetické bezpečnosti.

Podstata této strategie spočívá ve snaze posílit odolnost společnosti a infrastruktury v České republice. To se neobejde bez aktivního přístupu k problematice kybernetických hrozeb a spolupráce s aliančními partnery. Strategie si zakládá na třech základních pilířích:

- *„Sebevědomě v kyberprostoru.*
- *Silní a spolehlivá spojenectví.*
- *Odolná společnost.*“ (NÚKIB, 2020)

V současnosti je ICT neodmyslitelnou částí prakticky všech oblastí ve společnosti, čímž se stávají podstatnějšími cíli pro kybernetické hrozby. Hackeři mohou narušit stabilitu systému jako celku a proto je nutné na tyto hrozby brát zřetel a nepodceňovat je. Pro zajištění bezpečného prostředí je nezbytná včasná identifikace, vyhodnocení kybernetických hrozeb a v neposlední řadě je nutné vytvářet vhodná protiopatření (NÚKIB, 2020).

Konkrétní úkoly v oblasti kybernetické bezpečnosti jsou definovány v Akčním plánu, který vychází z Národní strategie kybernetické bezpečnosti ČR.

### **Akční plán k národní strategii kybernetické bezpečnosti české republiky na období let 2021 až 2025**

Obsahuje aktivity nutné pro splnění cílů Národní strategie kybernetické bezpečnosti v ČR. Podle svých definovaných kompetencí v zákoně 181/2014 Sb. o kybernetické bezpečnosti jsou jednotlivé subjekty zodpovědné za plnění těchto aktivit.

Akční plán k národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025 obsahuje konkrétní opatření, která mají pomoci naplnit cíle strategie. Mezi tato opatření patří například zlepšení ochrany kritické infrastruktury, posílení schopností detekovat a reagovat na kybernetické hrozby, podpora vzdělávání a osvěty v oblasti kybernetické bezpečnosti, či zlepšení spolupráce mezi subjekty odpovědnými za kybernetickou bezpečnost. Akční plán dále rozděluje tyto opatření podle zodpovědných subjektů a stanovuje harmonogram jejich realizace.

Plnění cílů stanovených v akčním plánu probíhá v určeném časovém rámci (NÚKIB, 2021).

### **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně pozdějších souvisejících zákonů**

Obsahem tohoto zákona je definice základních požadavků pro zachování kybernetické bezpečnosti v České republice, dále vymezuje povinnosti subjektů kybernetické bezpečnosti jako jsou správci systému, provozovatelé sítí a poskytovatelé připojení. Zákon také stanovuje, jak postupovat při kybernetických bezpečnostních incidentech a vymezuje pravomoci a povinnosti orgánů působících v této oblasti a v neposlední řadě stanovuje podmínky pro nakládání s informacemi o kybernetické bezpečnosti.

Na základě podpory NATO a Evropské unie byl vytvořen zákon o kybernetické bezpečnosti, který byl motivován narůstajícím počtem DDoS útoků. Jeho cílem je definovat právní rámec pro vznik státní instituce, která bude zodpovědná za zajištění kybernetické bezpečnosti státu a bude regulovat klíčové subjekty. Vzhledem k tomu, že je státní moc uplatňována pouze

na základě zákona, je nutné mít tento zákon, aby bylo možné účinně chránit stát před kybernetickými hrozbami (Doucek, Konečný a Novák, 2019).

### **Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti**

Tato vyhláška reguluje a implementuje Směrnici NIS pro kritické informační infrastruktury, včetně komunikačních systémů, významných informačních systémů, základních služeb a sítí elektronických komunikací využívaných poskytovateli digitálních služeb. Dále stanovuje pravidla pro obsah a strukturu bezpečnostní dokumentace, rozsah a povahu bezpečnostních opatření, typy a kategorie kybernetických bezpečnostních incidentů a jejich hodnocení, náležitosti a způsob hlášení kybernetických bezpečnostních incidentů, oznámení o reaktivních opatřeních a jejich výsledcích, vzor oznámení kontaktních údajů a způsob likvidace dat, provozních údajů, informací a jejich kopií (NÚKIB, 2021, b).

## **1.3 Právní úprava kybernetické bezpečnosti na Evropské úrovni**

Existuje několik mezinárodních dohod a rezolucí týkajících se kybernetické bezpečnosti, které se zaměřují na ochranu práv jednotlivců, mezinárodního obchodu a národní bezpečnosti v kyberprostoru. Nicméně tyto dohody nemají přímou závaznost a realizace závisí na politické vůli jednotlivých zemí.

V Evropě existuje několik iniciativ a dokumentů, jako např.

- Nařízení o kybernetické bezpečnosti (EU) 2019/881 a Směrnice o síťové a informační bezpečnosti (NIS) (EU) 2016/1148, které se týkají kybernetické bezpečnosti a stanoví požadavky na zajištění kybernetické bezpečnosti pro poskytovatele digitálních služeb a kritických služeb.
- Evropská strategie kybernetické bezpečnosti a plán kroku k digitální suverenitě EU poskytují opatření pro zlepšení kybernetické bezpečnosti.
- Agentura EU pro kybernetickou bezpečnost (ENISA) poskytující odbornou podporu.
- Evropská iniciativa pro kybernetickou bezpečnost (ECSO), která má za cíl podporovat inovace a spolupráci v oblasti kybernetické bezpečnosti v rámci EU.



## 2 ETICKÝ HACKING

Následující kapitola se bude zabývat základními pojmy a typy hackerů, kteří jsou často spojováni s kybernetickými útoky. Především půjde o etický hacking, ačkoliv techniky, které hackeři používají k neetickým útokům jsou stejné, jako ty od etických hackerů. Základní pojmy zahrnují vše od kybernetické bezpečnosti a hrozeb, až po typy a způsoby útoků. Následně budou vymezeny typy hackerů od těch, kteří se snaží získat neoprávněný přístup k systémům a sítím, až po ty, kteří se snaží poškodit data nebo organizaci jako celek.

### 2.1 Základní pojmy

**Kybernetická hrozba** je potenciální nebo skutečný nebezpečný pokus nebo útok, který má za cíl poškodit, zneužít nebo kontrolovat počítačový systém, síť nebo informaci. Tyto hrozby se mohou objevit v různých formách, jako jsou například e-maily, stažené soubory nebo připojení k počítačovým sítím. Kybernetické hrozby neustále evolvují a mění se, proto je nutná neustálá ostražitost a implementace adekvátních opatření k ochraně před útoky.

**Kybernetická bezpečnost** – samotná definice kybernetické bezpečnosti není vždy totožná, podle Jiráska, Nováka a Požára kybernetická bezpečnost představuje „...*souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.*“ Kolouch a Bašta (2019) ji popisují jako soubor přijatých opatření pro ochranu počítačového systému před neoprávněným přístupem a útokem.

Důležitými principy kybernetické bezpečnosti jsou i tzv. triády CIA, LTP a PDR. „*Kybernetická bezpečnost v posledním desetiletí získala na významu a stala se tak jednou z hlavních priorit v mnoha národních politikách. Je tomu zejména díky přesahu do jiných bezpečnostních sfér a taktéž díky incidentům, které tento pojem nechvalně proslavily a přiměly i širokou veřejnost přemýšlet o potřebě zabezpečení v kyberprostoru. S tím souvisí potřeba chránit kyberprostor tak, aby v nejvyšší možné míře byla zachována komplexní bezpečnost České republiky a zároveň práva jedinců na informační sebeurčení.*“ (NUKIB, 2017).

**Kybernetický útok** je jakýkoliv neoprávněný nebo nelegitimní pokus o získání přístupu k počítačovému systému nebo síti, nebo pokus o poškození či zneužití těchto systémů nebo sítí. Často je motivací politická či vojenská agenda (Jirásek, Novák a Požár, 2015).

Útoky mohou být provedeny prostřednictvím různých metod, jako je například napadení zranitelností, sociální inženýrství, phishing, DDoS útoky apod. Útoky se mohou týkat jak fyzické infrastruktury, tak i virtuálních systémů a mohou mít různé motivace – od zisku finančních prostředků, krádeže citlivých dat po politické nebo ideologické cíle.

**Počítačový systém** je soubor hardwarového a softwarového vybavení, který spolu koordinuje a řídí počítačové procesy a umožňuje tak uživatelům vykonávat různé úkoly. Hardware počítačového systému zahrnuje fyzické komponenty, jako jsou procesor, paměťové moduly, pevné disky, optické mechaniky, základní deska, napájecí zdroj, periferní zařízení (např. klávesnice, myš, tiskárna, monitor) a další komponenty, které umožňují vytváření a uchovávání dat, zpracovávání informací a provádění různých funkcí počítačového systému. Software zahrnuje operační systém, aplikace a ovladače, které umožňují hardwaru pracovat společně a poskytují uživatelům rozhraní pro práci s počítačem. Počítačové systémy mohou být různé velikosti a složitosti, od jednoduchých počítačů domácnosti až po složité sítě a datová centra.

**Kybernetická událost** je podle zákona o kybernetické bezpečnosti (č. 181/2014 Sb.) taková událost, která může mít vliv na funkčnost informačního systému nebo informační infrastruktury, včetně neoprávněného přístupu k informacím nebo úniku informací, poškození dat, narušení funkčnosti systému nebo jiného nežádoucího vlivu na informační systém nebo informační infrastrukturu.

**Kybernetický incident** definuje zákon o kybernetické bezpečnosti (č. 181/2014 Sb.) v § 7 odst. 2 jako situaci, kdy je narušena bezpečnost informací v informačních systémech nebo kdy je narušena bezpečnost, integrita nebo dostupnost služeb a sítí elektronických komunikací. Jde tedy o situaci, kdy došlo k narušení bezpečnosti v minulosti nebo narušení právě probíhá, což v kybernetické bezpečnosti může být zjištěno u některých útoků až ex-post. Jako příklad lze uvést phishingový e-mail obsahující odkaz na stažení škodlivého malwaru. Pokud uživatel na odkaz neklikne a malware se nespustí, jedná se o kybernetickou událost. V případě stažení a vzniku ohrožení, se jedná o kybernetický incident.

**Kybernetický prostor** je prostředí v digitální podobě, které umožňuje vytváření, zpracování a sdílení informací. Toto prostředí zahrnuje informační systémy, služby a elektronické komunikační sítě (Jirásek, Novák a Požár, 2015).

**Kyberterrorismus** je forma terorismu, která se zaměřuje na útoky proti informačním systémům, datům nebo programům, s cílem způsobit škodu nebo zmařit funkčnost cílových

zařízení. Tato forma terorismu se obvykle provádí s politickým motivem a využívá moderní informační technologie a elektronické sítě. Cílem kyberteroristů je často vyvolat chaos nebo destabilizovat společnost, aniž by způsobili fyzické zranění. Kyberteroristické útoky se většinou odehrávají v kyberprostoru (Správa sítě, 2016).

**Hackingem** se obvykle označují činnosti, které mají za úkol proniknout do digitálních zařízení, sítí nebo programů bez souhlasu majitele zařízení nebo oprávněné osoby. Tyto činnosti mohou mít různé motivace, včetně získání neoprávněného přístupu k informacím, získání finančního prospěchu nebo mohou být páčány pouze pro zábavu. Hacking se však nemusí vždy týkat nezákonných aktivit a může být prováděn jako etický hacking s cílem nalézt zranitelnosti v systému a pomoci vylepšit zabezpečení (Malwarebytes, 2022).

**Zranitelnost** je termín, který označuje existenci slabiny nebo chyby v implementaci, která může vést k bezpečnostní zranitelnosti, které může hacker pomocí exploitů využít a kompromitovat systém.

**Exploit** je útok na systém, navržený tak, aby využil výhody a konkrétní zranitelnost, kterou systémový kód nabízí k získání přístupu k systému, který následně kompromituje. Pokud existuje zranitelnost a exploit jí využije, dosáhne tak přístupu k systému (Bhadoria, 2018).

## 2.2 Typy hackerů

Ačkoliv v současnosti je hacker vnímám především jako pachatel kyberkriminality, v minulosti tento pojem nebyl spojován s tímto negativním významem. Pojem vymysleli studenti Massachusetts Institute of Technology, kteří vytvářeli jeden z prvních počítačů a tímto názvem označovali skupiny programátorů s přiděleným neomezeným přístupem k systému (Završník, 2017).

Kovalčík (2020) popisuje tři skupiny hackerů, které rozlišuje podle barev.

**Black-Hat Hacker**, označován též jako "cracker", je nejznámější typ hackerů, se kterým je hacking obvykle spojován. Jedná se o uživatele hackerských technik k nezákonným nebo škodlivým účelům, jako je krádež osobních informací, narušení nebo zničení počítačových systémů nebo šíření malwaru. Snaží se zneužít chyby v počítačových systémech nebo sítích k nelegitimnímu získání přístupu nebo k poškození systému. Cílem tohoto hackera je zpravidla získat přístup k citlivým datům, způsobit škody nebo získat finanční prostředky. Klasický hacking je nelegální a může být postihován trestním stíháním.

Často používají různé typy malwaru, jako jsou viry, červi, trojské koně a ransomware, sociální inženýrství a využívají známé zranitelnosti systémů k získání neoprávněného přístupu.

**White-Hat Hacker**, známý také jako "etický hacker", je jedinec využívající praktiku hackerských technik za účelem identifikace a odstranění zranitelností počítačových systémů a sítí. Cílem etického hackingu je zlepšit zabezpečení systému nebo sítě než způsobit škodu. Etičtí hackeři používají stejné nástroje a techniky jako Black-Hat hackeři, ale s explicitním svolením vlastníka systému nebo sítě a svá zjištění hlásí příslušným stranám k nápravě. Často jsou zaměstnáváni organizacemi k testování vlastních systémů nebo najímání společnostmi třetích stran k provádění hodnocení zabezpečení. Jejich podstatou je identifikovat potenciální zranitelnosti a doporučit způsoby jejich odstranění.

Etické hackery mohou zaměstnávat organizace, aby testovali jejich vlastní systémy, nebo si je mohou najímat společnosti třetích stran, aby prováděli hodnocení zabezpečení. Etický hacking je na rozdíl od běžného hackingu podle právních předpisů legální. Souhrnně lze říci, že Black-Hat hacking je nelegální a zákeřný, zatímco White-Hat hacking je legální a provádí se za účelem zlepšení bezpečnosti (G. Vishnuram et al., 2022).

**Grey-Hat Hacker** jsou hackeři na pomezí Black-Hat a White-Hat hackerů. Grey-Hat Hackeři jsou osoby, které zneužívají zranitelnosti pro osobní zisk nebo aby upozornily na bezpečnostní problémy, ale obvykle nezpůsobují škodu systémům nebo datům, ke kterým mají přístup. Místo toho se nabourávají jen pro zábavu nebo aby získaly popularitu a uznání v komunitě kybernetické bezpečnosti, což jim nepřímo pomáhá v kariérním růstu jako bezpečnostním profesionálům. Úmysly Grey-Hat Hackerů jsou často dobré, ale ne vždy se při svých hackerských technikách řídí etickými pravidly. Mohou například proniknout na webové stránky, do aplikací nebo IT systémů a hledat zranitelná místa bez souhlasu. Obvykle se však nesnaží způsobit žádnou škodu (G. Vishnuram et al., 2022).

Ačkoliv většina hackerů spadá do jedné z výše zmíněných třech skupin, existují ještě podkategorie hackerů, které Buxton (2022) rozeznává a popisuje taktéž dle barev. Stejně rozdělení podkategorií popisuje ve své práci i G. Vishnuram (2022).

**Red-Hat hackeři** využívají své technické dovednosti a znalosti k ochraně počítačového systému nebo sítě před Black-Hat Hackery. Tito lidé jsou hackeři, kteří se často rozhodnou podniknout agresivní kroky k zastavení Black-Hat Hackerů. Jsou specifictí v tom, že provádějí rozsáhlé útoky s cílem zničit servery a zdroje těchto agresorů. Red-hat hackeři

dosahují zneškodnění hackerů například Infikováním jejich systémů malwarem nebo zahájení DDoS útoků (G. Vishnuram et al.,2022).

**Blue-Hat Hacker** je bezpečnostní profesionál, který je najat, aby pro organizaci provedl penetrační testování nebo etický hacking a aby identifikoval potenciální zranitelnosti v jejích systémech a pomohl zlepšit její bezpečnostní pozici. Pojem "blue hat" označuje neformální klasifikaci bezpečnostních profesionálů. Termín Blue Hat používá také společnost Microsoft pro označení série bezpečnostních instruktáží (Buxton, 2022).

**Green-Hat Hacker** (také noob, newbie atd....) je někdo, kdo s hackingem začíná a nemá téměř žádné znalosti nebo zkušenosti s prací a metodami hackingu nebo souvisejícími technologiemi. Tito hackeři neznají bezpečnostní mechanismy a vnitřní fungování webu, ale nadšeně se učí a jsou odhodláni povýšit své postavení v hackerské komunitě. Ačkoli jejich záměrem není nutně způsobit škodu, mohou tak učinit při "hraní" s různým malwarem a útočnými technikami. V důsledku toho mohou být green-hat hackeři škodliví i proto, že si často neuvědomují důsledky svých činů a častokrát ani to, jak je napravit (G. Vishnuram et al.,2022).

**Script Kiddie** jsou také amatérští hackeři, ale místo toho, aby se učili nové hackerské techniky a programování, mají jednoduše zájem stáhnout nebo koupit malware, nástroje a skripty online a používat je. Hlavní rozdíl mezi Green-Hat a Script Kiddie spočívá v tom, že ti první jsou poměrně seriózní a pracovití a mají jasnou vizi zdokonalovat své dovednosti. Ti druzí se naopak zajímají pouze o používání již existujících skriptů a kódů k hackování. Green hat hackeři se často vydávají cestou řádného vzdělání, získávají certifikáty a navštěvují kurzy rozvoje dovedností, aby se naučili hackovat. Kdežto Script Kiddies si jednoduše najdou zkratky, jako je sledování videí na YouTube nebo čtení některých internetových článků či diskusí na fórech. V podstatě rádi provádějí hackerské útoky a kybernetické útoky, aniž by měli úplné znalosti o jejich důsledcích (Houser, 2013).

**Hacktivist** je hacker, který se nabourává do webových stránek nebo domovských stránek organizací obvykle za účelem zveřejnění sociálního, ideologického, kulturního nebo politického poselství. Nezajímají se o následky svého hackerského útoku a jejich cílem je oběť nenávratně poškodit. Obvykle jde o znehodnocení webu nebo stránky a útočí s cílem odepřít uživatelům služby (Houser, 2013).

Po celém světě existuje mnoho hacktivistických skupin, které usilují o různé, i když někdy stejné cíle – narušit nebo odhalit vnitřní fungování vládních nebo soukromých organizací

ve jménu transparentnosti a veřejného blaha. Nejznámější z těchto typů hacktivistických skupin je skupina známá jako "Anonymous". Hacktivistická skupina Anonymous, která vznikla v roce 2008, se dostala do povědomí díky odhalení scientologické církve prostřednictvím úniku videa s Tomem Cruisem na YouTube. Po žádostech vedení scientologické církve o stažení videa Anonymous pokračovali v útoku typu Distributed Denial of Service (DDoS), který vedl ke zničení internetových stránek církve. Od té doby skupina pokračuje ve svých kampaních formou online protestů s častými DDoS útoky. Ve snaze přinést světu svou verzi spravedlnosti se zaměřila i na teroristickou skupinu ISIS (G. Vishnuram et al., 2022).

## 2.3 Nástroje hackerů

Tato kapitola bude zaměřena na nástroje používané hackery jak klasickými, tak i etickými k provádění útoků na počítačové systémy. Kapitola shrne nejčastější nástroje používané k útokům na hesla, získání neautorizovaného přístupu k systému, průzkum sítě a další útoky.

### 2.3.1 Password crackers

Password crackery neboli prolamovače hesel jsou nástroje nebo programy používané k získání neautorizovaného přístupu k chráněným systémům nebo datům tím, že zkouší prolomit hesla a přihlašovací údaje uživatele. Základní princip fungování spočívá v zadávání všech možných kombinací znaků, a snaží se tak správné heslo rozluštit. Prolamovače hesel používají dva základní typy útoků.

**Brute force attacks** (útoky hrubou silou) je technika prolomení hesla, kdy útočník pokouší všechny možné kombinace znaků, dokud nenajde správné heslo. Tato technika je velmi časově náročná a vyžaduje silný výpočetní výkon, protože útočník musí projít obrovské množství možností.

**Slovníkové útoky** spočívají v tom, že útočník používá seznam běžných hesel nebo slovníků slov, aby uhádl správné heslo. Útočník může použít také různé varianty slov, například přidávat čísla nebo speciální znaky. Slovníkový útok může být mnohem rychlejší než brute force attack, protože útočník používá seznam slov nebo frází, které jsou pravděpodobnější, že se používají jako hesla.

Slovníkové útoky využívají takzvané wordlisty, to jsou seznamy slov a frází, které jsou používány jako zdroj pro slovníkové útoky. Tyto seznamy mohou být vytvořeny ručně nebo pomocí softwaru a mohou obsahovat různé kombinace slov a frází, například hesla

z nejčastěji používaných hesel, jména a příjmení, data narození atd. Password crackery zkouší všechna slova a fráze v seznamu, dokud nenajdou shodu s chráněným heslem. Tyto útoky jsou mnohem rychlejší než útoky hrubou silou a mohou být úspěšné, pokud je použité heslo součástí wordlistu. Tyto nástroje jsou často snadné na použití a mají graficky kvalitně zpracované uživatelské rozhraní. Kvalitu těchto nástrojů lze hodnotit podle toho, jaký obsah mají jejich slovníky, a především podle rychlosti jakou dokážou ověřit hesla, která byla vygenerována. Rychlost prolamovače hesel se odvíjí od použitého hardwaru, nejčastěji procesoru počítače, na kterém je spuštěn ale ovlivňuje je i typ hesla, umístění souborů nebo struktura kódového souboru (Techtarget, 2021).

### 2.3.2 Backdoors

Backdoors (zadní vrátka) je způsob, jakým se mohou útočníci dostat do systému nebo aplikace a získat přístup k informacím, aniž by museli použít standardní autentizační procesy. Backdoor může být vytvořen záměrně programátorem jako způsob, jak se dostat do systému pro účely údržby nebo ladění, nebo může být vytvořen útočníkem, který se pokouší obejít bezpečnostní opatření. Backdoors může být kódově vložen do aplikace nebo systému a může být spuštěn pouze specifickou sekvencí příkazů, aby se otevřel neautorizovaný přístup. Může také být vytvořen jako samostatná aplikace, která se instaluje na cílovém zařízení, aby umožnila útočnickovi vzdálený přístup. Zpravidla se jako backdoors označuje cokoli, co umožňuje oklikou získat přístup k systému nebo datům, které jsou chráněny před neoprávněným přístupem.

Výrobci mohou úmyslně do svých zařízení vkládat backdoors, jako příklad lze uvést výchozí heslo pro přihlášení k routeru. Pokud není změněno přímo uživatelem, může být heslo snadno zneužito. V některých případech jsou backdoors vytvářeny samotnými vývojáři nebo správci systému jako prostředek pro vzdálenou správu systému nebo v případě nouze. Nicméně, backdoors mohou být také vytvořeny útočníky nebo hackery, kteří chtějí získat neoprávněný přístup k systému a informacím, a tak umožňují útočnickovi přístup do systému bez znalosti hesla nebo jiného ověřovacího mechanismu. Výsledkem může být zneužití systému k odcizení dat, šíření virů, provádění škodlivých činností nebo dalších útoků (Jirovský, 2007).

Backdoor je často těžké odhalit, pokud je jeho funkce správná a není využíván příliš často. Nejčastěji jsou ukryty pod názvy procesů běžících na pozadí, které mohou mít stejné názvy, jako reálné procesy operačního systému. Mezi útočníkem a infikovaným zařízením probíhá

komunikace pomocí nástrojů, které jsou spuštěny na portech s vysokými čísly. Další možností je ukrytí této komunikace pod standardní služby, jako například http (port 80) nebo ssh (port 22). To však může být riskantní, protože tyto služby nemusí být detekovány a zablokovány firewallem (Jirovský, 2007).

Během roku 2021 se začaly objevovat zprávy o novém malware fungujícím na principu backdoor, který dostal název MysterySnail. Za odhalení stojí společnost Kaspersky. Tento malware zneužívá na zařízeních s operačním systémem Windows vzniklou chybu v zabezpečení v ovladači Win32k, čímž útočník dostává možnost získat přístup k počítači poškozeného a uděluje mu vyšší uživatelská oprávnění. Microsoft tuto chybu opravil již během prvních pár měsíců. Tuto zneužitelnost bylo možno provést na zařízeních s operačním systémem Windows 7 až po nejnovější Windows 11 a Windows 2022, které nebyly aktualizovány proti této chybě (Larin a Raiu, 2022).

### 2.3.3 Skenery

Skenery slouží k prohledávání sítě a identifikaci aktivních síťových zařízení a portů, které jsou na nich otevřené. Tyto nástroje mohou být použity pro různé účely, jako je zajištění bezpečnosti sítě, identifikace síťových chyb a hledání chyb v konfiguraci. Skenery pracují tím, že odesílají zprávy na různé porty a čekají na odpovědi. Pokud je port otevřený a aktivní, zařízení pošle odpověď, která indikuje, že port je aktivní a připravený na připojení.

Síťové skenování je proces, který zahrnuje různé techniky pro zjištění informací o sítích a systémech, jako jsou aktivní hostitelé, porty, služby a operační systémy, které jsou využívány cílovou organizací. Tento proces také umožňuje identifikovat zranitelnosti a hrozby v síti. Síťové skenování může být využito k získání informací o cílové organizaci, což bývá obvykle první krok před zahájením útoku (Co je skenování portů, 2022).

#### *Flipper Zero*

Jedná se o open-source hardware nástroj pro penetrační testování, hacking a výzkum kybernetické bezpečnosti. Flipper Zero bylo možno vytvořit za podpory přispěvatelů na portálu Kickstarter, kde vybral osmdesátinásobek požadované částky, která činila 60 000 \$, na tuto částku přispělo před 37 000 podporovatelů. Zařízení existuje od začátku roku 2021 a v současné době se prodává na Amazonu za přibližně 250 dolarů. Zařízení disponuje řadou možností připojení a funkcí, jako je emulátor RFID, NFC, Bluetooth a klonování digitálních přístupových klíčů. Některé funkce zařízení mohou být na hranici mezi legálním a nelegálním hackováním. Autor však tvrdí, že hackování je spíše prostředkem k vyjádření



zvědavosti a učení než k porušování zákona za účelem finančního zisku nebo slávy (SecureWorld, 2022).

Flipper Zero se používá pro testování zabezpečení a průnik do různých zařízení a systémů, jako jsou bezdrátové sítě, mobilní telefony, dveře, auta a další. Umožňuje provádět různé útoky, jako jsou útoky na hesla, útoky na síťové protokoly, manipulaci se signály a další. Přístroj lze ovládat pomocí tlačítek, dotykového displeje nebo pomocí mobilní aplikace. Obsahuje také port pro připojení rozšíření a může být napájen pomocí USB.

## 2.4 Kali linux

Kali Linux je operační systém založený na Linuxu, který je specializovaný na testování zabezpečení a provádění různých typů penetračních testů a bezpečnostních auditů. Obsahuje předinstalované nástroje pro skenování sítí, exploity, průzkum webů, prolomení hesel, forenzní analýzu a další úkoly, které pomáhají odborníkům na kybernetickou bezpečnost identifikovat a řešit zranitelnosti a bezpečnostní hrozby. Kali Linux je vyvíjen a udržován firmou Offensive Security, která se specializuje na bezpečnostní školení a penetrační testování. Díky tomu, že je Kali Linux vybaven širokou škálou nástrojů pro testování zabezpečení, je oblíbeným operačním systémem mezi profesionálními penetračními testery a bezpečnostními specialisty. Kali Linux je volně dostupný ke stažení a použití a lze jej nainstalovat na běžné počítače nebo použít jako virtuální stroj v prostředí virtualizace. Obsahuje více než 600 předinstalovaných nástrojů pro penetrační testování a zabezpečení sítě. Je důležité mít na paměti, že systém je určen pro legální a etické testování zabezpečení a jeho použití k nelegálním účelům může být trestné (Kali Linux, 2023).

## 2.5 Kybernetické útoky

Kybernetické útoky jsou záměrné pokusy ovlivnit, poškodit nebo získat neoprávněný přístup k počítačovým systémům, sítím nebo zařízením. Tyto útoky mohou být prováděny různými způsoby, jako jsou například útoky na hesla, malware, útoky prostřednictvím virů a červů apod. Cílem kybernetických útoků je získat citlivé informace nebo způsobit škodu.

### 2.5.1 Rootkity

Rootkit je druh malwaru, který skrývá svou existenci na infikované počítači a umožňuje útočnickovi udržovat neoprávněný přístup a kontrolu nad cizím počítačem. Tento přístup představuje velké riziko hlavně proto, že útočník se dostává do režimu správce, což mu umožňuje provádět prakticky jakékoliv operace. Rootkity se snaží zůstat utajeny

před uživatelem a na rozdíl od virů a červů se ani nijak nereplikují. Kombinace těch umožněných oprávnění a toho, že jsou rootkity většinou dobře skryty má za následek jejich velmi obtížnou detekci. Často je poté jediným východiskem přeinstalace celého operačního systému, protože rootkity se často mohou dostat až do jádra systému. Jedná se tedy o soubor technik pro skrývání činnosti prováděných na operačním systému, které umožňují hackerovi získat neomezený přístup ke stroji (Alenezi et al., 2020).

Rootkity se dělí do 4 hlavních typů:

- Hardwarový (firmwarový) rootkit.
- Bootloader rootkit.
- Paměťový rootkit.
- Kernel mode rootkit.

Rootkity se dostaly do podvědomí díky skandálu společnosti Sony, která vložila do svých hudebních CD systém XCP, pro ochranu autorských práv. Tento systém se poté automaticky nainstaloval uživateli do počítače, a nebylo možné jej odstranit. Sony byla donucena vydat opravný program, který ale na místo řešení problému vytvořil další v podobě bezpečnostní díry. Situaci vyřešilo až stažení všech CD se systémem XCP z oběhu (Jirovský, 2007).

### 2.5.2 Trojské koně

Trojský kůň je druh škodlivého softwaru (malware), který se maskuje jako legitimní program, aby uživatele přiměl k jeho instalaci a následnému spuštění. Jakmile je trojský kůň spuštěn, může provést různé škodlivé aktivity, jako například odcizit data, ovládat počítač z dálky, instalovat další škodlivý software nebo sloužit jako zadní vrátka (backdoor) pro útočníky k získání neoprávněného přístupu do systému.

Název trojský kůň pochází z řecké mytologie, konkrétně z příběhu o pádu Troje. Tento příběh poskytuje dobrý obraz toho, jak trojský kůň využívá maskování, aby pronikl do cílového systému a způsobil škodu. Slangově se tento vir označuje jako „Trojan“, tento termín je taky nejčastěji detekovaný antivirem v případě nalezení programu, který nepochází z legitimního zdroje a snaží se provést v počítači změny (Coffey, 2016).

Tyto malé programy jsou distribuovány v kódech nebo hrách, které jsou často k dispozici ke stažení zdarma a slouží k různým účelům, jako je sledování činnosti počítače nebo útoky typu DoS. Často se jedná o freeware programy nebo pirátské verze (Clark, Cobb, 2022).

Hlavní rozdíl mezi trojským koněm a virem či červem je v tom, že trojské koně nejsou schopni se sami replikovat a rozšiřovat do dalších programů. Je však možné tyto nástroje kombinovat, kdy například počítačový červ infikuje počítač, do kterého nainstaluje trojského koně.

### 2.5.3 Počítačové viry

Počítačový virus funguje na principu vkládání svého kódu do existujícího spustitelného souboru nebo systémové složky. Když je tento infikovaný soubor spuštěn, virus se aktivuje a začne se šířit dál na další soubory nebo počítače

Ke svému fungování potřebuje virus nějaký program, do kterého se může infiltrovat a také lidský zásah pro prvotní spuštění, aby se mohl dále rozšířit. Při spuštění tohoto hostitelského programu je zároveň aktivován i virus, který začne své kopie a škodlivé kódy replikovat dále a tím způsobit poškození zařízení. Virus se může přenést mezi počítači pomocí lidské iniciativy nebo počítačové sítě. Každý virus musí mít vyhledávací algoritmus a instrukce pro replikaci kódu (Avast, 2021).

Virus se skládá z infekčního mechanismu, spouštěče a payloadu, což je část dat, která plní jeho škodlivý účel. To tedy znamená, že k jeho spuštění je potřeba nějaký impulz ze strany uživatele. Virus se snaží obejít antivirový software pomocí komplexních anti detekčních strategií (Noyes, 2022).

### 2.5.4 Počítačové červi

Počítačový červ specifický počítačový program, který má schopnost automaticky vytvářet svoje kopie, které následně rozšiřuje do dalších souborů a nebo na další zařízení pomocí počítačové sítě. Nedostatečné zabezpečení počítače je často primární faktor, který umožňuje nákazu a vytváří možnost další replikace. Rozdíl mezi počítačovým červem a virem je zejména ve formě, jakou se šíří. Červ se umí samovolně replikovat do dalších počítačových systémů, kdežto virus je často maskován do nějakých spustitelných souborů, dokumentů anebo spustitelných příloh v emailů a jeho aktivace tedy závisí od manuálního spuštění uživatelem (Avast, 2021).

Je několik druhů počítačových červů. Jejich dělení závisí od způsobu jejich šíření:

- **Emailové červi** – jedním ze způsobů je šíření pomocí internetové pošty. Červ po infikování počítače rozešle na adresy uložené v adresáři napadeného zprávy obsahující škodlivý program, případně přímý odkaz na infikovanou stránku.

- **Internetový červ** – tento druh skenuje síťové prostředky a vyhledá další zařízení v jedné síti. V případě, že sken objeví další zranitelný počítač, červ se do něj rozšíří a nainstaluje i zde škodlivý kód.
- **IM a IRC červi** – využívají různé komunikátory v reálném čase pomocí nichž šíří škodlivé zprávy se spustitelnými soubory případně odkazy na infikované stránky.
- **Červi šířící se pomocí sdílených umístění v počítači** – Tento typ kopíruje svůj program jako spustitelný soubor na sdílené umístění a po jeho spuštění dojde k infikaci počítače. Tím vznikají tzv. botnety. Ty jsou speciálním případem, kdy jsou počítače infikovány určitým červem a jsou použity k hromadnému rozesílání spamu nebo útoků typu DDoS na cíle útočníků (Hub, 2013).

### 2.5.5 Spyware

Spyware je typ škodlivého softwaru, který se instaluje na počítač bez vědomí uživatele a sleduje jeho aktivity. Spyware může shromažďovat informace o uživateli, jako jsou webové stránky, které navštěvuje, hledaná klíčová slova, přihlašovací údaje a další citlivé informace, které mohou být použity k odcizení identity nebo ke zpomalení výkonu počítače. Spyware se obvykle šíří prostřednictvím nelegálních a nebezpečných stahování nebo instalací softwaru, který obsahuje tento škodlivý kód. Mohou se také šířit prostřednictvím phishingových e-mailů, webových stránek nebo neaktualizovaných softwarových aplikací. (Hadnagy, 2018)

## 2.6 Síťové útoky

Jedná se o útoky cílené na počítačové sítě, jež mají za cíl nejčastěji odposlouchávat síťový provoz. Útočník může pomocí síťových útoků získat informace a data, ke kterým by jinak neměl přístup. Další možností je vyřadit z provozu počítače, servery nebo síťové služby.

### 2.6.1 Zero-Days Vulnerability

Česky známé jako zneužití nulového dne jsou bezpečnostní chyby v softwaru, které jsou nevědomě zapsány do kódu v nově vydané verzi jakéhokoliv programu, a pro které zatím neexistuje žádné oficiální řešení. Tyto chyby mohou být zneužity k neautorizovanému přístupu k systému, odcizení dat nebo jiným útokům na počítačové systémy. Když útočník najde takovou chybu, může ji zneužít k útoku na cílový systém bez toho, aby byl odhalen nebo zablokovan bezpečnostními opatřeními. Souběžně se vývojáři softwaru snaží najít

řešení, aby se chyba mohla opravit. Kromě toho mohou být vydány updaty, které zlepšují bezpečnost systému a minimalizují škody způsobené chybou. Útok zneužitím nulového dne poskytuje útočníkům obrovskou výhodu, protože bezpečnostní ochrana není na tuto chybu připravena. Úspěch útoku závisí na době mezi objevem zneužití a jeho opravou (Zero-Day Vulnerability, 2014).

### **2.6.2 Sniffing**

Sniffing, také známý jako "odposlech", je proces zachytávání a sběru síťového provozu, který prochází přes počítačovou síť. Útočníci mohou tuto techniku využít ke zjištění citlivých informací, jako jsou například hesla, uživatelská jména nebo platební údaje, které jsou přenášeny v nešifrované podobě přes síť. Proti sniffingu mohou být použity opatření jako šifrování komunikace nebo využití zabezpečených protokolů, jako je HTTPS, SSH nebo VPN (Awad a Fairhust, 2018).

### **2.6.3 Man-In-the-Middle**

Man-in-the-Middle (MITM) útok je typem útoku, kdy se útočník zapojí do komunikace dvou stran a předává zprávy mezi nimi, takže si každá strana myslí, že komunikuje s druhou stranou, ale ve skutečnosti komunikuje s útočníkem. Tento typ útoku umožňuje útočníkovi zachytit citlivé informace, jako jsou hesla, uživatelská jména, platební údaje nebo další citlivá data, která se přenášejí mezi komunikujícími stranami, a může také měnit nebo vkládat falešné informace do této komunikace (Awad a Fairhust, 2018).

### **2.6.4 DoS – Denial of service**

Cílem útoku DoS (odepření služby) je zahltit cílovou službu obrovským množstvím požadavků, aby se stala nepoužitelnou a uživatelé se k ní nedostali. Útočník se snaží přetížít cílový server, síť nebo aplikaci takovým množstvím požadavků, že nebudou schopny reagovat na legitimní požadavky uživatelů. DoS útoky mohou být realizovány i například přetížením sítě nebo serveru, zneužitím chyb v aplikaci, využitím tzv. zombie počítačů (botnetů) nebo odesíláním neplatných nebo zfalšovaných požadavků. Tyto útoky mohou být vykonávány ručně nebo pomocí specializovaných nástrojů, které jsou běžně dostupné. V současné době se obvykle používá distribuovaný útok DDoS, kdy jsou požadavky odesílány z mnoha webů, často bez vědomí jejich vlastníků, kteří byli napadeni škodlivým softwarem (Awad a Fairhust, 2018).

DoS útoky je možno rozdělit podle způsobu realizace do dvou kategorií, první kategorie jsou útoky hrubou silou, mezi které se řadí:

- ICMP floods.
- Peer-to-peer attacks.
- Distributed Denial of Service (DDoS).
- Unintentional attack.

DoS útoky, které využívají chyb v aplikaci se dělí na:

- Teardrop attack.
- Nuke.
- LAND attack.
- Slowloris (Imperva, 2022).

### **ICMP floods**

Jedná se o typ útoku na síť, při kterém útočník zahltí cílový server velkým množstvím ICMP (Internet Control Message Protocol) zpráv. Tyto zprávy mohou být například žádosti o odezvu (ping) a útok tak může způsobit přetížení sítě a výpadek služeb.

### **Peer-to-peer attacks**

Tento typ útoku využívá decentralizovanou strukturu peer-to-peer sítí k rychlému šíření škodlivého kódu mezi mnoha počítači bez zjevného centrálního bodu. Útočník může také využít síť k distribuci spamu, phishingových pokusů a jiných typů útoků.

### **Teardrop attack**

Využívá zranitelností v procesu fragmentace IP datagramů. Útočník zasílá zmanipulované fragmenty datagramů, které jsou navrženy tak, aby byly při reasemblování detekovány jako nesprávné, což vede k pádu cílového systému nebo aplikace. Název "teardrop" (slza) je odvozen od tvaru fragmentů, které připomínají slzy. Tento typ útoku je již zastaralý, jelikož moderní operační systémy a firewally obsahují ochranná opatření proti němu (Brooks, Grow, Craig Jr. a Short, 2018).

### **DDoS – Distributed denial of service**

Distribuovaný útok typu DDoS mají za cíl přetížit množstvím požadavků hostitele, server nebo síťový prostředek do té míry, že přestane funkčně poskytovat své služby. Útoky DDoS

jsou navíc tak snadné, že i nezkušený útočník, tzv. script kiddie, může spustit útok, který v síti způsobí spoušť. Je důležité mít plán, jak s těmito útoky bojovat, protože jsou velmi snadno proveditelné a mohou způsobit velké škody. DDoS útoky fungují pomocí množství botnetů, tedy infikovaných počítačů, které je možné spustit vzdáleně a provést tak útok ze stovek či tisíců zařízení najednou. V závislosti na přesné povaze útoku může být výpadek dočasný nebo časově neomezený (Brooks, Grow, Craig Jr. a Short, 2018).

### **Botnet**

Botnet je síť počítačů, které jsou infikovány malwarem (většinou trojským koněm) a jsou ovládány z centrálního místa (řídícího serveru), obvykle bez vědomí majitelů těchto počítačů. Tyto napadené počítače jsou často označovány jako "zombie".

## **2.7 Útoky na webové aplikace**

Útoky na webové aplikace jsou záměrné snahy prolomit zabezpečení webových aplikací a získat neoprávněný přístup k citlivým informacím nebo způsobit škodu. Tyto útoky mohou být prováděny různými způsoby, jako jsou například SQL injection, Cross-site scripting (XSS) nebo http Response Splitting. Cílem útoků na webové aplikace je získat citlivé informace uložené v databázích nebo na serveru, nebo poškodit funkčnost aplikace a způsobit škodu uživatelům.

### **2.7.1 Cross-Site Scripting**

Útoky typu Cross-site scripting (XSS) je typ útoku na webovou aplikaci, při kterém útočník vkládá škodlivý kód (často JavaScript) do webové stránky, a tyto vložené škodlivé kódy nebo skripty se následně spustí v prohlížeči současně s webovou stránkou. Útočník využívá těchto prostředků jako médium pro rozšíření kódů všem, kdo danou infikovanou stránku navštíví. Kódy útočník nejčastěji nahrává pomocí formulářů, tudíž jsou nejzranitelnější ty stránky, kde webová aplikace používá vstup od uživatele. XSS lze využít k ukradení souborů cookies oběti a tím získat citlivé informace. Payload se spustí okamžitě po otevření webové stránky (V. T. En a V. Selvarajah, 2022).

### **2.7.2 SQL injection**

SQL Injection je chyba v bezpečnosti, která umožňuje útočníkovi manipulovat s daty v databázi bez nutnosti mít k nim oprávnění. Tato chyba může postihnout nejen webové aplikace, ale také všechny aplikace pracující s databázemi. Podobně jako u XSS útoku, se

útočník snaží pomocí nezabezpečených vstupů vložit svůj kód do aplikace, aby změnil SQL dotaz. Tím může získávat, upravovat nebo mazat data v databázi, ke kterým by normálně neměl přístup.

Hlavní rozdíl mezi útoky SQL injection a XSS spočívá v tom, že zatímco útoky SQL injection jsou zaměřeny na krádež informací z databází, útoky XSS jsou zaměřeny na přesměrování uživatelů na webové stránky, kde mohou být jejich data odcizeny. Souhrnně lze tedy říci, že SQL injection se zaměřuje na databáze, zatímco XSS útočí na koncové uživatele.

K SQL injection dojde, když je strukturovaný dotazovací jazyk (SQL) vložen do formulářů, souborů cookie nebo hlaviček HTTP, které nepoužívají metody pro ověření nebo dezinfekci dat, takže data odpovídají předepsaným parametrům GET nebo POST. Tato chyba umožňuje útočníkům filtrovat, měnit nebo mazat data z databází připojených k webovým stránkám.

Na druhé straně útoky XSS využívají škodlivý kód k přesměrování uživatelů na škodlivé webové stránky a k odcizení souborů cookie nebo ke zneužití webových stránek. Tyto útoky obvykle provádějí škodlivé skripty, které se spouští v klientských prohlížečích díky vstupům uživatele, funkčním příkazům, klientovým požadavkům nebo jiným výrazům. Útočníci mohou například použít phishingové e-maily nebo e-mailové přílohy s vloženými odkazy ke zneužití škodlivě vytvořených adres URL (SQL vs. XSS Injection Attacks Explained, 2018).

### 2.7.3 HTTP response splitting

HTTP response splitting je bezpečnostní chyba, která využívá nesprávnou validaci uživatelského vstupu. Útočník se snaží vložit do webové aplikace určitý vstup, kterým lze rozdělit původní odpověď serveru na více odpovědí, což může vést k dalším útokům. Tuto zranitelnost lze využít díky neočekávanému řetězci, který útočník vkládá do webové aplikace spolu se vstupem. Tímto způsobem útočník může manipulovat s odpovědí a ovlivnit nejen hlavičku a tělo zprávy, ale také vytvořit další odpovědi zcela pod svou kontrolou (Cyphere, 2022).

### 2.7.4 Penetrační testování

Penetrační testování je proces, který slouží k testování bezpečnosti sítě a jeho hlavním cílem je získat kontrolu nad celou sítí. Sekundárním cílem je identifikovat chyby v síti, které by umožnily útočníkovi získat kontrolu nad sítí. Penetrační testování je tedy vhodnou



metodou pro ověření účinnosti bezpečnostních opatření a identifikaci slabých míst v obraně sítě. Tento proces spočívá v simulaci útoku na síť, což umožňuje otestovat síť a systémy v reálných podmínkách a zjistit, jak dobře jsou chráněny před útoky.

Existuje mnoho různých nástrojů, které mohou být použity při penetračním testování, avšak nejúčinnější je přístup využívá kombinaci manuálních technik a automatizovaných nástrojů.

Manuální techniky zahrnují testování zranitelností a ověření bezpečnosti sítě a systémů pomocí manuálních metod, jako jsou ruční ověřování konfigurace sítě, analýza zdrojových kódů a ověření oprávnění uživatelů. Automatizované nástroje pak slouží k automatizaci části penetračního testování. Tyto nástroje jsou programy nebo sady skriptů, které se používají k rychlému vyhledání zranitelností a ověření bezpečnosti sítě a systémů. Mezi nástroje penetračního testování patří například Kali Linux, Metasploit, Wireshark, w3af, John The Ripper, Nessus, Nmap, Dradis nebo BeEF (Denis a kol., 2016).

Proces penetračního testování zahrnuje několik kroků. Prvním krokem je sběr informací o síti a systémech, které mají být testovány. Poté následuje analýza těchto informací a identifikace možných zranitelností. Následně se provádí samotné testování, během kterého jsou využívány různé techniky pro ověření bezpečnosti sítě a systémů. Výsledky testování jsou následně zhodnoceny a vyhodnoceny, aby bylo možné identifikovat případné zranitelnosti a navrhnout vhodná opatření pro zvýšení bezpečnosti sítě a systémů.

## 2.8 Sociální inženýrství

Sociální inženýrství neboli sociotechnika, funguje na principu psychologické manipulaci lidí, které si klade za cíl oběti ovlivnit a oklamat. Útočník se snaží zmanipulovat oběť tím, že vystupuje pod falešnou identitou a navozuje u oběti pocit důvěryhodnosti, ta mu díky této povedené manipulaci často dobrovolně nevědomky poskytne své osobní informace, které jsou pak snadné zneužít. Tato technika může být u určitého druhu obětí mnohem snazší než překonávání technických zabezpečení, už jen z toho důvodu, že sociotechnici se dokážou chovat v mnoha případech opravdu mile a zdvořile a v lidech tak vzbuzují pocit porozumění a důvěry (Hub, 2013).

Tento koncept útoku je často bagatelizován a lidé často nevěří, že se někdo může nechat takto podvést, ale sociální inženýrství funguje překvapivě dobře i bez nutnosti přílišné pečlivosti nebo sofistikovanosti. Hlavním problémem je, že lidé jsou často příliš důvěřiví

a ochotní. Některé podvody jsou ale naopak tak realistické a dobře provedené, že je možné je rozeznat pouze s extrémní pečlivostí. Běžný uživatel často není schopen ani takto podrobné analýzy, a proto je nejúčinnějším bojem proti této technice obecné vzdělávání v této problematice (Brooks, Grow, Craig Jr. a Short, 2018).

### 2.8.1 Phishing

Phishing je jedním z druhů sociálního inženýrství, který má za úkol získat citlivá data o uživateli jako jsou například hesla či údaje o platební kartě tím, že se vydává za oběti známou organizací. Nejčastěji se jedná o formu emailů, které obsahují odkazy na falešné webové stránky, které na první pohled vypadají jako oficiální stránky nějaké organizace. Na těchto stránkách je připravený formulář k vyplnění. Data, které uživatel vyplní jsou následně odeslány přímo útočníkovi.

I přesto že princip fungování tohoto podvodu je poměrně jednoduchý a snadno odhalitelný, opak je pravdou a phishingové útoky jsou jedny z nejčastějších. Neefektivnějším způsobem, jak se bránit phishingu, je poskytnout uživatelům vzdělání. Samotný vzhled e-mailu nebo webové stránky nemusí být spolehlivým ukazatelem pravosti, protože tyto prvky lze snadno padělat nebo zkopírovat (Brooks, Grow, Craig Jr. a Short, 2018).

Sociální inženýrství i phishing jsou typy útoků na informační bezpečnost, které se zaměřují na využívání lidských chyb a slabostí k dosažení cíle. Nicméně, existují některé rozdíly mezi těmito dvěma koncepty.

Sociální inženýrství je širší pojem, který se vztahuje na jakýkoli druh útoku, při kterém útočník využívá sociálního inženýrství, aby se dostal k informacím nebo zdrojům, ke kterým by jinak neměl přístup. To může zahrnovat různé techniky, jako je například přesvědčování, manipulace, vydávání se za někoho jiného, nebo zneužívání důvěry a ochoty pomoci.

Na druhé straně, phishing je konkrétní typ sociálního inženýrství, při kterém se útočník vydává za důvěryhodnou osobu, organizaci nebo službu s cílem získat citlivé informace, jako jsou například hesla, čísla platebních karet nebo další osobní údaje. Phishing obvykle využívá různé formy podvodné komunikace, například falešné e-maily, webové stránky nebo textové zprávy, které mají vypadat jako legitimní.

Zkráceně řečeno, sociální inženýrství se zaměřuje na využití lidských chyb a slabostí k dosažení cíle, zatímco phishing je konkrétní technikou sociálního inženýrství, která se zaměřuje na získání citlivých informací pomocí podvodné komunikace.

Obecně lze způsob páčání phishingu shrnout do tří metod:

### ***1. Phishing s URL odkazem***

Phishing s URL odkazem je jednou z nejstarších a nejrozšířenějších forem phishingových útoků. Útočníci vytvářejí falešné webové stránky, které vypadají jako legitimní stránky známých společností a organizací. Tyto stránky obsahují formuláře pro zadání citlivých informací, jako jsou hesla, uživatelská jména nebo kreditní karty. Tyto formuláře jsou pak odeslány na webový server útočníka, kde jsou uloženy a mohou být zneužity k podvodům.

### ***2. Phishing s přímým vyžádáním údajů***

V případě phishingových útoků s přímým vyžádáním údajů se útočníci snaží nalákat uživatele k poskytnutí citlivých informací přímo, bez nutnosti kliknout na odkaz nebo otevřít přílohu. Útočník může například zavolat na telefon nebo poslat e-mail s výmluvou, že potřebuje ověřit identitu uživatele a že k tomu potřebuje získat určité informace, jako jsou hesla nebo kódy z autorizačních aplikací. Tento druh phishingu vyžaduje od útočníka více úsilí, jelikož se musí snažit přesvědčit uživatele, aby poskytl citlivé informace.

### ***3. Phishing se zavírovanou přílohou***

Phishingový útok obsahující zavírovanou přílohu spočívá v odeslání e-mailu nebo jiného typu zprávy s přílohou obsahující škodlivý software, například vir nebo malware. Příloha může být například dokument, který vypadá jako faktura nebo jiný oficiální dokument. Pokud uživatel otevře tuto přílohu, software se nainstaluje na jeho počítač a může být použit k odcizení citlivých informací.

## **2.8.2 Typy Phishingu**

Existuje až 19 různých typů phishingu (Fortinet, 2023), z nichž každý má své specifické vlastnosti a cíle. Tyto útoky se liší formou, použitými technikami a účelem. Některé se zaměřují na získání hesel a jiných citlivých údajů, jiné se snaží nalákat oběti na stahování škodlivého softwaru, a další mohou být zaměřeny na podvodné nákupy nebo žádosti o finanční pomoc. Všechny typy phishingu mají společné to, že se snaží vylákat informace od uživatelů tím, že je přesvědčí, aby klikli na odkaz, stáhli soubor nebo zadali své osobní údaje. V této podkapitole budou představeny a popsány některé z nich.

### **Spear Phishing**

Spear phishing spočívá v tom, že se útočník zaměří na konkrétní osobu v organizaci a pokusí se ukrást její přihlašovací údaje. Útočník často před zahájením útoku nejprve shromáždí informace o dané osobě, jako je její jméno, pozice a kontaktní údaje.

### **Clone Phishing**

Klonový phishingový útok spočívá v tom, že hacker vytvoří identickou kopii zprávy, kterou příjemce již obdržel. Do této zprávy uvede frázi jako "posílám znovu" a do e-mailu umístí škodlivý odkaz.

### **Vishing**

Vishing, což je zkratka pro voice phishing, tedy hlasový phishing, je situace, kdy se někdo snaží ukrást informace pomocí telefonu. Útočník může předstírat, že je důvěryhodný přítel či příbuzný, nebo že je zastupuje.

### **Smishing**

Smishing je phishing prostřednictvím nějaké formy textové zprávy nebo SMS.

### **Email Phishing**

Při Emailovém phishingu útočník odešle e-mail, který vypadá jako legitimní a jehož cílem je přimět příjemce, aby v odpovědi nebo na webu zadal informace, které může hacker použít ke krádeži nebo prodeji jeho údajů.

### **Whaling**

Whaling (z angl. whale – velryba) má za cíl vedoucího pracovníka či jiného, pro systém důležitého uživatele. Tito lidé mají často hluboký přístup k citlivým oblastem sítě, takže úspěšný útok může vést k přístupu k cenným informacím celé organizace.

### **HTTPS Phishing**

HTTP phishing je technikou, kdy útočník využívá nedostatečně zabezpečenou komunikaci mezi webovým prohlížečem uživatele a webovým serverem, aby získal citlivé informace. To znamená, že útočník zachytává nešifrovaný provoz mezi prohlížečem a serverem, aby získal přístupové údaje, jako jsou hesla nebo kreditní karty.

### **Evil Twin Phishing**

V případě tohoto útoku hacker vytvoří falešnou síť Wi-Fi, která vypadá jako skutečná. Pokud se do ní někdo přihlásí a zadá citlivé údaje, hacker jeho informace zachytí.

### **Water Hole Phishing**

Při phishingovém útoku typu water hole hacker zjistí, které stránky skupina uživatelů obvykle navštěvuje. Poté ji použije k infikování počítačů uživatelů a pokusí se proniknout do sítě (Fortinet, 2023).

### **2.8.3 Pharming**

Pharming je forma kybernetického útoku, kdy útočník manipuluje s provozem webové stránky s cílem přeměřovat uživatele na falešný web, který vytvořil. Tento falešný web může být například podvodná bankovní stránka nebo internetový obchod. Cílem útočníka je získat citlivé informace, jako jsou uživatelská jména, hesla a finanční údaje (Kolouch a Bašta, 2019).

Pharming se liší od phishingu tím, že nezahrnuje přímou manipulaci s uživateli, ale spíše manipulaci s DNS, aby byl uživatel přeměřován na falešnou stránku.

### **3 ORGÁNY OCHRANY OBYVATELSTVA JAKO SUBJEKTY KYBERNETICKÉ BEZPEČNOSTI**

Modernizace a elektronice všech systémů se nevyhnula ani oblasti veřejné správy a kritických infrastruktur, které se tímto fenoménem postupně propojují. Právě proto je nezbytně nutné vymezovat veškeré tyto kritické body v oblasti kybernetiky a vyvíjet co nejvyšší úsilí pro zachování jejich bezpečnosti.

Tato kapitola bude poskytovat přehled o orgánech ochrany obyvatelstva jako subjektech kybernetické bezpečnosti a jejich roli v ochraně kritické infrastruktury. Kapitola se mimo jiné zaměřuje na významné informační systémy, provozovatele informačních systémů a prvky kritické informační infrastruktury, které jsou pro společnost nezbytné a zároveň jsou vystaveny kybernetickým hrozbám.

#### **3.1 Subjekty ochrany obyvatelstva**

Pro správné vymezení subjektů ochrany obyvatelstva je nutné nejprve definovat samotný pojem ochrana obyvatelstva.

Ochrana obyvatelstva je multidisciplinární obor, který zahrnuje různé aspekty a subjekty, které mají za úkol chránit obyvatelstvo před různými hrozbami a riziky. Tento obor je často označován jako "multiresortní" disciplína, což znamená, že zahrnuje spolupráci a koordinaci mezi různými resorty nebo ministerstvy, které mají v dané oblasti pravomoci a odpovědnosti. Každý z těchto resortů má své specifické znalosti, zdroje a schopnosti, které mohou být využity pro ochranu obyvatelstva. (Koncepte ochrany obyvatelstva do roku 2020 s výhledem do roku 2030)

Při řešení krizových situací, je důležité, aby tyto resorty spolupracovaly a koordinovaly své činnosti. To zahrnuje sdílení informací, plánování a přípravu, koordinaci operací a spolupráci při řešení problémů. Multiresortní přístup k ochraně obyvatelstva umožňuje efektivnější a účinnější reakci na krizové situace, a tím pomáhá chránit životy a majetek obyvatelstva. (Koncepte ochrany obyvatelstva do roku 2020 s výhledem do roku 2030)

Subjekty ochrany obyvatelstva jsou poté organizace nebo skupiny, které mají za úkol chránit obyvatelstvo před nebezpečím, katastrofami, násilím, terorismem a dalšími formami hrozeb. Mezi tyto subjekty mohou patřit například ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory, havarijní služby, organizace pro ochranu lidských práv, nevládní organizace, místní úřady a další instituce. Souhrnně lze tedy říci, že mezi subjekty ochrany

obyvatelstva se řadí všechny orgány, které zajišťují bezpečnost České republiky (MVČR, 2013).

### 3.2 Významné informační systémy

Podle definice v § 2 písm. d) ZoKB jsou významné informační systémy informačními systémy, které jsou spravovány orgány veřejné moci a nejsou považovány za kritickou informační infrastrukturu nebo za informační systémy základní služby. Pokud by došlo k narušení bezpečnosti informací v těchto systémech, může být omezen nebo značně ohrožen výkon orgánu veřejné moci.

Významné informační systémy (dále jen "VIS") jsou definovány jako informační systémy spravované orgány veřejné moci, které nejsou kritickou informační infrastrukturou ani informačními systémy základní služby a u kterých může narušení bezpečnosti informací omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci. Pro určení, zda se jedná o VIS, je tedy nutné splnění všech těchto definičních znaků. Nicméně, pouhé splnění těchto znaků samo o sobě neznamená, že se jedná o VIS a je třeba provést další posouzení.

### 3.3 Provozovatelé informačních systémů

Pro správné porozumění zbytku problematiky je nejprve nezbytné, vymezit si význam pojmů správce a provozovatel informačního systému.

Správce informačního systému je definován v § 2 písm. e) ZoKB jako osoba nebo orgán, který má pravomoc určovat účel zpracování informací a podmínky provozování tohoto systému. Zpravidla existuje pouze jeden správce, který je buďto ten, kdo požaduje vytvoření systému, poskytuje jeho služby nebo mu byla správa systému svěřena na základě právního předpisu. Správce má také výhradní informace o tom, co je součástí systému, zda ho sám provozuje nebo jestli ho provozuje v kooperaci s jinými dodavateli. Správce má schopnost určit role a povinnosti těchto dodavatelů a posoudit, zda jejich činnosti jsou součástí zajišťování funkčnosti technických a programových prvků tvořících systém, a tudíž, zda jsou provozovatelem systému v souladu se zákonem (Núkib, 2023).

Provozovatel informačního systému je osoba nebo organizace, která se aktivně zabývá zajištěním správného fungování technických a programových prvků tvořících daný informační systém, aby mohl poskytovat požadované služby. Tento proces zahrnuje nejen jednorázovou dodávku technických a programových prvků, ale také následné činnosti, jako jsou opravy, aktualizace softwaru a implementace nových technologií (Núkib, 2023).

### 3.4 Prvky kritické informační infrastruktury

Prvky kritické infrastruktury (dále PKI) se určují na základě průřezových a odvětvových kritérií a obecně zde řadíme budovy, zařízení a veřejnou infrastrukturu. Informační systém lze mezi prvky PKI zařadit za předpokladu, že je platné ale aspoň jedno průřezové a jedno odvětvové kritérium. V případě, že jde přímo o systém některé organizační složky státu, je tento systém zahrnut do seznamu kritické infrastruktury vytvořeného vládou. V opačném případě rozhodují o určení kritických systémů příslušná ministerstva anebo Národní bezpečnostní úřad v oblasti informačních technologií. Je však možné, že ačkoliv systém nenaplnuje kritéria potřebná do zařazení mezi kritické prvky, stále se může jednat o významný informační systém a jeho povinnosti jsou v tomto případě obdobné (Smejkal, 2015).

Pro zařazení prvků kritické infrastruktury se používají kritéria, která jsou určena na základě průřezového kritéria definovaného vládou. Ty zahrnují situace, které by mohly vést k:

- Více než 250 úmrtím.
- K více než 2,5 tisícům osob s dlouhodobou hospitalizací.
- Ekonomickému dopadu vyššímu než 0,5% HDP.
- Dopadu na veřejnost s mezní hodnotou rozsáhlého omezení nezbytných služeb pro každodenní život postihující více než 125 tisíc osob.

V případě prvků informační infrastruktury se moc často s prvními dvěma nesetkáme, poslední kritérium se zase týká pouze konkrétních subjektů, které utvářejí uspořádání veřejného sektoru v České republice (Smejkal, 2015).

Ačkoliv se oblast kybernetické bezpečnosti přidala mezi odvětvová kritéria poměrně nedávno, neznamená to, že by nebyla důležitá ve srovnání s jinými oblastmi. Téměř cokoliv se spojitostí s oblastí informačních technologií je součástí kritické infrastruktury, například sítě, komunikační a poštovní služby, televizní a rozhlasové vysílání, různé informační systémy apod. Oblast kybernetické bezpečnosti tak představuje zvláštní význam a jak již bylo zmíněno, i v případech, kdy nebyl naplněn předpoklad pro žádné kritérium, stále se může jednat o prvek kritické infrastruktury v případech, kdy je například informační systém nenahraditelný a nebo obsahuje citlivé osobní informace, jejichž zneužití by mělo za následek narušení bezpečnosti obyvatel (Smejkal, 2015).



## 4 DÍLČÍ ZÁVĚR

Z teoretické části je patrné, že oblast etického hackingu je velice rozsáhlým odvětvím, proto je téměř nemožné, pojmout celou problematiku ve formátu diplomové práce. V první fázi této práce však bylo popsáno co možná nejlépe vše potřebné, pro pochopení problematiky etického hackingu, ale i klasického hackingu a kybernetické bezpečnosti obecně.

Bylo definováno, které instituce lze řadit mezi subjekty ochrany obyvatelstva a vysvětlena důležitost informačních systémů a v neposlední řadě vymezeny kritéria, která jsou nutná pro zařazení do prvků kritické infrastruktury, včetně specifikace nutných náležitostí pro zařazení mezi prvky kritické informační infrastruktury.

Jak již bylo řečeno, klasičtí i etičtí hackeři mohou používat ve své podstatě ty stejné techniky, liší se pouze jejich cíl. Proto bylo popsáno několik způsobů útoku a byla nastíněna i častá motivace útočníků při napadání zařízení. Jednou z těchto kombinací může být phishingový útok se záměrem získat přihlašovací údaje uživatelů a tím pádem získat přístup k soukromým citlivým datům. Právě tuto situaci bude rozebírat praktická část této práce.

## **II. PRAKTICKÁ ČÁST**

## 5 PHISHINGOVÁ KAMPAŇ ETICKÉHO HACKERA

Následující kapitola bude věnována představení nástroje a subjektu, které budou v rámci praktické části nezbytné. Výzkum prováděný v praktické části této práce byl proveden na konkrétní korporátní společnosti zabývající se především pojišťovnictvím. Z hlediska bezpečnosti je nutné ponechat tuto společnost anonymizovanou. Veškeré analytické informace byly poskytnuty seniorním specialistou bezpečnostní IT této firmy. Vzhledem k okolnostem a požadavkům poskytovatele je nutno konkrétní data anonymizovat, v důsledku toho budou všechny informace, které by mohly vést k rozpoznání společnosti skryty. Výzkumným vzorkem pro tuto práci byli pouze zaměstnanci této společnosti pracující pod českou pobočkou s příslušnými náležitostmi pro pracovní poměr.

### 5.1 Představení společnosti

Tato podkapitola stručně představí společnost, ve které probíhala phishingová kampaň popsána dále v této práci. Z důvodu anonymizace se jedná pouze o obecné představení bez uvedení konkrétních údajů prozrazující identitu.

Jedná se o nadnárodní společnost, která poskytuje služby v oblasti pojišťovnictví a financí. Její portfolio produktů a služeb zahrnuje životní pojištění, pojištění majetku a odpovědnosti, cestovní pojištění a investiční fondy. Působí v mnoha zemích po celém světě, jako například Itálie, Francie, Německo, Rakousko, Španělsko, Švýcarsko a Spojené státy americké. Tato firma zaměstnává více než 70 tisíc lidí, kteří se starají o více než 60 milionů klientů.

### 5.2 Nástroj PhishMe

PhishMe je nástroj pro školení phishingu, který umožňuje organizacím provádět tréninkové simulace phishingových útoků na své zaměstnance. Jak již bylo popsáno v teoretické části této práce, phishing je technika útoku, při které útočník získává citlivé informace, jako jsou hesla, bankovní údaje nebo jiné důvěrné informace tím že se vydává za legitimní zdroj a přesvědčuje oběť, aby dobrovolně poskytla své informace.

Tento nástroj umožňuje organizacím vytvářet vlastní phishingové e-maily a webové stránky, které jsou simulací reálných útoků, a posílat je svým zaměstnancům. Organizace následně mohou sledovat a vyhodnocovat, jak reagují zaměstnanci na tyto simulace. To jim poskytuje nástroje k vytváření a řízení školení zaměřených na zvyšování povědomí o bezpečnosti a prevenci phishingových útoků.

PhishMe poskytuje také analýzy úspěšnosti simulací, včetně statistik o tom, kolik zaměstnanců kliklo na odkazy v phishingových e-mailech, kolik poskytlo citlivé informace a kolik zaměstnanců odhalilo phishingový útok a hlásilo ho. Tyto informace mohou pomoci organizacím posoudit úroveň rizika a poskytnout jim informace k vylepšení bezpečnosti svých systémů a tréninků zaměstnanců.

Jedná se o užitečný nástroj pro organizace, které chtějí zvýšit povědomí o phishingových útocích a ochranu proti nim. Pomáhá také organizacím identifikovat slabá místa a zlepšit bezpečnost svých systémů a informuje zaměstnance o nebezpečích phishingových útoků a jak se jim vyhnout.

### 5.3 Terminologie nástroje PhishMe

Při práci s nástrojem PhishMe je možno narazit na některé termíny, tato podkapitola vysvětluje základní z nich.

**Cílová skupina** – skupina lidí, která je cílem phishingové kampaně. Může se jednat například o zaměstnance konkrétní společnosti nebo uživatele určitého e-mailového serveru.

**Template** – (neboli šablona phishingové zprávy) předloha, která obsahuje falešnou zprávu nebo webovou stránku, kterou oběť uvidí při phishingovém útoku.

**Cílový odkaz** – odkaz v phishingové zprávě, který má přimět oběť ke kliknutí a přesměrovat ji na falešnou stránku, kde jsou získávány citlivé informace.

**Falešná stránka** – stránka, která vypadá jako legitimní webová stránka, ale ve skutečnosti slouží k získání citlivých informací od oběti.

**Phishingová kampaň** – cílený proces využívající phishingové emaily a jiné podvodné aktivity k získání citlivých dat uživatelů.

**Výsledky kampaně** – statistiky o úspěšnosti kampaně, jako je počet otevřených zpráv, počet kliknutí na odkazy a počet přihlašovacích údajů, které byly získány.

**Zpráva** – textová nebo vizuální informace, kterou oběť obdrží při phishingovém útoku.

**Cíl** – cíl kampaně, tedy například získání hesla, čísla kreditní karty atd.

**Metriky** – měření úspěšnosti kampaně na základě počtu otevřených zpráv, kliknutí na odkazy a dalších ukazatelů.

**Šablona reportů** – zpráva o výsledcích kampaně, která může obsahovat informace o počtu odeslaných zpráv, počtu otevřených zpráv a kliknutí na odkazy a dalších metrikách.

**Zpětná vazba** – informace o úspěšnosti a neúspěšnosti kampaně, která slouží k vylepšení strategie a zvýšení účinnosti

#### 5.4 Preventivní phishingové školení zaměstnanců

Pomocí již představeného nástroje PhishMe využívá společnost preventivní školení zaměstnanců v oblasti informační bezpečnosti. Konkrétně se zde jedná o emailové kampaně, které záměrně obsahuje zprávy fungující na principu Phishingu, které však neobsahují škodlivý odkaz, ani se nesnaží adresátovi uškodit. Kampaně jsou cíleny jak na nováčky ve společnosti, tak i stálé zaměstnance. Kampaně mohou být rozeslány náhodě na automaticky vybrané zaměstnance, tak i cíleně, například na zaměstnance, kteří byli v minulých kampaních neúspěšní.

Jak již bylo zmíněno, společnost působí v různých zemích světa, každou zemi na starosti místně příslušné IT oddělení, tudíž nejsou rozesílány kampaně mezinárodně, ale pouze v místně zaměstnání. I přesto jsou však výsledky kampaní sdíleny mezi pověřenými pracovníky napříč společnostmi a na základě získaných výsledků jsou prováděny potřebné kroky k posílení bezpečnosti.

Poté, co zaměstnanec obdrží tento email, měl by správně zareagovat tím způsobem, že nahlásí phishingový email pomocí tlačítka na nahlášení v emailovém klientu. Jsou i případy, kdy pracovníci tento email prostě ignorují, i to je ve své podstatě správný krok. Dalšími případem je, že zaměstnanec klikne na odkaz obsažený v emailu, který ho přesměruje na stránku, kde je po něm vyžadováno přihlášení, v tomto případě již jedná chybně. Je však stále možnost tuto stránku uzavřít a žádné své údaje nesdělovat. Pakliže i vyplní údaje, které po něm falešná stránka vyžaduje, jedná se již o regulérní porušení bezpečnostních pravidel a tím pádem v této kampani zcela neuspěl.

Pokud se uživatel dostal až na konec phishingové kampaně, což je zpravidla proklik na falešnou stránku případně vyplnění osobních údajů na této stránce, je nakonec přesměrován na stránku, která mu oznámí že se stal terčem phishingového útoku, ve kterém neuspěl a jsou mu předložena pravidla kybernetické bezpečnosti, případně může být odkázán na video, kde jsou tyto pravidla vysvětlena. V obou případech po tomto ví, že se jednalo

o kampaň s cílem osvěty v oblasti informační bezpečnosti. Tím je také naplněn cíl kampaně a na důsledných statistikách je možno sledovat uživatelské počínání v dalších kampaních.

**Toto byla schválená simulace phishingu**

Pokud dostanete e-mail, který ve vás vzbudí podezření, že jde o phishingový útok, nebo máte dotazy či zpětnou vazbu k tomuto cvičení, napište e-mail na adresu [itsec@](mailto:itsec@)

### Cílený phishing

Ke kompromitování naší sítě stačí jediné kliknutí. Cílený phishing představuje jednu z hlavních příčin úniků dat. Vzhledem k rostoucímu počtu kybernetických útoků a úniků dat je nutné mít povědomí o nejnovějších metodách cíleného phishingu.

### Co je cílený phishing?

Cílené phishingové zprávy jsou zasílány malým skupinám či jednotlivcům. Útočníci tyto zprávy uzpůsobují tomu, aby je technická opatření, jako jsou antispamové filtry, nezachytily.

Cílené phishingové e-maily:

- **Obsahují v příloze soubory**, které mohou počítač infikovat malwarem.
- **Snáží se vás přimět, abyste klikli na odkazy** vedoucí na webové stránky, které následně infikují váš počítač.
- **Vyžadují sdělení přihlašovacích údajů** či jiných citlivých informací, aby útočníci získali přístup do naší sítě.

Cílené phishingové útoky jsou nebezpečné, protože často cílí na konkrétní jedince. Útočníci si o svém cíli zjistí spoustu informací a své e-maily posílají tak, aby se příjemcům zdály věrohodné. Často si například vyhledávají informace z profilů na sociálních sítích a použijí je ve svých e-mailech, aby působily věrohodněji. Cílené phishingové e-maily mohou dále hrát na emoce. Mohou vyvolávat strach, zvědavost či dojem naléhavosti, případně se mohou příjemcům podbízet.

### Rychlé tipy

- **Buďte opatrní.** E-maily si pozorně pročítejte a všimněte si výrazů, jako „pozor“, „varování“ nebo „neotálejte“, které navozují dojem naléhavosti a snaží se vás přimět, abyste rychle zareagovali.
- **Kontrolujte název domény.** Někteří útočníci se spoléhají na nepozornost příjemců a zneužívají domény s mírně odlišným názvem. Když je například správná adresa domény „www.example.com“, phishingový útočníci si mohou zaregistrovat doménu „examp1e.com“ nebo „example.co“.
- **Kontrolujte své emoce.** Phishingový útočníci často hrají na emoce, jako je strach, či zvědavost příjemců. Používají k tomu podbízející titulky nebo sdělení, že váš účet byl napaden.
- **Vždy ověřujte.** Rychlým telefonátem si ověřte, zda e-mail pochází od skutečného odesílatele. Každý podezřelý e-mail nahlaste.

**Máte-li podezření, že jste v práci obdrželi cílený phishingový e-mail, jedněte podle našich pravidel a neprodleně situaci ohlaste.**

Obrázek 1: Edukační obrazovka na konci phishingové kampaně (zdroj: vlastní)

Nástroj PhishMe pracovníkům kybernetické bezpečnosti umožňuje důkladnou analýzu všech kroků, které provedli uživatelé, na které byla kampaň cílena. Je možno sledovat kolik procentuálně pracovníků email nahlásilo, kolik ignorovalo, kdo se dostal na další stránku, případně vyplnil osobní údaje. Dále je taky možné vidět kolik času uživatel strávil na edukační stránce na konci kampaně. PhishMe však sleduje i více konkrétní údaje o tom,

v jakém čase, kdo a jak s emailem interagoval, jaký byl nejkratší čas pro nahlášení, jaký byl průměrný čas nahlášení, jaké prohlížeče uživatelé použili nebo jaké měli emailové klienty. Mimo jiné ukazuje i informace jako jsou IP adresy, případně geografickou lokaci zařízení. Veškeré tyto informace shrnuje do přehledných reportů, které následně prezentuje ve formě grafů nebo tabulek. Celý report se všemi výsledky kampaně si poté můžou bezpečnostní pracovníci stáhnout v různých formátech jako .pdf nebo .xml.

## 5.5 Phishingové emaily

V rámci preventivního školení a odhalování nedostatků v oblasti kybernetické bezpečnosti jsou zaměstnancům pravidelně zasílány phishingové emaily, které však nezpůsobují žádnou škodu, ale odkazují na stránku se školením v případě, kdy uživatel provede všechny kroky, které jsou po něm v těch emailech vyžadovány.

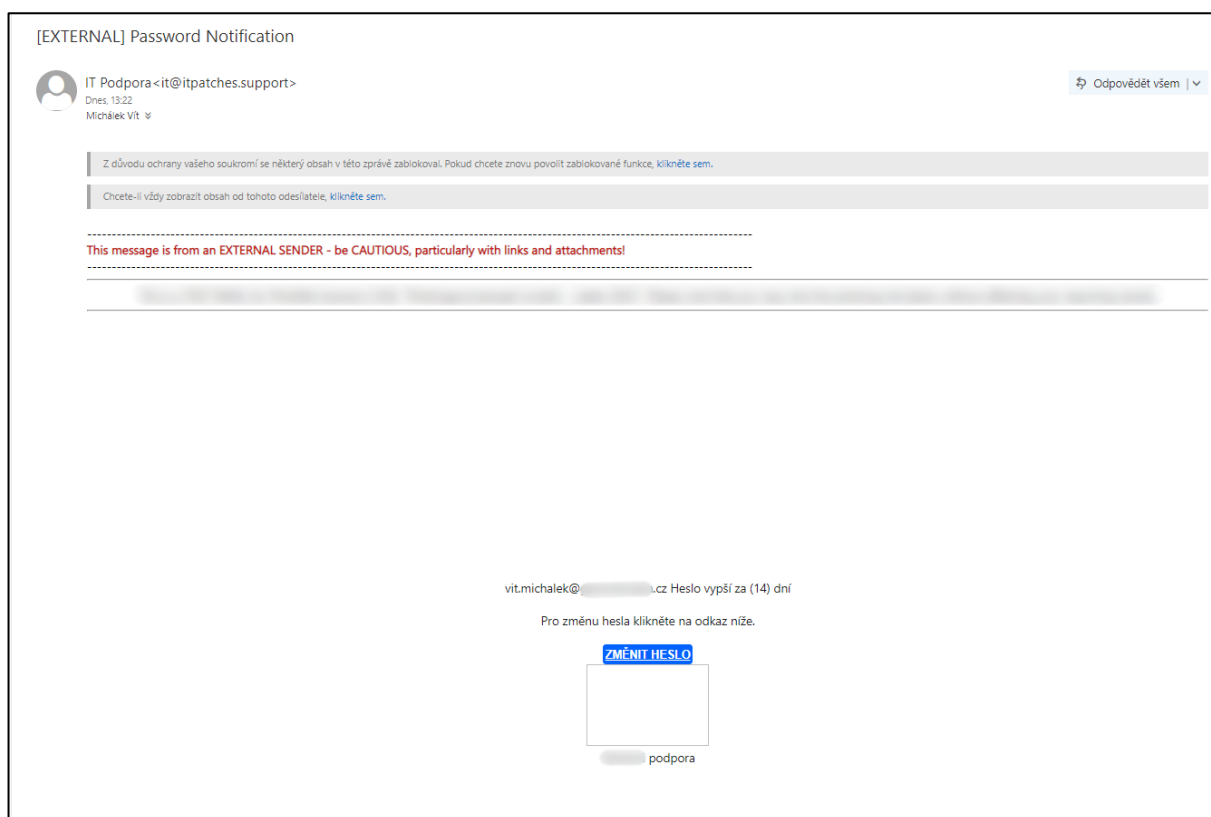
Tyto phishingové kampaně jsou obecně vypracovány ve třech různých obtížnostech, respektive jsou používány tři šablony, přičemž se postupně stupňuje složitost a propracovanost emailů, čímž se stávají pro uživatele těžší na odhalení. Stupňování je prováděno zpravidla na základě propracovanějšího grafického zpracování, formátováním a stylistikou textu, nebo grafickými prvky jako jsou reálná loga společností apod. Toto stupňování bylo navrženo na základě zkušeností z opravdových phishingových emailů, které běžně používají útočníci s cílem uškodit. I v těchto případech si lze často všimnout odlišené propracovanosti emailů. Nežádá se, aby se stávalo, že jsou k přepisu textu používány různé programové překladače, které nedokážou správně vygenerovat věty tak, aby zněly jak od rodilého mluvčího.

### První stupeň obtížnosti

V prvním stupni bývají emaily zpravidla jednoduché, bez výrazných grafických prvků, formátování a stylistika je na chabé úrovni a případný škodlivý odkaz nebo přílohu se nesnaží nijak výrazně maskovat. Často se stává že útočníci necílí přímo na vlastní zemi, případně na zemi s jazykem, který sami ovládají. Proto není výjimkou, že jsou emaily překládány pomocí online překladačů, obsahují gramatické chyby anebo nesprávný slovosled. Obtížnost odhalení takového emailů není příliš velká, proto by se nemělo stávat, že jej školený zaměstnanec neodhalí. V případě této společnosti jsou emaily odesílány na pracovní emailové adresy, pro zaměstnance tudíž může být obrovskou nápovědou i to, že zprávy obsahují sdělení, které s výkonem povolání vůbec nesouvisí.

Obecně lze shrnout tyto emaily do následujících bodů:

- Obecně špatná gramatika.
- Slovosled nekoresponduje se skutečnou řečí rodilého mluvčího.
- Formátování emailů je velice podprůměrné.
- Zpráva obsahuje více jazyků, či nemusí být vůbec přeložená do jazyka příjemce.
- Odesílatel se nijak nesnaží skrývat svoji emailovou adresu.
- Grafické zpracování je strohé a neodráží základní šablony emailů ze známých organizací.



Obrázek 2: První stupeň obtížnosti phishingových emailů (zdroj: vlastní)

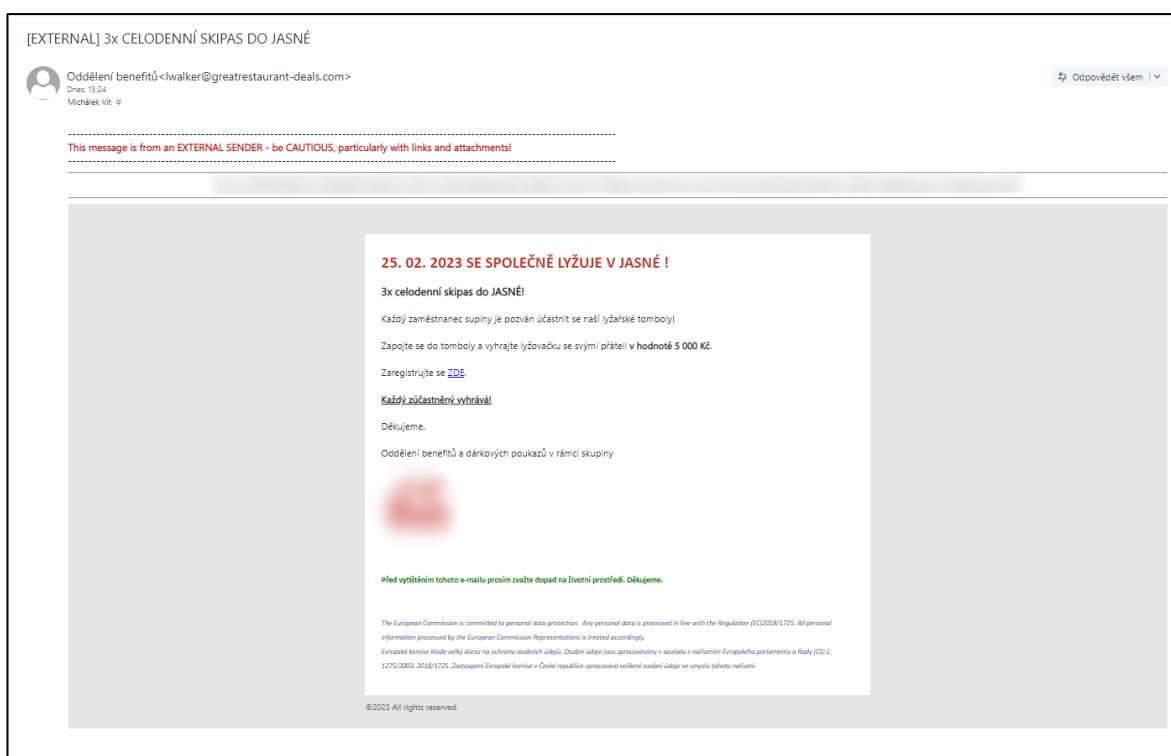
Z obrázku je patrné, že ačkoliv jde o zprávu, která se na první pohled může jevit jako relevantní pro výkon zaměstnání, vzhledem k bezpečnostnímu pravidlu změny hesla v pravidelných intervalech, je zde na první pohled patrné hned několik ukazatelů napovídajících, že se jedná o podvodný email. Hned v nadpisu emailu je možné si všimnout anglického jazyka, ačkoliv název odesílatele je IT podpora, konkrétní emailová adresa není z domény zmiňované společnosti. Dále je zde varování přímo od emailového klienta, že se



jedná o zprávu z externího zdroje a uvádí varování před odkazy a přílohami. Samotné sdělené emailu je strohé a po grafické stránce nekoresponduje s grafickým stylem společnosti.

### Druhý stupeň obtížnosti

V dalším stupni je phishingovým emailům věnováno mnohem více pozornosti. Emaily jsou často doplněny o grafické prvky, nadpisy jsou koncipovány tak, aby uživatele vybízeli k nějaké akci, případně mohou být emaily doplněny o přílohy, které se snaží přidat na důvěryhodnosti. Emaily korespondují se základními barvami společnosti a obsahují logo. Emailům je věnována větší péče, jsou celé lokalizované a můžeme zde naléznout i detaily, které bývají v zápatí emailů.

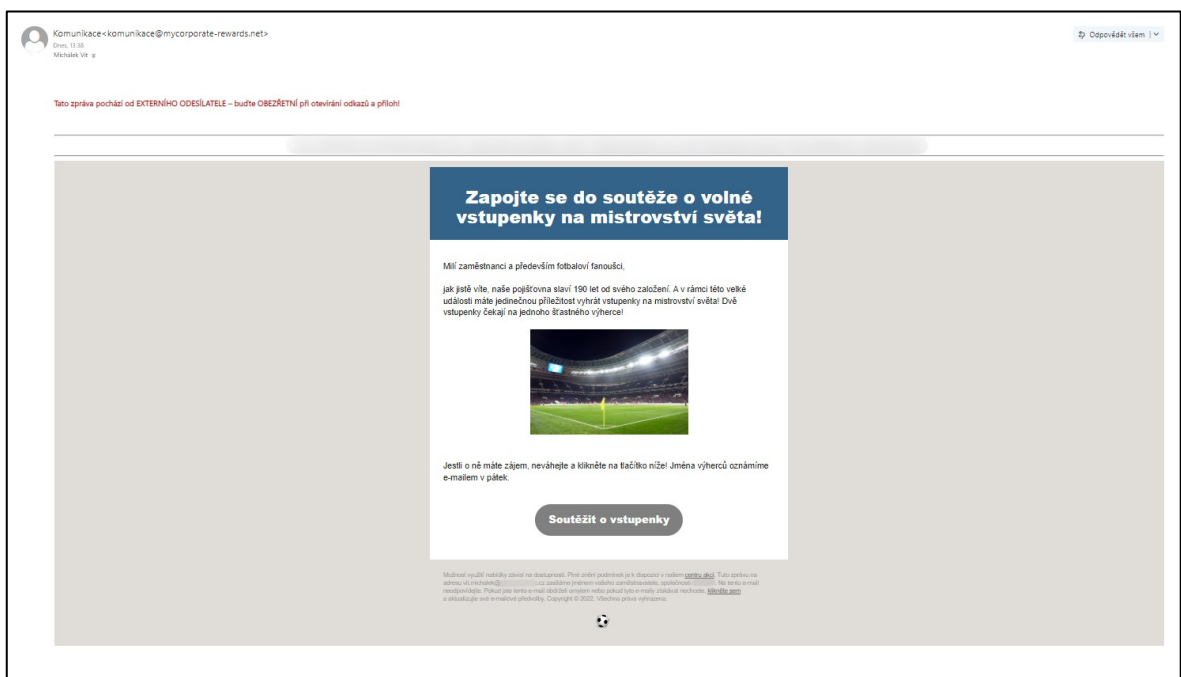


Obrázek 3: Druhý stupeň obtížnosti phishingových emailů (zdroj: vlastní)

Obrázek zachycuje příklad emailů spadajícího do druhé kategorie obtížnosti. Všechny potřebné prvky jsou v češtině, email dodržuje zásady formátování a formální obsah emailu, obsahuje oficiální společnosti logo a drží se firemních barev. Dále zde můžeme naléznout detaily jako je informace o šetření životního prostředí a zásady zpracování osobních údajů podle zákona. Všechny tyto prvky přidávají na důvěryhodnosti. Dalším faktorem je i to, že tento phishingový email vybízí k soutěži, což obecně vždy lidi přitahuje více.

### Třetí stupeň obtížnosti

Poslední stupeň bývá zpravidla nejpropracovanější a nejtěžší na odhalení, proto není divu, že se uživatel nechá nachytat, pokud nevěnuje důkladnou pozornost veškerým detailům. Email je po textové stránce napsaný správně, může obsahovat části, které zlepšují jeho důvěryhodnost, například podpis konkrétní osoby nebo oddělení, od kterých může uživatel reálně nějakou korespondenci očekávat. V případě, že tato zpráva obsahuje odkaz na falešnou stránku, kde je většinou vyžadováno ověření jménem a soukromým heslem, je i ona často vytvořená do detailů. Obsahuje loga konkrétních, často nadnárodních a známých společností, neznámá kdy i loga jiných souvisejících institucí pro přidání na důvěryhodnosti. Prostředí těchto falešných stránek je okopírované přesně podle skutečných stránek společnosti, včetně všech barev, animací a tvarů elementů.



Obrázek 4: Třetí stupeň obtížnosti phishingových emailů (zdroj: vlastní)

Na tomto příkladu je možné vidět již na první pohled kvalitní grafické zpracování. Ačkoliv se v tomto případě nejedná přímo o konkrétní společnost, je zde využito i konkrétní doby, respektive události, kterou je v té době zrovna probíhajícího mistrovství světa ve fotbale. Jako u druhého příkladu i zde je nabízena soutěž, konkrétně možnost výhry vstupenek na zmiňovaný fotbalový zápas. Email je adresovaný přímo zaměstnancům, kteří jsou zde osloveni a je zmíněn údaj o výročí vzniku pojišťovny, který tak přidává

na autentičnosti a konkrétním zaměření. Ve spodní části je kromě ochrany o osobních údajích zmíněna i možnost odhlásit odběr podobných emailů, to může být past i pro zkušené uživatele, kteří sice nevěří reklamnímu sdělení emailů, ale často automaticky klikají na odhlášení odběru, aby další podobné emaily už nedostávali. I tento odkaz však může odkazovat na falešnou stránku.

## 5.6 Školení zaměstnanců v oblasti kybernetické bezpečnosti

Pro zajištění maximální bezpečnosti a integrity společnosti je každý nově příchozí zaměstnanec povinen vyplnit řadu testů, zaměřené na různé okruhy i s přihlédnutím na jeho kompetence a náplň pracovní činnosti. Jsou však i povinné testy, které plní všichni zaměstnanci bez rozdílu, jedním z nich je i test s názvem Školení informační bezpečnosti.

Tento kurz je sestaven ze čtyř okruhů:

- Informační bezpečnost.
- Bezpečnostní povědomí (Security Awareness Program, Security Awareness Program).
- Bezpečnost v kanceláři (Office Security).
- Phishing.

Jak již názvy napovídají, kurzy jsou zaměřené napříč celým spektrem kybernetické bezpečnosti a jsou zahrnuty okruhy, které musí každý zaměstnanec pojišťovny znát, aby zajistil maximální ochranu dat svých, i klientů.

Kurzy jsou prováděny různými formami – ať už klasický textový kurz, animované kurzy nebo i videokurzy, kdy je prostřednictvím videa zobrazeno pochybení s jeho dopadem a je zde vysvětleno, jak by se měl uživatel správně zachovat. Na závěr kurzu je připraven test na 25 minut, který obsahuje 20 otázek. Pro úspěšné absolvování je nutné mít alespoň 80 % správně. Po splnění kurzu je uživateli garantována platnost po dobu 2 let, poté je nutné kurz vyplnit znovu.

Je důležité zaměstnance vzdělávat a informovat v kybernetické bezpečnosti převážně z důvodu, že uživatelé představují z pohledu IT bezpečnosti nejslabší článek zabezpečení. A proto je více jak 90 % kybernetických útoků směřováno právě na ně (Stay Secure, 2022).

Útočník využívá nejrůznější techniky, jak zaujmout zaměstnance natolik, aby klikl na jeho odkaz v emailu. Uživatelé si často neuvědomují, s jakými daty pracují a jak s nimi

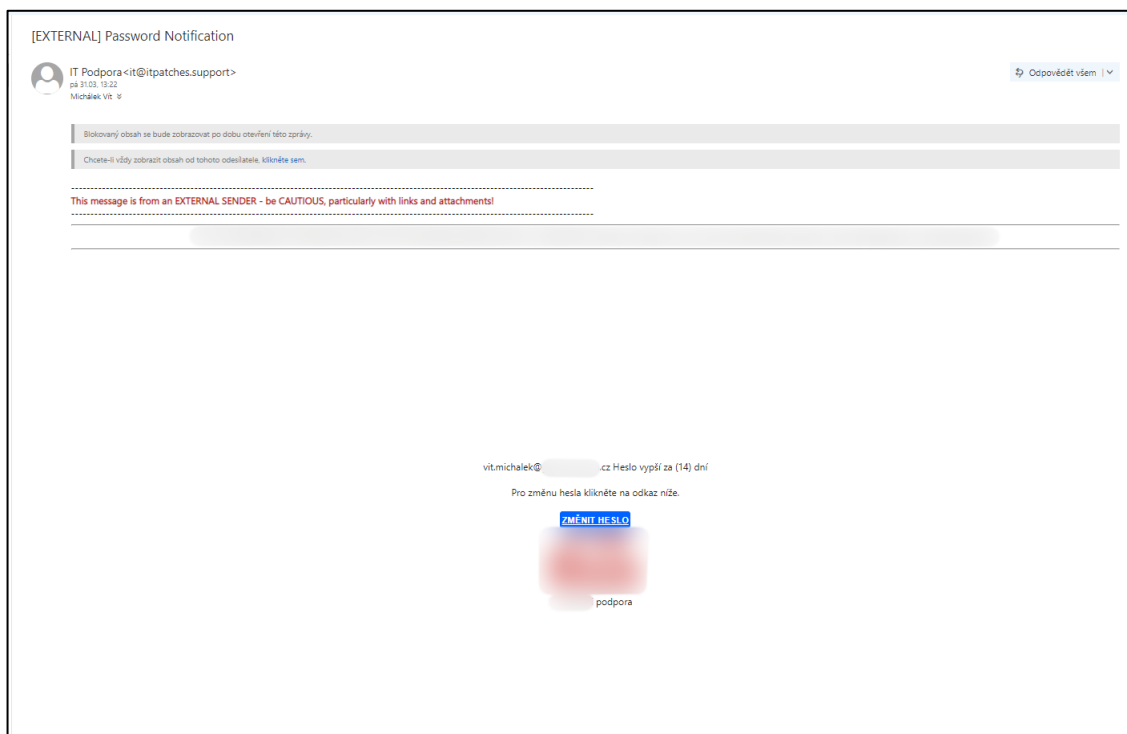
pracují. Zvyšování povědomí o kybernetické bezpečnosti může uživatele uchránit i v soukromém životě. Z toho důvodu jsou všechny kurzy Informační bezpečnosti povinné pro všechny zaměstnance a uživatele, kterým byl kurz přidělen.

## 5.7 Hodnocení úspěšnosti

Následující kapitola bude rozebírat phishingovou kampaň ve zmiňované společnosti, která byla zacílena na letošní nové zaměstnance s datem nástupu v lednu 2023. Budou zde uvedena všechna důležitá vstupní data podstatná pro pochopení celé kampaně. Pomocí snímků obrazovky bude znázorněn celý průběh kampaně a všechny náležitosti emailu tak, jak jej obdržel příjemce. Následně zde budou zanalyzovány výsledky z kampaně a vyveden závěr včetně zhodnocení úspěšnosti.

## 5.8 Phishingová kampaň

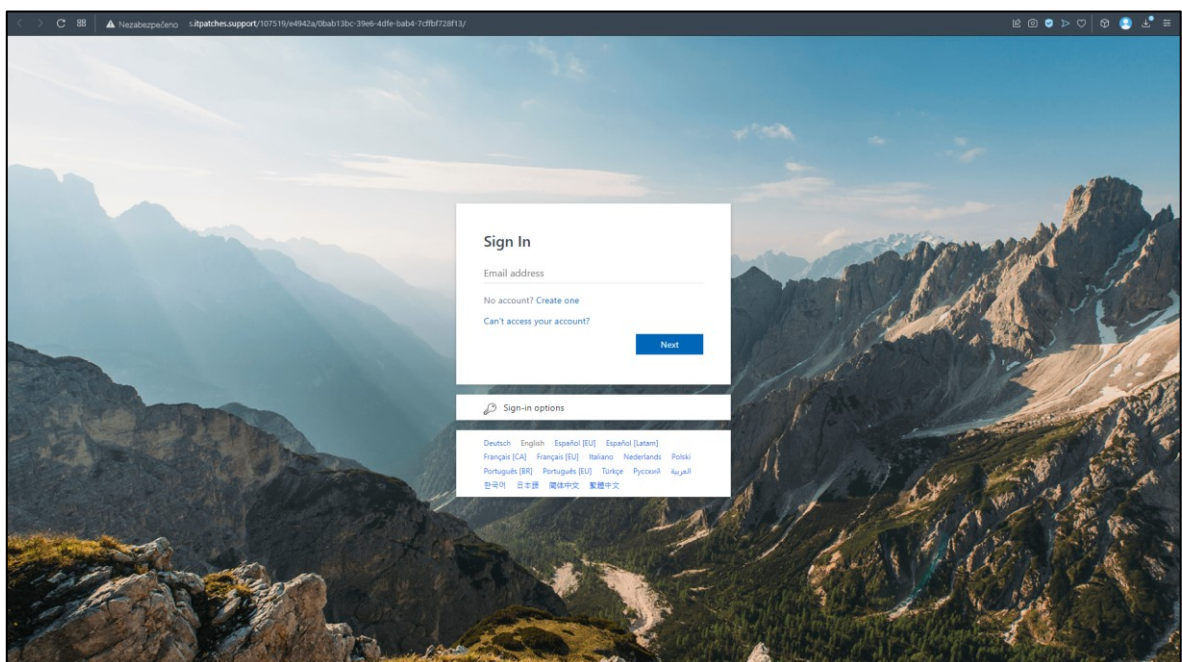
Kampaň proběhla v době od 25. ledna, kdy byly emaily rozeslány všem nově nastupujícím zaměstnancům a ukončena byla přesně o 5 dní později, tedy 30. ledna. V průběhu těchto pěti dní, měli všichni příjemci možnost jakkoliv interagovat s emailem, ať už pouhým přečtením, nahlášením případně kliknutím na odkaz v emailu. Této kampaně se účastnilo celkem 48 osob. Všichni měli v době phishingové kampaně splněné kurzy informační bezpečnosti a byli řádně proškoleni vstupním školením rozepsaným v předchozích kapitolách.



Obrázek 5: Phishingový email z kampaně pro nováčky (zdroj: vlastní)

Tento obrázek ukazuje, jak přesně vypadal email, který v rámci kampaně respondenti obdrželi. Email vyzývá ke změně hesla a vzhledem k situaci zaměřených osob, je možné takovýto email očekávat. Je zde však možné povšimnout si hned několika znaků upozorňujících na nepravost emailu. Příkladem je možno uvést doménu odesílatele, která není shodná s emailovou doménou pojišťovny. Dále je zde varování od emailového klienta upozorňujícího na nedůvěryhodný externí zdroj a formátování textu je zde na mizerné úrovni. Jsou zde i prvky, které naopak pravost emailu podporují, jako logo společnosti, konkrétní email příjemce, což vyzdvihuje konkrétní zacílení a na konci je uvedený podpis podpory dané společnosti.

Podle předchozího rozdělení obtížnosti emailů je možno usoudit, že se jedná o jednodušší možnost a proškolený zaměstnanec by měl být schopný rozeznat, zdali se jedná o podvodný email.



Obrázek 6: Stránka zobrazená po kliknutí na odkaz (zdroj: vlastní)

V případě, že uživatel nerozeznal phishingový email a kliknul na odkaz, který měl údajně odkazovat na změnu hesla, byl přesměrován na stránku zobrazenou na obrázku 7. Zde se uživateli zobrazil formulář, který vyžadoval jeho pracovní přihlašovací údaje, tj. jméno a heslo. V tomto případě je stránka zjevně vytvořená z přednastavené šablony, a zpracování vypadá na první pohled docela důvěryhodně. Je zde obrázkové pozadí, přihlašovací formulář vypadá podobně jako je tomu například při přihlašování k serverům Microsoftu

a je zde dokonce možnost volby jazyka. Jedinou možností, jak je možné odhalit nekalost v případě této stránky je URL adresa.



Obrázek 7: Nedůvěryhodná URL adresa (zdroj: vlastní)

V tomto případě zde vůbec není zmíněn název společnosti, ačkoliv doména může zdánlivě tíhnout k IT podpoře, jako celek působí nedůvěryhodně. Útočníci často využívají reálný název stránky, pod jejíž jménem se snaží vystupovat a URL změni jen například v jednom znaku, v tomto případě to může být „s“ na začátku adresy. Z logického hlediska je však nesmyslné i pokračování adresy. Důležitým faktorem je i to, že tato adresa nemá šifrování https, na což se snaží upozornit i samotný prohlížeč informací o zabezpečení před konkrétní doménou.

Pokud uživatel ani do této chvíle nerozeznal nepravost stránky, a rozhodl se pro vyplnění údajů, které po něm formulář vyžadoval, potenciálně tím útočnickovi poslal své rozšifrované údaje pro přihlášení do pracovního profilu společnosti. V případě této kampaně však byl po vyplnění těchto údajů přesměrován na stránku, kde mu bylo oznámeno že se stal potenciální obětí phishingu. V tomto případě měl takový uživatel možnost si v krátkém videu prohlédnout tipy, které mu do budoucna pomohou lépe rozpoznat phishingové emaily.



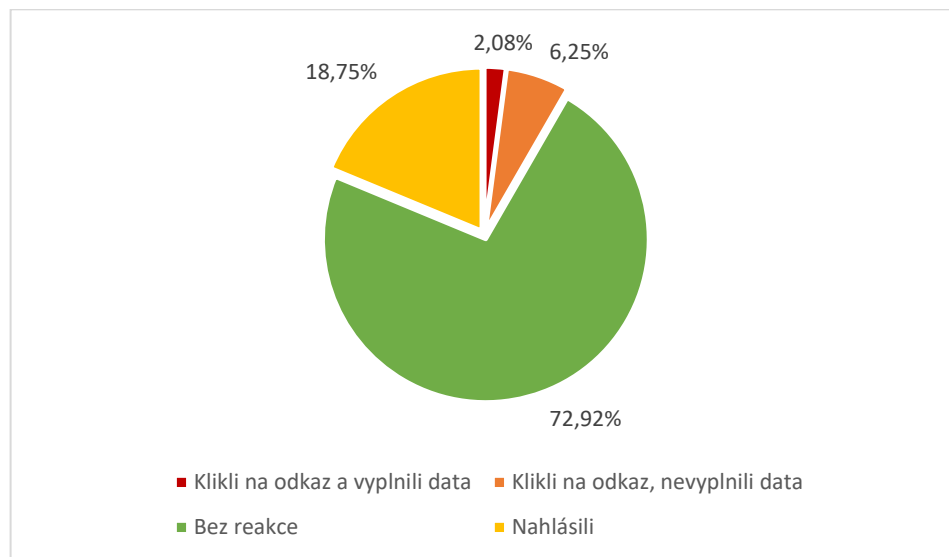
Obrázek 8: Edukační obrazovka na konci phishingové kampaně pro nováčky (zdroj: vlastní)

### Výsledek phishingové kampaně

Jak již bylo zmíněno, celkem se této kampaně účastnilo 48 zaměstnanců. Z výsledného reportu vyplývá, že všech 48 phishingových emailů bylo doručeno, tím pádem je i celkový výsledek počítaný z reakcí kompletního vzorku.

Z celkem 48 uživatelů jich 9 správně email nahlásilo jako phishingový a tím pádem zareagovali přesně tak, jak jim bylo na školeních vysvětlováno. Největší zastoupení celkem 35 uživatelů bylo těch, kteří na email nijak nereagovali, tudíž si jej pouze přečetli a ignorovali, nebo jej ani nečetli, případně rovnou vymazali. Další 3 uživatele si email přečetli, klikli na odkaz který obsahoval, ale data nevyplnili. Už i tím však porušili jednu ze

zásad bezpečnosti, což je neklikat na odkazy v emailech z nedůvěryhodných zdrojů. Pouze jeden uživatel z celkového vzorku na odkaz v emailu klikl a poté i vyplnil data.



Graf 1: Reakce respondentů (zdroj: zkoumaná společnost)

## 5.9 Vyhodnocení

Z výsledků kampaně rozebraných v předchozí podkapitole je patrné, že ačkoliv cílová skupina byla proškolení zaměstnanci od jejichž proškolení uběhly maximálně tři týdny, s ohledem na termín jejich nástupu a dobu, kdy probíhala kampaň, se i přesto našli jedinci, kteří phishing neodhalili. Může být tedy položena otázka, jak účinné školení jsou a jakými způsoby je případně možné těmto bezpečnostním selháním předcházet. Phishingové kampaně mohou být právě proto výhodné jak pro firmy, které mají možnost sledovat míry proškolení jejich zaměstnanců v oblasti informační bezpečnosti a zároveň zaměstnanci zůstávají ve střehu před skutečnými phishingovými emaily. Jedná se o výjimečnou kombinaci teoretických znalostí a konkrétní využití v praxi, proto se tato metoda testování, respektive školení, jeví jako vhodná.



## 6 NÁVRH SCÉNÁŘE PHISHINGOVÉHO ÚTOKU NA SUBJEKT OCHRANY OBYVATELSTVA

V předchozí kapitole bylo představeno, jak fungují phishingové kampaně v rámci velkých společností. Bylo možné nahlédnout do detailů proškolení v oblasti kybernetické bezpečnosti a z hodnocení vyplynula celková úspěšnost těchto kampaní. V této kapitole bude přiblíženo, jak by v teoretické rovině mohl probíhat takovýto phishingový útok na subjekt ochrany obyvatelstva. Zmiňovaná společnost byla zvolena především z toho důvodu, že je možné srovnávat její strukturu a zabezpečení s obdobně rozsáhlým subjektem ochrany obyvatelstva. V této kapitole bude vytvořen scénář phishingového útoku na zvolený subjekt OO. Bude popsán důvod volby právě tohoto subjektu, následně názorně zaznamenán průběh tvorby phishingového emailu a následovat bude model, který celý postup znázorní ve strukturovaném grafu.

### 6.1 Volba subjektu ochrany obyvatelstva

V dnešní moderní společnosti se může zdát, že útoky na nemocnice, ať už konvenčními zbraněmi či kyberútoky jsou tabu s ohledem na pravidla Ženevské úmluvy a jejich dodatkových protokolů. Ty mají za cíl chránit jak civilní obyvatelstvo, tak i obecně všechny lidi, kteří nejsou přímo zapojeni do boje. Opak je však pravdou a v současnosti i moderních dějinách existuje hned několik záznamů o útocích na nemocniční zařízení, jejich personál, či v případě kybernetických útoků především na citlivé informace, které jsou nezbytnou součástí těchto zařízení (Lékaři bez hranic, 2023).

Právě kybernetické útoky na nemocniční zařízení se staly i na území České republiky stále častějším úkazem. To dokazují i nepříliš staré události posledních 3 let, kdy bylo zaznamenáno hned několik útoků na nemocnice po celé ČR. „*Hackerský útok odrazila ostravská nemocnice, pokusy o útok zaznamenaly také Fakultní nemocnice Olomouc nebo nemocnice Pardubického kraje. Další pokusy odrazila Karlovarská krajská nemocnice.*“ (Novinky.cz, 2023) Tento útok měl za cíl získat především přístupové údaje zaměstnanců do interních systémů. Další obdobný případ následoval nedlouho poté na jiná zdravotnická zařízení. „*Hackeri zaútočili na tři soukromé polikliniky v centru Prahy. Poliklinikám v Legerově, Kartouzské a Myslíkově ulici nefungovala e-mailová pošta ani objednávkový systém a lékaři přišli o přístup do databází laboratoří. Následující den hackeři napadli podle médií i zdravotnické zařízení ministerstva vnitra, které má citlivé informace o příslušnících bezpečnostních složek.*“ (Novinky.cz, 2023)

Dalšímu velkému kybernetickému útoku čelila Fakultní nemocnice Brno, v tomto případě útočníci způsobili i velkou škodu. „*Fakultní nemocnice Brno čelila kybernetickému útoku. Postupně padaly jednotlivé počítačové systémy, a proto bylo potřeba vypnout všechny počítače. Základní provoz nemocnice Brno zůstal zachován, postupně byly zapojeny všechny počítačové systémy. Nemocnici vznikla škoda v desítkách milionů korun.*“ (Novinky.cz, 2023)

Právě v posledním zmiňovaném případě, se dle odkazovaného serveru jednalo o phishingový útok, kdy útočník poslal prostřednictvím emailu některému za zaměstnanců malwarový soubor Defray. Ten cílí především pro útok na zdravotnické instituce. K jeho rozšíření útočníci používají právě emaily, ve kterých se vydávají za legitimní osoby. „*V phishingových e-mailech zmiňuje skutečné osoby, které v organizaci pracují, popřípadě s organizací spolupracují. Používá též korporátní identitu organizace, jehož zaměstnanec napodobuje – záhlaví a zápatí, logo společnosti, druh písma, aj. je v e-mailu stejné jako mají skuteční zaměstnanci organizace.*“ (ITBiz.cz. 2019)

Hlavním důvodem útoků na nemocnice a podobné zařízení jsou především citlivé osobní informace, lékařské záznamy a podobně zneužitelná data. Tyto ukradené záznamy poté útočníci prodávají na darknetu, kde se mohou pohybovat v cenách od 5 do 60 dolarů za jeden takovýto záznam. Při jednom útoku jich může být v některých případech získáno stovky tisíc až miliony (Seznam Zprávy, 2023).

Z tohoto důvodu je jako subjekt ochrany obyvatelstva zvoleno zdravotnické zařízení. V rámci výzkumné části bude hlavním cílem simulovat takovýto útok z pohledu absolutního laika, tzv. Script kiddies.

Nemocnice jsou klíčovými prvky v rámci zdravotnického systému a mají velký vliv na zdraví a kvalitu života obyvatelstva v celé zemi. Zabezpečení informačních systémů a ochrana citlivých dat pacientů jsou proto kritickými otázkami v ochraně zdraví a bezpečnosti obyvatelstva. O to důležitějším prvkem mohou být fakultní nemocnice. Fakultní nemocnice mají na starosti poskytování specializované zdravotní péče a výzkumu, a často zajišťují také odbornou výuku budoucích lékařů a zdravotních sester. Výsledky výzkumu a inovace z fakultních nemocnic mohou mít vliv na celou zdravotnickou oblast, a do určité míry i na ekonomiku státu.

Simulace scénáře phishingového útoku na nemocnici může pomoci připravit personál a zaměstnance na tyto hrozby a zlepšit ochranu dat a informačních systémů. Tato praktická

část diplomové práce může být prospěšná pro nemocnice, která může využít získaných poznatků ke zlepšení svého bezpečnostního plánu a ochrany citlivých dat pacientů a zaměstnanců.

Bude navržen možný scénář kybernetického útoku formou phishingu za účelem získání přihlašovacích údajů zaměstnanců zdravotnického zařízení s využitím poznatků zjištěných při phishingové kampani v předchozích kapitolách. Tento scénář bude pouze v teoretické rovině pro zdokumentování toho, jak by mohl potenciální útočník zneužít veřejně dostupné informace.

## 6.2 Tvorba phishingového útoku

Prvním krokem, co by útočník udělal je výběr subjektu, proti kterému útok bude směřovat, v tomto případě to budou již zmíněná nemocniční zařízení. Jsou dvě možnosti, jakým by mohli být útoky cíleny, buďto výběr jednoho konkrétního zařízení a tím pádem cílením všech atributů emailů na konkrétní subjekt anebo vytvoření obecného phishingového útoku napříč nemocnicemi. V tomto případě by útočník musel vymyslet nějaké obecné téma, které by bylo relevantní bez konkrétní lokace. Musel by email koncipovat tak, aby měli uživatelé pocit, že email pochází od nějakého nadřazeného subjektu, jako třeba ministerstva zdravotnictví. V této práci však bude zpracována první možnost, a to sice že útočník zvolil jeden konkrétní subjekt, ačkoliv je tento scénář aplikovatelný na jakoukoliv nemocnici s dostupnými informacemi. Z důvodu bezpečnosti bude tento subjekt obecný.

Dále by útočník musel zjistit všechny potřebné informace, to znamená emailové adresy pracovníků, na které bude cílit a adresy vedoucích pracovníků, případně jedné konkrétní osoby, pod jejímž jménem bude falešný email rozesílat. Seznam vedoucích pracovníků jednotlivých oddělení jsou ve většině případů dostupné pro veřejnost, tudíž není problém zvolit si oddělení, na které bude phishing mířit.

Následuje fáze zakládání emailu, tato fáze se můžeš lišit podle toho, jak zpracovaný může být útok. Většina poskytovatelů emailových služeb umožňuje zvolit si vlastní jméno, které se adresátovi objeví v příchozím emailu. Samotný název emailu případně název serveru je tak snadné přehlédnout. V případě, že chce být útočník pečlivý, může si založit email s vlastní emailovou doménou.

Dalším krokem je vytvoření falešné stránky, ta bývá zpravidla okopírovaná z nějaké již existující stránky, v případě nemocničních zařízení by to například mohl být webmail,

kam se zaměstnanci přihlašují pomocí pracovních emailů. Falešná stránka by měla obsahovat přihlašovací formulář, který by však neodkazoval na další stránku, ale zadané údaje by se poslali útočníkovi.

Posledním krokem je napsat phishingový email, který by oběť nalákal na tuto stránku a donutil ji zadat své údaje. Pro větší důvěryhodnost emailu by útočník měl zjistit jaké náležitosti jsou v emailech daných zařízení běžně používány. Dále by měl být email přehledný, systematický, úderný a po všech stránkách by měl vypadat důvěrně.

### 6.2.1 Analýza funkcionality nástroje SET

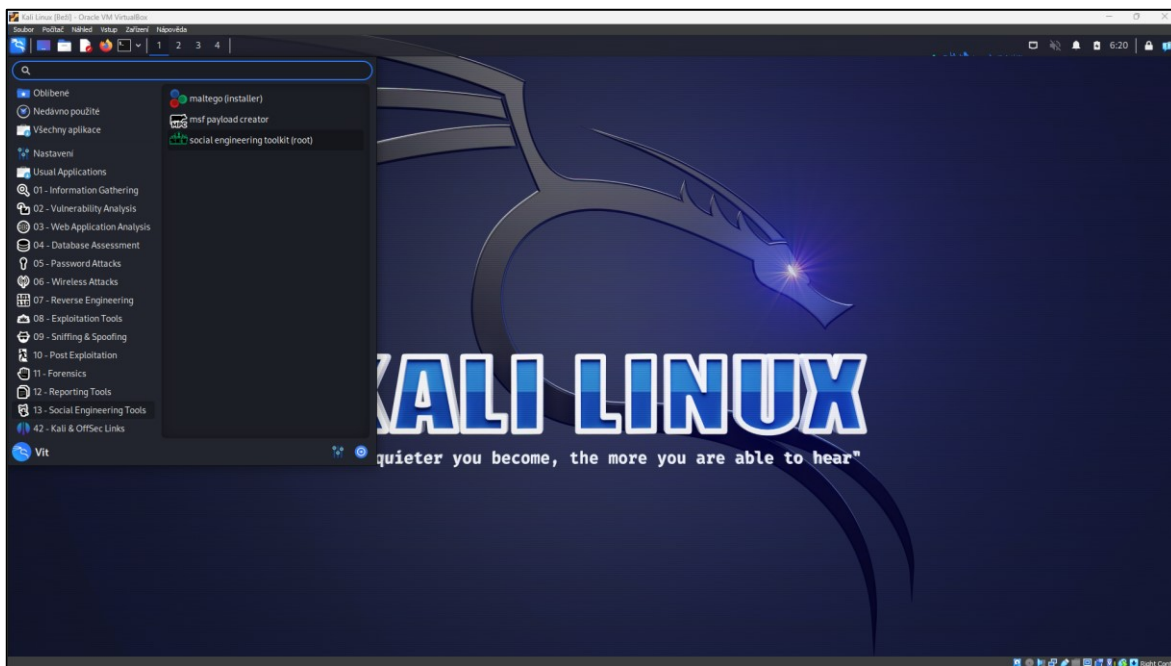
V této podkapitole bude demonstrováno, jak snadno lze vytvořit repliku jakékoli webové stránky bez nutnosti znalosti programovacího jazyka či jiných kvalifikací. Proces bude podrobně zdokumentován a k vytvoření této repliky bude využit operační systém Kali Linux, jak bylo již zmíněno v předchozích kapitolách. Výsledkem této části bude průchod procesem tvorby falešné phishingové stránky, přičemž pro tyto účely bude použita stránka STAGu Univerzity Tomáše Bati.

Pro dosažení co nejvěrnějšího zobrazení reálných kybernetických útoků, byl pro tvorbu použit open source nástroj The Social-Engineer Toolkit (SET), který je široce využíván penetračními testery a etickými hackery. SET umožňuje komplexní simulace kybernetických útoků na profesionální úrovni s možností úpravy operací podle vlastního uvážení. Tento nástroj je často využíván jak etickými, tak i klasickými hackery.

Na rozdíl od nástroje PhishMe, který byl zmíněn v předchozích kapitolách, SET umožňuje tvorbu komplexních kybernetických útoků s širokou paletou funkcí, které jsou prakticky neomezené a lze je upravovat podle potřeby. PhishMe na druhé straně funguje především výborně jako prostředek pro sběr a vyhodnocení dat z phishingových kampaní, které lze pomocí něj i vytvářet, ale jeho použití je omezeno několika faktory, jako je nutnost předplatného plné verze a omezení na počet domén. Pro účely návrhu kybernetického útoku v této práci by PhishMe nebyl dostačující.

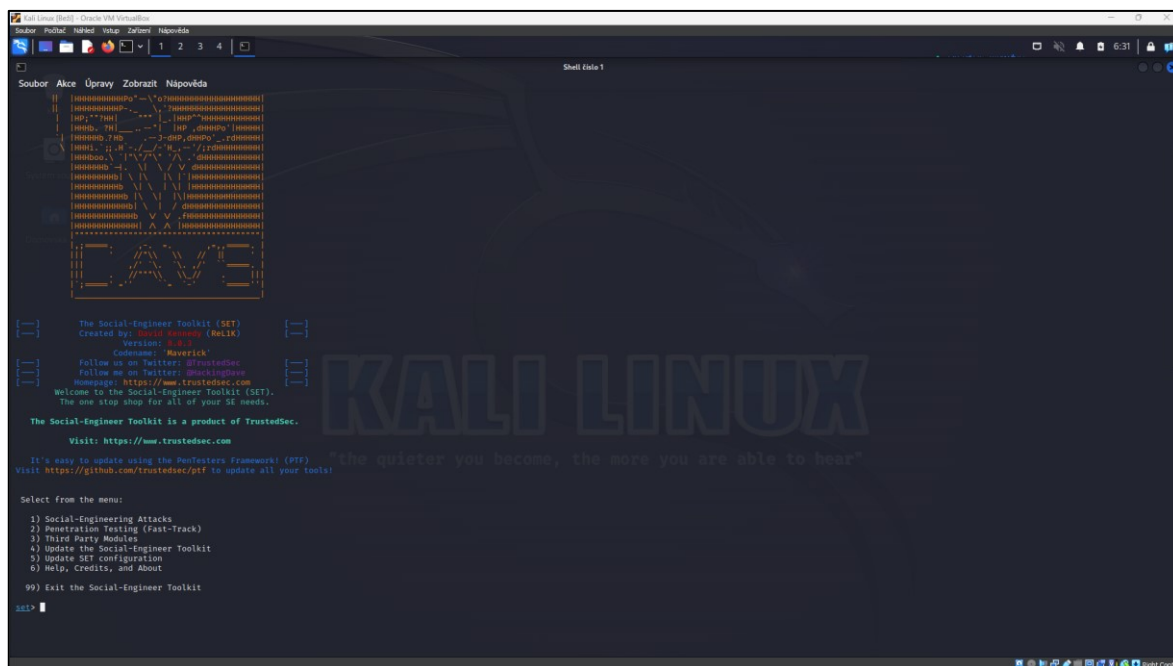
Kali Linux, jehož je SET součástí, je dostupný v freeware verzi a jeho použití tedy nepodléhá žádným omezením. SET nabízí většinu různých druhů útoků, na které má ve většině případů zabudovaný přímo vlastní nástroj, a je tudíž výhodnější volbou pro vytvoření scénáře útoku, který co nejvěrněji odráží reálné útoky prováděné hackerem.

Podmínkou užití SETu není vlastnit systém Kali Linux, ale v tomto systému je předinstalovaný jako defaultní nástroj, proto je využití celého operačního systému nejjednodušší možností. Nástroj SET je umístěn v menu aplikací Kali Linuxu, konkrétně v 13. kategorii Social Engineering Tools.



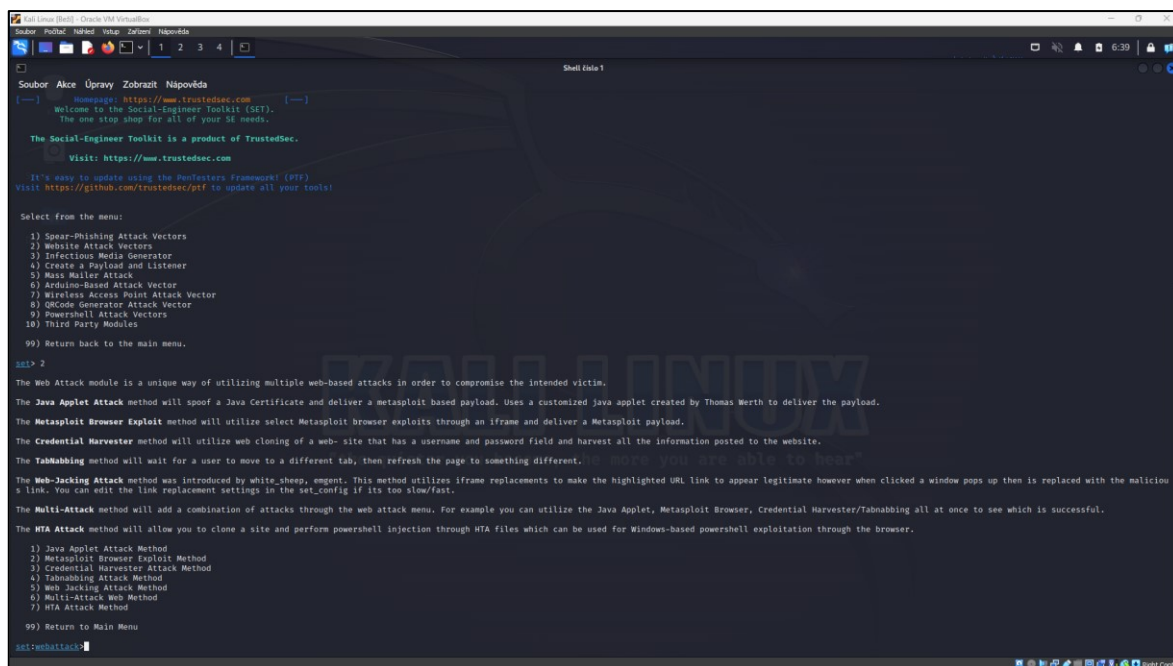
Obrázek 9: Umístění nástroje SET (zdroj: vlastní)

Po spuštění tohoto nástroje bude veškerá činnost prováděna formou příkazů v prostředí terminálu. V úvodu bude na výběr v menu z několika různých činností možných s tímto nástrojem dělat, v tomto případě bude zvolena možnost 1) Social-Engineering Attacks zadáním hodnoty 1 do příkazového řádku a potvrzením klávesou Enter.



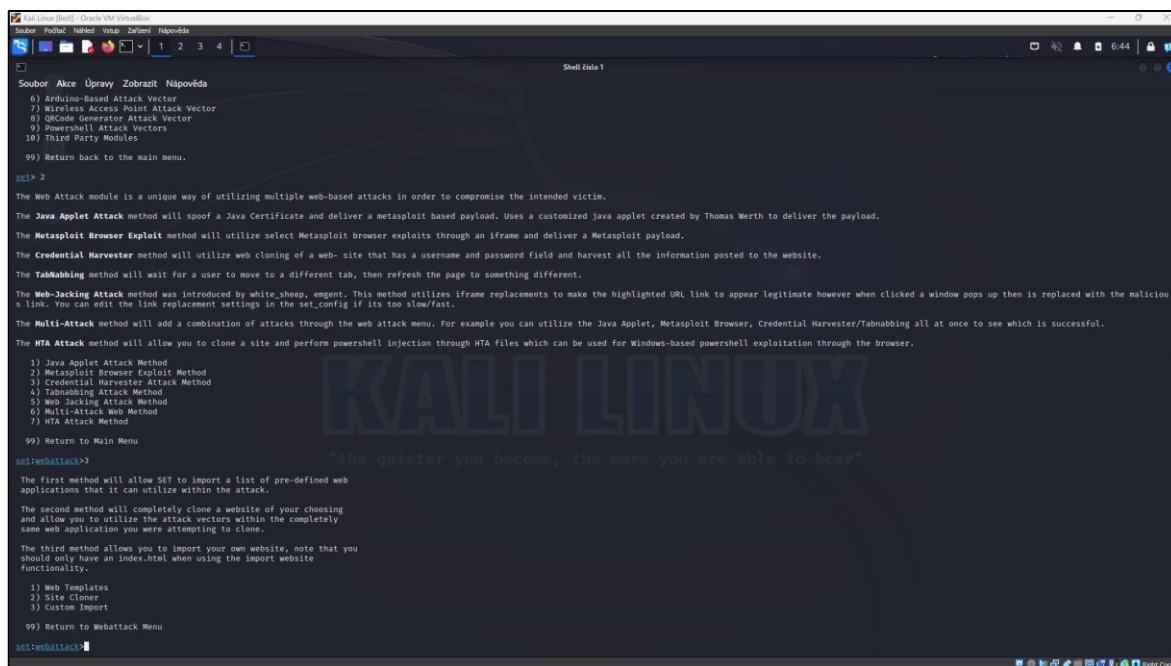
Obrázek 10: Menu možností nástroje SET (zdroj: vlastní)

Poté bude k dispozici další podrobnější menu, kde bude na výběr z několika možností útoků od spear phishingu přes možnosti generovat hromadné emaily, až po zahrnutí různých modulů vytvořených třetími stranami jako rozšíření nástroje SET. V tomto případě bude potřebné zvolit útoky na webové stránky, tudíž zapsání hodnoty „2“.



Obrázek 11: Nabídka webových útoků (zdroj: vlastní)

V dalším menu budou na výběr konkrétní útoky na webové aplikace. Všechny možnosti jsou v tomto případě i vysvětleny přímo v terminálu. V tomto případě je na výběr ze 7 různých metod. Metoda Credential Harvester Attack Method má za cíl získat přihlašovací údaje tím, že vytvoří webovou stránku identickou s cílovou stránku; tentokrát tedy bude pro výběr zapsána hodnota „3“.



```
Shell (msf5)
Soubor: Alice Úpravy Zobrazit Nápověda
0) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

msf5> web
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.
The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web-Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu

msf5:webattack> 3
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

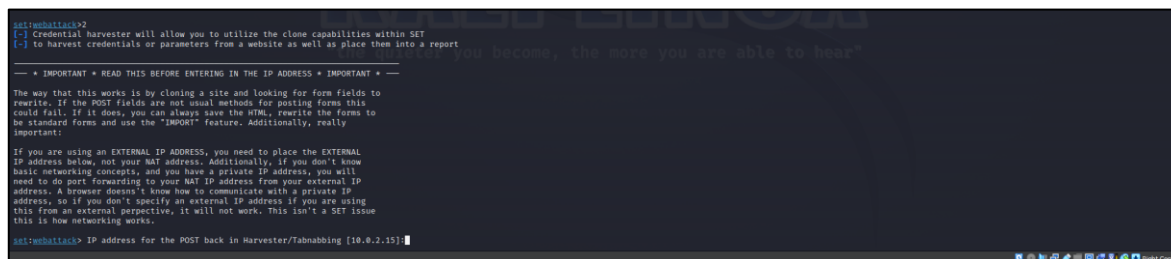
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu

msf5:webattack>
```

Obrázek 12: Výběr konkrétních metod (zdroj: vlastní)

V této nabídce jsou na výběr už jen tři možnosti, první nabízí zobrazení seznamu předdefinovaných webových aplikací, druhá možnost kompletně okopíruje jakoukoli webovou stránku a třetí možnost nabízí import vlastní webové stránky. Jako možnost bude tedy zapsána hodnota „2“.



```
msf5:webattack> 2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-----
* IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *
-----

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

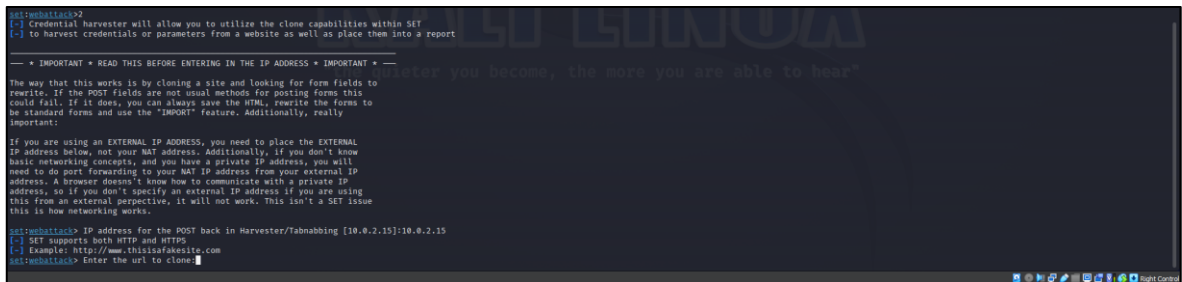
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

msf5:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
```

Obrázek 13: Zadání IP adresy (zdroj: vlastní)

V dalším kroku bude vyžadováno zadání IP adresy, která bude prozatím fungovat místo URL adresy falešné stránky.

Pozn. IP adresa se hodnotí jako citlivý údaj, pro účely této práce je Kali Linux spuštěn na virtuálním počítači. Každý virtuální počítač má vlastní virtuální síťové rozhraní s unikátní IP adresou, která je platná pouze v rámci této interní virtuální sítě.



```
set:~#kali@kali>
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important!

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

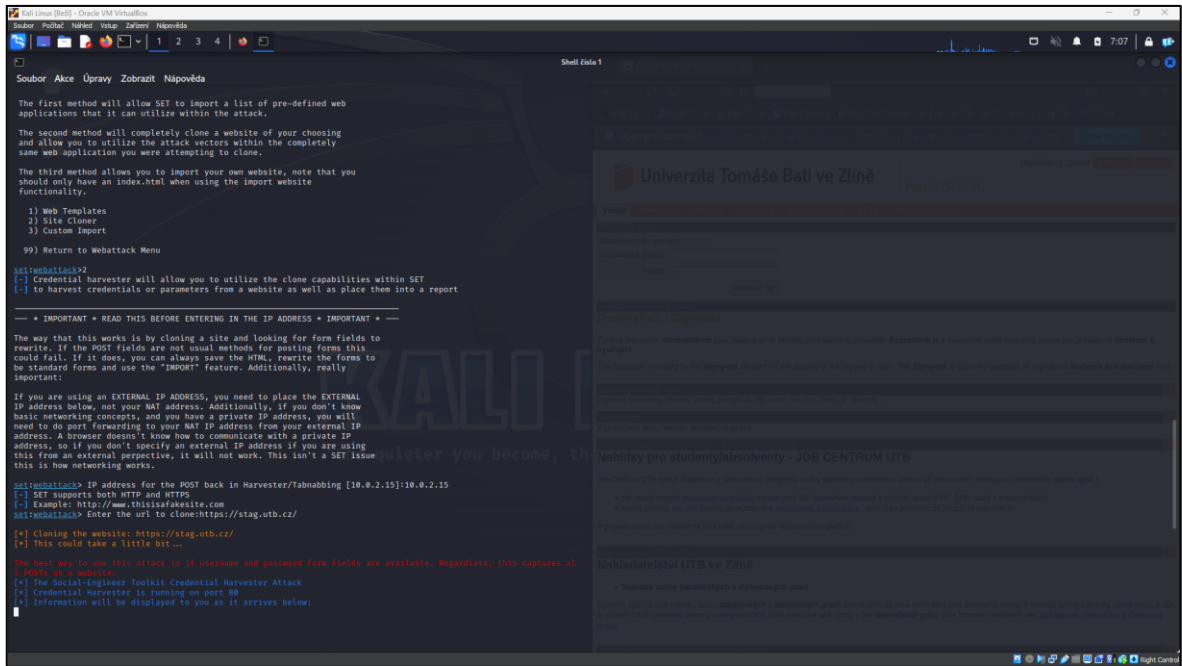
set:~#kali@kali> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.0.2.15
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakeite.com
set:~#kali@kali> Enter the url to clone:
```

Obrázek 14: Vložení URL adresy stránky k naklonování (zdroj: vlastní)

Pro názornou ukázkou v této práci nebude využito konkrétní nemocniční zařízení, ale replikovaná stránka bude informační systém pro studenty UTB Zlín. Jedná se pouze o edukační účely a tato práce není návod na kybernetický útok ani na páchaní žádné trestné činnosti. Stejným způsobem by se dala okopírovat jakákoliv jiná stránka, například pro přihlášení zaměstnanců do systémů příslušné nemocnice.

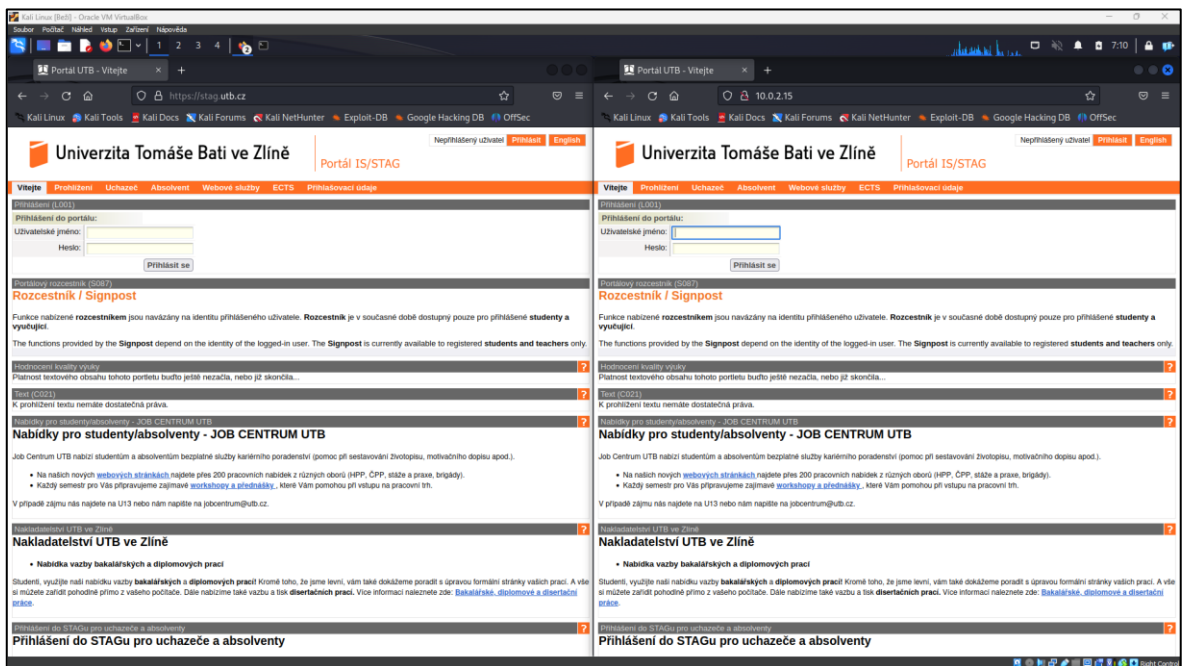
Do terminálu tedy bude zadáno <https://stag.utb.cz>. Odkaz na tuto stránku je dostupný z oficiálních stránek univerzity v záložce Portál IS/STAG.





Obrázek 15: Zadání cílové stránky (zdroj: vlastní)

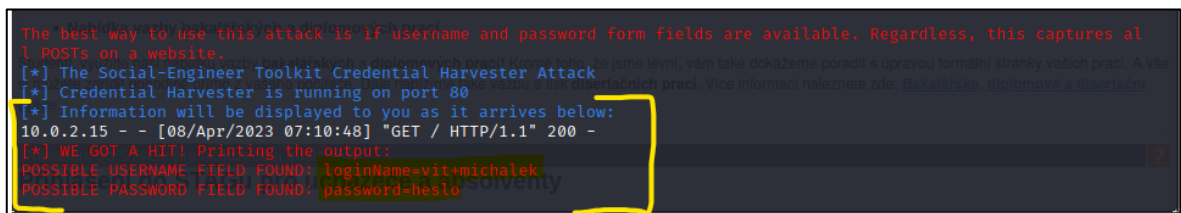
V této chvíli je stránka připravena a běží na adrese předtím zadané IP adresy, do prohlížeče v části URL adresy musí být teda zadána stejná IP adresa. Terminál vyobrazuje krátké shrnutí toho, co bylo zadáno a informuje o tom, že veškerou aktivitu na falešné stránce bude vypisovat níže.



Obrázek 16: Srovnání originální (vlevo) a falešné stránky (vpravo) (zdroj: vlastní)

Ze srovnání je patrné, že rozdíly v originální, a právě replikované stránky jsou doslova nulové. Veškeré prvky které obsahuje stránka jsou zkopírovány do podoby falešné stránky, fungují všechny animace tlačítek při pohybu myši. V případě, že uživatel klikne na některý z odkazů přesměrovávající na jinou stránku, respektive stránku, při které se změní URL adresa, bude odkázán na skutečnou stránku, kam by byl odkázán při kliknutí na stejný odkaz na originální stránce. URL adresa je v tomto případě jediné, co originální a falešnou stránku odlišuje, jak již bylo zmíněno v teoretické části této práce, URL je originální a nelze replikovat 1:1, falešná stránka tedy vždy bude nějak odlišná, byť jen v jednom znaku.

Zbývá teda jen zkouška vyplnění údajů, jestli budou po zadání do přihlašovacího formuláře falešné stránky zobrazeny odkryté v terminálu. Terminál by měl zobrazovat jakékoliv zadané údaje bez ohledu na to, jestli přihlášení proběhne nebo ne, je tedy možno zadat i falešné údaje pro demonstraci.



```
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [08/Apr/2023 07:10:48] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: loginName=vit+micchalek
POSSIBLE PASSWORD FIELD FOUND: password=heslo
```

Obrázek 17: Údaje zadané do přihlašovacího formuláře falešné stránky (zdroj: vlastní)

Jak je možno vidět, terminál vypsal zadané údaje včetně časového údaje, kdy k tomu došlo. Falešná stránka se po zadání údajů aktualizovala, potenciální oběti se tedy objevila stránka znovu bez přihlašovacích údajů. K přihlášení tedy nedošlo, všechny zadané informace však v této chvíli už mohl potenciální útočník vidět v terminálu nástroje SET. Útok byl tedy v tomto případě úspěšný a útočník může využít získané údaje k přihlášení na skutečné stránce a bude tak mít k dispozici všechna data, která měla zůstat zabezpečená.

V tomto případě má tedy útočník vytvořenou během pár kliknutí věrnou kopii webové aplikace spuštěnou na IP adrese, kterou zadal. Pro rozeslání oběti je vhodné aby falešná stránka běžela na klasické URL adrese, ideálně co nejpodobnější s originální URL adresou stránky. Jedním z možných způsobů, jak by se dala webová stránka spuštěná na IP adrese předělat na klasickou URL adresu, je zakoupit doménu a nastavit ji tak, aby směřovala na IP adresu, na které je webová stránka hostována.

Proces nastavení domény tak, aby směřovala na IP adresu, se liší v závislosti na poskytovateli domén a hostingu. Většina poskytovatelů domén má nástroje pro nastavení DNS, kde lze přidat A záznam (anglicky "A record"), který přidává záznam pro doménu a mapuje ji na konkrétní IP adresu. Pokud má webová stránka klasickou URL adresu, je možné také provést přesměrování pomocí konfigurace serveru, kde je stránka hostována. V tomto případě by bylo nutné konfiguraci serveru změnit tak, aby požadavky na klasickou URL adresu přesměroval na IP adresu, kde webová stránka běží.

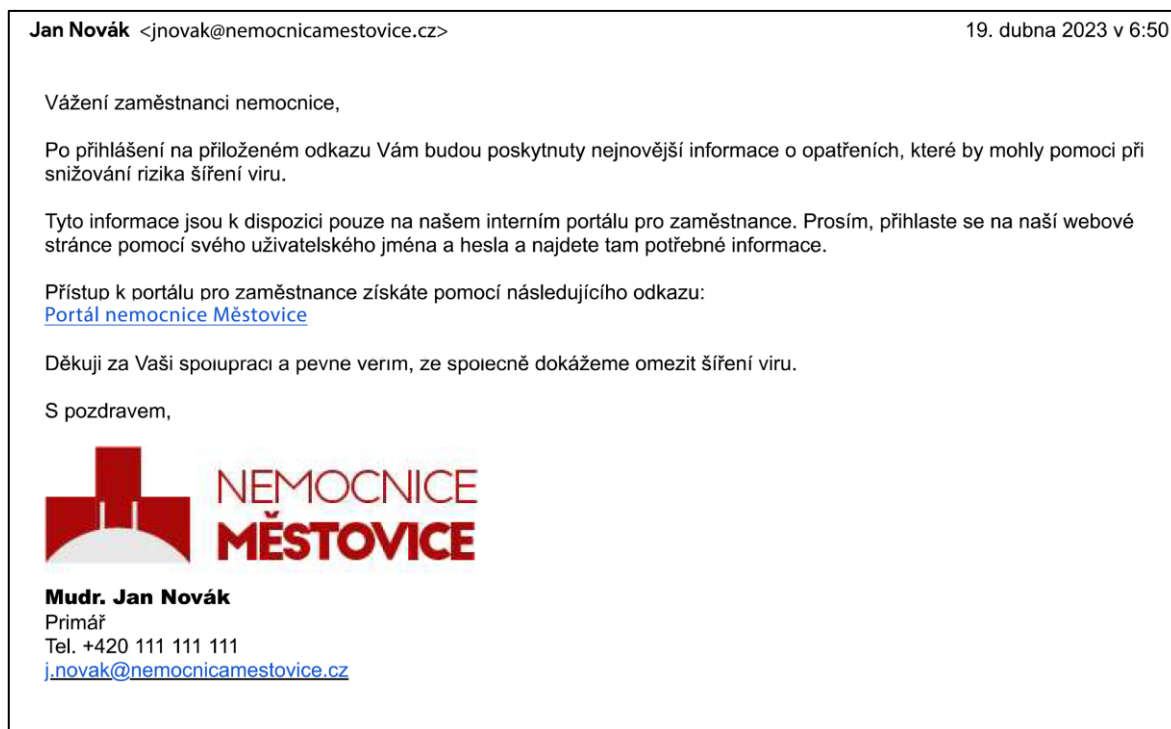
### 6.2.2 Vytvoření spear-phishingového emailu

V této kapitole budou vytvořeny dva phishingové emaily, které budou cílit na smyšlené zaměstnance fiktivní nemocnice. Útok by mohl potenciálně cílit na jakoukoliv nemocnici, pokud by byly do příkladu dosazeny reálné údaje. Pokud útočník cílí na konkrétní objekt je výhodné zajistit si kopii emailu přímo od některého ze zaměstnanců. To může být provedeno například posláním emailu s nějakým obecným dotazem, který mu bude zodpovězen. Tím získá šablonu pro tvorbu phishingového emailu z hlediska potřebných grafických prvků a formátování.

Pro příklad budou vytvořeny vzory phishingových emailových útoků na fiktivní Fakultní nemocnici v Městovicích. V případě úspěšného útoku by byl útočník schopný dostat se pomocí přihlašovacích údajů zaměstnanců do interní databáze nemocnice, kde by mu mohly být zpřístupněny osobní informace ze zdravotní dokumentace klientů.

V prvním případě bude vytvořen scénář klasického phishingového emailu, který bude cílit na všechny zaměstnance nemocnice. Cílem útočníka bude získat jejich pracovní přihlašovací údaje, které by mohli vést do interní komunikace nemocnice, případně k citlivým informacím klientů nemocnice.

Útočník bude v emailu vystupovat jménem fakultní nemocnice v Městovicích, primáře MUDr. Jana Nováka. Předmětem emailu budou aktuální koronavirová opatření v nemocnici. Email bude vyzývat k přihlášení se do portálu zaměstnance pomocí přiloženého odkazu, ten bude odkazovat na falešnou stránku vzhledově totožnou s reálným přihlašovacím portálem zaměstnanců.



Obrázek 18: Návrh phishingového emailu cílící obecně na zaměstnance nemocnice (zdroj: vlastní)

V druhém návrhu bude zobrazen spear phishingový email, tedy email cílící na konkrétního člověka. Rozdíl ve vytváření je především v tom, že obsah spear phishingového emailu by měl mnohem více konkrétní a zacílený, tak aby měla oběť pocit důvěry v email, respektive odesílatele a v kombinaci s tím, že je urgována důležitou zprávou, nevěnovala dostatečnou pozornost odhalování manipulace.

Cílem tohoto spear phishingového emailu bude hlavní vrchní sestra Mgr. Kateřina Marešová. Kontaktní údaje, jako je pracovní email, telefonní číslo a pozice, kterou zastává v nemocnici, jsou dostupné na webových stránkách nemocnice pro veřejnost. Útočník tedy zjistí potřebné informace online. Odesílatel bude užívat identitu Ing. Martina Krále, specialisty na bezpečnost IT. Potřebné informace pro odcizení jeho pracovní identity jsou také dostupné na webových stránkách nemocnice. Předmětem bude kybernetický incident, následkem kterého bude sestra kontaktována s žádostí o zabezpečení pracovního účtu.



Obrázek 19: Návrh spear phishingového emailu cílící na konkrétní osobu (zdroj: vlastní)

Jak je možné vidět v obou vzorech úroveň propracování je velmi vysoká. Ve své podstatě lze říct, že jediný údaj, který útočník nemůže okopírovat, je samotná emailová adresa, ze které je email odeslán. Často je však možné změnit pouze jediný symbol, kterého si na první pohled nemusí oběť všimnout. V tomto případě lze předpokládat, že zaměstnanci nemocnice používají emailové adresy ve formátu [j.prijmeni@nemocnicamestovice.cz](mailto:j.prijmeni@nemocnicamestovice.cz). V těchto vzorech je možno si povšimnout, že emaily pochází z adresy ve vzoru [jprijmeni@nemocnicamestovice.cz](mailto:jprijmeni@nemocnicamestovice.cz). Stačí tedy odlišit pouhou tečkou reálnou adresu od té falešné. Všechny ostatní údaje mohou být reálné údaje osoby, které ukradená identita původně patří.

### 6.3 Model procesu phishingového útoku

V této kapitole bude vytvořen model vývojového diagramu, který bude zobrazovat celý proces phishingového útoku od výběru cíle až po získání citlivých dat. Tento model bude pouze orientační za účelem vzdělávání a nejedná se o návod pro páčání kybernetické kriminality.

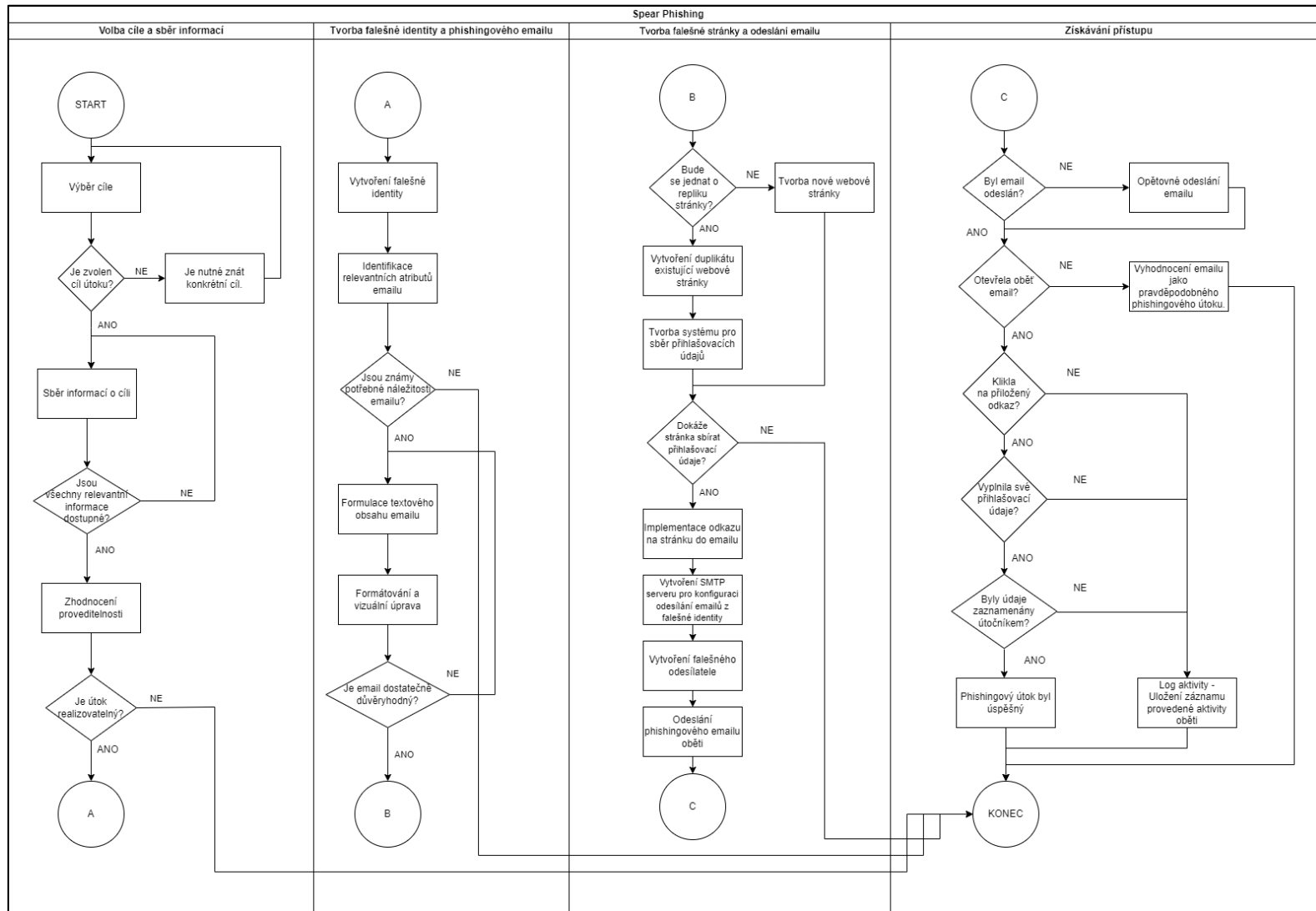
Jedná se o grafické zobrazení postupu, procesu nebo algoritmu pomocí standardizovaných symbolů a propojení mezi nimi. Jeho cílem je vizualizace a zjednodušení složitých postupů pro lepší pochopení a efektivní komunikaci mezi týmy nebo jednotlivci.

Vývojový diagram se skládá ze symbolů, které představují jednotlivé kroky nebo činnosti, a z propojení mezi nimi, což reprezentuje tok informací, materiálů nebo dat. Existuje několik druhů symbolů, které se používají v závislosti na tom, jaké kroky jsou zahrnuty. Například symbol pro počáteční a konečný bod, symbol pro podmínky nebo rozhodování, symbol pro příkaz nebo akci, symbol pro vstup nebo výstup dat a další.

Fungování vývojového diagramu začíná vytvořením celkového plánu nebo náčrtu procesu nebo algoritmu. Tento plán se pak převede do grafické podoby pomocí symbolů a propojení mezi nimi. Každý symbol představuje konkrétní činnost nebo rozhodnutí, které je třeba provést v daném kroku. Propojení mezi symboly ukazuje, jak informace, materiály nebo data putují mezi jednotlivými kroky a jak se proces vyvíjí.

Vývojový diagram může být použit v mnoha oblastech, například v programování, inženýrství, řízení projektů, marketingu nebo výrobě. Jeho hlavní výhodou je, že umožňuje snadno pochopit postup a identifikovat možné chyby nebo úzká místa v procesu.

K vytvoření vývojového diagramu bude použit software yEd, který umožňuje tvorbu profesionálně vypadajících diagramů s množstvím funkcí pro editaci a úpravu.



Obrázek 20: Model procesu phishingového útoku (zdroj: vlastní)

## 6.4 Návrh opatření

V průběhu práce bylo popsán proces phishingového útoku a prostřednictvím navrženého modelu byl znázorněn. Na základě těchto zjištění je možnost zaměřit se na příčiny, respektive konkrétní kroky, na základě nich bylo možno útok provést. Právě na základě těchto zjištěných slabin je vhodné navrhnout opatření pro jejich posílení.

Pro zajištění integrity a maximální kybernetické bezpečnosti digitálních aktiv a ochranu citlivých údajů je nutné přijmout a zajistit proaktivní opatření. Tento návrh uvádí řadu opatření ke zvýšení kybernetické bezpečnosti. Pro přehlednost je návrh rozdělen do několika kategorií.

**Informovanost zaměstnanců** – Všichni zaměstnanci si musí být vědomi rizik kybernetických útoků, včetně phishingu, malwaru a ransomwaru. Je třeba zavést pravidelná školení a programy zvyšování povědomí o kybernetické bezpečnosti, které zaměstnance poučí o nebezpečí otevírání podezřelých e-mailů, klikání na škodlivé odkazy a stahování neautorizovaného softwaru.

Chráněné subjekty mohou například zařadit phishingové kampaně, stejně jako tomu bylo u společnosti v praktické části. Existuje celá řada podobných služeb, jako je PhishMe, kde je možné zaregistrovat svoji společnost a mít tak přístup k rozsáhlým možnostem vytváření kybernetických kampaní pro testování zaměstnanců. Tyto kampaně se nemusí nutně týkat phishingu, naopak je žádoucí rozšiřovat povědomí o všech formách kybernetických útoků

Je nutné zajistit, aby všichni noví zaměstnanci prošli školením týkajícím se kybernetické bezpečnosti před zahájením práce. Dalším nezbytným opatřením je implementovat školením všech zaměstnanců týkající se kybernetické bezpečnosti s pravidelnými obnovovacími kurzy. Jak bylo v průběhu práce zmíněno několikrát, trendy kybernetických útoků se neustále mění, proto je vhodné zařadit tyto školení a přezkušování v častějších intervalech, například každých 6 měsíců. Chráněný subjekt může taktéž zavést opatření pro monitorování a hlášení kybernetických incidentů. Možné je i zvážit vytvoření interní příručky pro zaměstnance s pravidly a postupy týkajícími se kybernetické bezpečnosti. A dále zajistit, aby každý zaměstnanec měl přístup k aktuálním informacím a tipům týkajícím se kybernetické bezpečnosti.



Pro zvýšení zájmu o tuto problematiku mezi zaměstnanci, je možné zapojit zaměstnance do procesu zvyšování bezpečnosti a vytváření vlastních návrhů na zlepšení kybernetické bezpečnosti v organizaci.

**Řízení přístupu** – Přístup k citlivým údajům musí být omezen pouze na oprávněné pracovníky. Musí být zaveden systém silných kontrol přístupu, který zajistí, že k datům budou mít přístup pouze zaměstnanci, kteří to potřebují. To zahrnuje používání silných hesel, dvou faktorového ověřování a omezení administrátorských oprávnění.

Pro zajištění řízení přístupu k citlivým údajům je třeba zavést silné kontroly přístupu, které omezí přístup pouze na oprávněné zaměstnance. Jedním z opatření může být zavedení centrálního systému správy identit a přístupů (IAM), který umožní spravovat a sledovat přístupová práva všech uživatelů. IAM systém by měl být důkladně nastaven s ohledem na potřeby jednotlivých uživatelů a měl by umožnit nastavit přístupová práva jen na konkrétní data, která jsou pro ně potřebná.

Dalším opatřením může být zavedení silných hesel pro všechny zaměstnance a pravidelné změny hesel. Silná hesla by měla být složená z kombinace velkých a malých písmen, číslic a speciálních znaků a měla by být dostatečně dlouhá, aby byla odolná proti brute force attackům. Zaměstnanci by měli být pravidelně školeni, aby byli schopni si takové heslo vytvořit a používat.

Pro posílení zabezpečení je též vhodné zavedení dvou faktorového ověřování (2FA) pro přístup k citlivým údajům. 2FA umožní ověření totožnosti uživatele pomocí dvou nezávislých faktorů, jako jsou například heslo a kód, který uživatel dostane na svůj mobilní telefon. Toto opatření výrazně zvýší bezpečnost přístupu k citlivým datům.

Chráněný subjekt by měl omezit administrátorské oprávnění pouze na nezbytné zaměstnance. Administrační účty mají mnohem větší přístupová práva než běžné účty, proto je důležité, aby měli přístup jen ti, kteří skutečně potřebují. Tím se minimalizuje riziko zneužití administrátorských oprávnění a snižuje se tak úroveň rizika kybernetických útoků.

Posledním navrhovaným opatřením z oblasti řízení přístupu je zabezpečení všech zařízení, na kterých jsou uloženy citlivé údaje, včetně telefonů a počítačů, a zavedení protokolů pro odstraňování citlivých dat z těchto zařízení v případě ztráty nebo odcizení pomocí specializovaných nástrojů pro správu mobilních zařízení (MDM) nebo vzdálené správy počítačů (RMM). Tyto nástroje umožňují správcům IT týmu centrálně spravovat počítače a mobilní zařízení v rámci organizace, včetně provádění vzdáleného mazání dat.

Data uložená na zařízení by měla být šifrována, aby se zabránilo jejich neoprávněnému přístupu. To zahrnuje použití technologií jako je BitLocker pro Windows nebo FileVault pro MacOS.

**Softwarová ochrana** – Významným nástrojem pro ochranu proti phishingovým i jiným útokům je používání antivirového softwaru s funkcemi, jako jsou detekce a blokování phishingových webových stránek. Mezi antivirové programy s touto funkcí patří Avast, Avira, Kaspersky a další. Mnoho internetových prohlížečů (např. Google Chrome, Mozilla Firefox, Microsoft Edge) nabízí anti-phishingová rozšíření, která umožňují rychlé zjištění, zda je navštívená stránka podezřelá. Tato rozšíření například kontrolují URL adresy a srovnávají je s databází známých phishingových webů. Jednou z možností mohou být též DNS filtry. Jedná se o nástroj, který umožňuje blokovat přístup k nebezpečným webovým stránkám na úrovni sítě. Mezi DNS filtry patří například OpenDNS nebo Cisco Umbrella.

**Zabezpečení sítě** – Síťová infrastruktura musí být zabezpečena proti hrozbám. Firewally musí být nakonfigurovány tak, aby blokovaly neoprávněný přístup, a musí být zavedeny systémy detekce narušení, které budou odhalovat narušení a předcházet jim. Síťový provoz musí být monitorován kvůli známým škodlivé činnosti a musí být pravidelně aplikovány záplaty a aktualizace.

Prvním fází je nakonfigurovat firewally tak, aby blokovaly neoprávněný přístup. Firewall je základním prvkem zabezpečení sítě a slouží k ochraně sítě před útoky ze strany vnějšího světa. Firewally musí být pravidelně aktualizovány a je třeba zajistit, aby je nebylo možno obejít.

Dalším krokem je zavedení systémů detekce narušení, které pomohou odhalit útoky a předcházet jim. Tyto systémy sledují síťový provoz a hledají známky škodlivé činnosti. Pokud detekují podezřelou aktivitu, okamžitě upozorní správce, bylo možno rychle reagovat a odstranit hrozbu. Kromě toho je také nutné pravidelně aplikovat záplaty a aktualizace na všechny sítě a zařízení v síti. Záplaty a aktualizace obsahují opravy a vylepšení, které odstraňují známé bezpečnostní chyby a zabraňují útokům.

Důležitým bodem je pravidelné monitorování síťového provozu. To pomůže odhalit škodlivou činnost a umožní rychle reagovat na hrozby. Monitorování síťového provozu lze provádět pomocí specializovaného softwaru, který umožňuje sledovat všechny události v síti a detekovat neobvyklé aktivity. Takový software může být například SolarWinds Network

Performance Monitor, Wireshark nebo Splunk Enterprise. Výběr konkrétního nástroje závisí na potřebách a velikosti organizace, stejně jako na finančních možnostech.

**Zálohování a obnova dat** – Je třeba zavést plány zálohování a obnovy dat, aby se zajistilo, že v případě kybernetického útoku nedojde ke ztrátě kritických dat. Je třeba provádět pravidelné zálohování a zálohy musí být uloženy mimo pracoviště na bezpečném místě. Plány obnovy musí být pravidelně testovány, aby se zajistila jejich účinnost.

Pro zabezpečení dat je nutné pravidelné zálohování dat na primárních serverech a jejich kopírování na externí zálohovací zařízení. Pro významné celostátní zařízení je však důležité zajistit vysokou dostupnost a rychlou obnovu dat v případě havárie. Proto je možno využít různé technologie a postupy, jako je duplicita dat na více serverech, použití technologií jako RAID a SAN, testování a ověřování zálohovacích procesů a obnovy dat. Tyto postupy a technologie umožňují organizacím rychle reagovat na havárie a minimalizovat výpadky činnosti a ztráty dat.

Pro zavedení zálohovacích plánů je třeba vypracovat podrobný plán zálohování a obnovy dat. Tento plán by měl obsahovat informace o tom, jaké soubory a data budou zálohovány a jak často. Je důležité mít také jasnou definici, jaké jsou kritická data a jak se budou zálohovat.

Dalším krokem je zajištění bezpečného uložení záloh. Kritická data musí být zálohována mimo pracoviště, například v cloudu nebo na externích discích, které jsou uloženy v bezpečném místě, kam se hackeři nemohou dostat.

Plán obnovy dat musí být pravidelně testován, aby se zajistila jeho účinnost v případě krize. Tento proces musí být také dokumentován a řádně zaznamenán, aby v případě potřeby bylo možné okamžitě obnovit data. Je důležité mít také jasně definované odpovědnosti a pravomoci v rámci plánů zálohování a obnovy dat, a to včetně toho, kdo bude zodpovědný za jejich implementaci, kdo bude zodpovědný za testování a jak budou v případě potřeby data obnovena.

V neposlední řadě je třeba také zajistit pravidelné aktualizace a údržbu systémů zálohování a obnovy dat, aby byly v souladu s nejnovějšími požadavky kybernetické bezpečnosti a aby byly schopny účinně reagovat na aktuální hrozby.

**Plán reakce na incidenty** – V případě narušení kybernetické bezpečnosti je nezbytné mít k dispozici plán reakce na incident. Plán by měl popisovat kroky, které je třeba v případě narušení provést, včetně informování zúčastněných stran, uchování důkazů a obnovení

provozu. Plán musí být pravidelně revidován a aktualizován, aby byla zajištěna jeho účinnost.

Pro efektivní reakci na kybernetický incident je klíčové vytvořit tým odborníků s odpovídajícími znalostmi a zkušenostmi, který bude schopen rychle reagovat na incidenty, sbírat důkazy a koordinovat s ostatními zainteresovanými stranami. Tento tým by měl být zodpovědný za vytvoření a implementaci plánu reakce na incidenty. V tomto plánu je důležité stanovit kritické systémy a data, které musí být chráněny a v případě výpadku obnovovány jako první. Plán by měl obsahovat seznam kroků, které je třeba v případě incidentu provést, včetně izolace infikovaných systémů, změny hesel a zvýšení bezpečnostních opatření.

Dalším důležitým opatřením je pravidelné testování plánu, které ověří jeho funkčnost a připravenost týmu na různé scénáře kybernetických útoků. Testování může být provedeno pomocí simulací a cvičení, která simulují různé typy útoků a umožní týmu lépe porozumět situaci a připravit se na ni.

Plán by měl být pravidelně revidován a aktualizován v souladu s novými hrozbami a vývojem technologií. Je důležité přizpůsobit plán aktuálním potřebám organizace a změnám v prostředí, ve kterém organizace působí. Revize a aktualizace plánu zajistí jeho stále větší připravenost a schopnost rychle a efektivně reagovat na kybernetické hrozby.

Výše uvedená opatření jsou důležitá pro zvýšení kybernetické bezpečnosti subjektu. Je nezbytné, podniknout proaktivní kroky k ochraně digitálních aktiv a citlivých údajů před kybernetickými hrozbami. Zavedením těchto opatření je možné snížit riziko kybernetických útoků a zajistit, aby subjekt zůstal bezpečný.

## ZÁVĚR

V rámci této práce byl proveden průzkum problematiky etického hackingu a jeho využití v kontextu subjektů ochrany obyvatelstva. Vzhledem k rozsáhlosti a hloubce celé problematiky kybernetických útoků, byla praktická část cílena převážně na jeden konkrétní typ útoku, tedy phishing.

Na základě získaných poznatků bylo provedeno zhodnocení využitelnosti etického hackingu v této oblasti. Tomuto dopomohla mimo jiné praktická analýza kybernetického zabezpečení na dostupném subjektu podobného rozsahu, která ukázala že zkoumaná problematika je v této oblasti velmi aktuální a významná.

Rešerše související problematiky prokázala, že etický hacking může jako nástroj významně dopomoci ke zvýšení kybernetické bezpečnosti. Zvláště důležitou součástí zabezpečení je pravidelné vzdělávání a aktualizace. To platí i pro etické hackery, kteří musí neustále sledovat nové trendy z oblastí kyberprostoru, jelikož se jedná – jak bylo již několikrát zmíněno – o neustále se rozvíjející obor, v rámci něhož vznikají neustále nové způsoby a metody útoku i obrany proti nim.

Proto je zvláště důležité, aby etičtí hackeři byli schopni identifikovat slabiny v systémech a navrhnout účinná opatření pro zajištění jejich ochrany proti stále sofistikovanějším útokům. Práce etického hackera může subjektu dopomoci odhalit chyby a slabiny v zabezpečení a mimo jiné i dopomoci s jejich nápravou. Pro každý takový subjekt rozhodně stojí za zvážení využití služeb etického hackera, obzvláště v případě, kdy je působení tohoto subjektu zahrnuto do působnosti ochrany obyvatelstva České republiky.

Na základě navrženého scénáře kybernetického útoku bylo možné identifikovat slabá místa v bezpečnostních opatřeních subjektu ochrany obyvatelstva. Mimo jiné bylo ukázáno, jakými prostředky může být útok veden, a na základě této informace mohou být vyvinuty prostředky k ochraně před útoky. Podle výsledných poznatků byla navržena konkrétní opatření, která by měla být implementována pro zvýšení bezpečnosti. Během testování byl použit nástroj SET, který se jeví jako velice přehledný a nenáročný jak na výkon počítače, tak i na pochopení i pro neprofesionály.

V závěru této práce lze konstatovat, že etický hacking může být velmi významným nástrojem pro zajištění kybernetické bezpečnosti subjektů ochrany obyvatelstva. Z plynoucích výsledků této práce je možné shledat hlavní cíl a dílčí cíle stanoveny v úvodu této práce jako splněné.

## SEZNAM POUŽITÉ LITERATURY

19 Types of Phishing Attacks with Examples | Fortinet. Global Leader of Cybersecurity Solutions and Services | Fortinet [online]. Copyright © 2023 Fortinet, Inc. All Rights Reserved. [cit. 08.03.2023]. Dostupné z:

<https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks>.

ALENEZI, M.N., ALABDULRAZZAQ, H., ALSHAHER, A.A. and ALKHARANG, M.M., 2020. Evolution of Malware Threats and Techniques: A Review. International Journal of Communication Networks and Information Security, 12, vol. 12, no. 3, pp. 326-337 ProQuest Central. ISSN 2073607X.

ANTOŠ, Michal. Regulace kybernetické bezpečnosti v soukromém sektoru. Právní prostor [online]. 2020 [cit. 2023-02-07]. Dostupné z:

<https://www.pravniprostor.cz/clanky/obcanske-pravo/regulace-kyberneticke-bezpecnosti-v-soukromem-sektoru>.

AWAD, Ali Ismail a Machael FAIRHUST, 2018. Information security : foundations, technologies and applications [online]. London: Institution of Engineering & Technology [cit. 2023-03-03]. ISBN 978-1-84919-976-6.

BHADORIA, Nikhalesh. First Step To Ethical Hacking. Tennessee, USA: LIGHTNING SOURCE, 2018. ISBN 9386447193.

BROOKS, Charles J., Christopher GROW, Philip A. CRAIG Jr., Donald SHORT, 2018. Cybersecurity Essentials. Indianapolis: John Wiley & Sons. ISBN: 978-1-119-36239-5.

BUXTON, Oliver. Hacker Types: Black Hat, White Hat, and Gray Hat Hackers. AVAST [online]. 2022 [cit. 2023-02-02]. Dostupné z: <https://www.avast.com/c-hacker-types>.

CLARK, Casey a Michael COBB. Trojan horse (computing). SearchSecurity: Information Security information, news and tips [online]. Newton: TechTarget, c2000 2022 [cit. 2023-01-23]. Dostupné z: <https://www.techtarget.com/searchsecurity/definition/Trojan-horse>.

Co je skenování portů, © 2022. Avast [online]. [cit. 2023-03-03]. Dostupné z: <https://www.avast.com/cs-cz/business/resources/what-is-port-scanning#pc>.

COFFEY, Brain. The Black Book: Ethical Hacking + Reference Book. Blurb, 2016. ISBN 1367590493.

CyberSecurity.CZ. CyberSecurity.CZ [online]. 2017 [cit. 2023-02-02]. Dostupné z: <https://cybersecurity.cz/law.html>.

ČESKO. zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 1. 9. 2021. In: *Zákony pro lidi.cz* [online]. © AION CS 2010- 2022 [cit. 13. 2. 2023]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2014-181#p7-1>.

ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 6. 8. 2022. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2023 [cit. 13. 4. 2023]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2014-181>.

ČESKO. Zákon č. 89/2012 Sb., občanský zákoník - znění od 6. 1. 2023. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2023 [cit. 13. 4. 2023]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2012-89>.

DDoS Attack Types & Mitigation Methods | Imperva. Cyber Security Leader | Imperva, Inc. [online]. Copyright © 2022 Imperva. All rights reserved [cit. 03.03.2023]. Dostupné z: <https://www.imperva.com/learn/ddos/ddos-attacks/>.

DENIS, Matthew; ZENA, Carlos; HAYAJNEH, Thaier. Penetration testing: Concepts, attack methods, and defense strategies. In: 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016. p. 1-6.

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK, 2019. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing. ISBN 978-80-88260-39-4.

Features | Kali Linux. *Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution* [online]. Copyright © OffSec Services Limited 2023. All rights reserved. [cit. 08.04.2023]. Dostupné z: <https://www.kali.org/features/>.

Flipper Zero: Next Gen Hacking Tool for the Next Generation. Cybersecurity Conferences & News | SecureWorld [online]. Copyright © 2022 Seguro Group Inc. All rights reserved. [cit. 09.03.2023]. Dostupné z: <https://www.secureworld.io/industry-news/flipper-zero-next-gen-hacking-tool>.

G. Vishnuram, K. Tripathi and A. Kumar Tyagi, "Ethical Hacking: Importance, Controversies and Scope in the Future," 2022 International Conference on Computer

Communication and Informatics (ICCCI), Coimbatore, India, 2022, pp. 01-06, doi: 10.1109/ICCCI54379.2022.9740860.

Hackerským útokům čelily v Česku nemocnice, Národní knihovna či volební web - Novinky. [online]. Copyright © 2003 [cit. 05.04.2023]. Dostupné z: <https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-hackerskym-utokum-celily-v-cesku-nemocnice-narodni-knihovna-ci-volebni-web-40394428>.

HADNAGY, Christopher. Social Engineering: The Science of Human Hacking. 2nd Edition. Indianapolis: Wiley, 2018. ISBN 978-1-119-43372-5.

Houser, Pavel. 2013. „Bezpečnostní přehled: proč nepodceňovat nástroje pro script kiddies.“ ITBIZ [online]. 2022 [cit. 2023-02-02]. Dostupné z: <https://www.itbiz.cz/clanky/bezpecnostni-prehled-nepodcenovat-nastroje-pro-script-kiddies>.

HTTP response splitting attack. Cyphere. (2022, April 29). [online]. [cit. 2023-03-03]. Dostupné z: <https://thecyphere.com/blog/http-response-splitting/>.

HUB, Miloslav. Bezpečnost a ochrana informací v prostředí internetu. Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8.

I válka má svá pravidla | Lékaři bez hranic. Lékaři bez hranic | Nestranně, nezávisle, neutrálně [online]. Copyright © Ricardo Garcia Vilanova [cit. 05.04.2023]. Dostupné z: <https://www.lekari-bez-hranic.cz/pravidla-valky>.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virecha trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

Když se řekne ransomware - ITBiz.cz. Zprávy ze světa IT a byznysu - ITBiz.cz [online]. Copyright © 2019 Vydává [cit. 05.04.2023]. Dostupné z: <https://www.itbiz.cz/clanky/kdyz-se-rekne-ransomware>.

KOLOUCH, Jan a Pavel BAŠTA, 2019. CyberSecurity. 1. vydání. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-31-7.

KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.



Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030, 2013. Praha: Ministerstvo vnitra – generální ředitelství Hasičského záchranného sboru České republiky.

KOVALČÍK, Marek. 2020 [online]. Etický hacking – laicky a jednoduše. BDO Česká republika. [cit. 2023-02-02]. Dostupné z <https://www.bdo.cz/cs-cz/blog/it-security/12-2020/eticky-hacking---laicky-a-jednoduse>.

LARIN, Boris a Costin RAIU. MysterySnail attacks with Windows zero-day. Securelist [online]. Moscow: Kaspersky, c2022, 12 Oct 2021 [cit. 2023-02-28]. Dostupné z: <https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/>.

Malwarebytes: Hacking definition: What is hacking? [online], 2022. [cit. 2022-02-02]. Dostupné z: <https://www.malwarebytes.com/hacker>.

Ministerstvo vnitra – generální ředitelství Hasičského záchranného sboru České republiky. Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030. In: *Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030* [online]. Praha, 2013, s. 61 [cit. 2023-04-26]. Dostupné z: [https://www.vlada.cz/assets/ppov/brs/dokumenty/Koncepce-ochrany-obyvatelstva-2020-2030\\_1\\_.pdf](https://www.vlada.cz/assets/ppov/brs/dokumenty/Koncepce-ochrany-obyvatelstva-2020-2030_1_.pdf)

Národní úřad pro kybernetickou a informační bezpečnost - FAQ. Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka [online]. Dostupné z: <https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/#otazka4>.

NOYES, Katherine. Why Linux Is More Secure Than Windows. PCWorld [online]. San Francisco: IDG Communications, c2022 [cit. 2023-01-03]. Dostupné z: [https://www.pcworld.com/article/508291/why\\_linux\\_is\\_more\\_secure\\_than\\_windows.html](https://www.pcworld.com/article/508291/why_linux_is_more_secure_than_windows.html).

NUKIB, 2017. In: NUKIB: Zpráva o stavu kybernetické bezpečnosti za rok 2017 [online]. Praha [cit. 2023-02-06].

NÚKIB, 2020. Národní strategie kybernetické bezpečnosti České republiky na období let 2021-2025. In: NÚKIB [online]. Brno: NÚKIB [cit. 2023-2-20]. Dostupné z: [https://www.nukib.cz/download/publikace/strategie\\_akcni\\_plany/narodni\\_strategie\\_kb\\_2020-2025\\_%20cr.pdf](https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf).

NÚKIB, 2021, a. Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021-2025. In: NÚKIB [online]. Brno: NÚKIB [cit. 2023-1-21]. Dostupné z:

[https://www.nukib.cz/download/publikace/strategie\\_akcni\\_plany/akcni\\_plan\\_2021-2025.pdf](https://www.nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf).

NÚKIB, 2021, b. Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2023-1-20]. Dostupné z: <https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-akontrola/legislativa/>.

RAUTER, Thomas. Judicial Practice, Customary International Criminal Law and Nullum Crimen Sine Lege. Salzburg: Springer International Publishing, 2017, 260 s. ISBN 9783319644769.

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL, 2019. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o. ISBN 9788073807658.

SMEJKAL, Vladimír. Jaké povinnosti vyplývají pro orgány veřejné moci ze zákona o kybernetické bezpečnosti? - II. Právní Prostor [online]. 2015, [cit. 2023-03-17]. Dostupné z: <https://www.pravniprostor.cz/clanky/ostatni-pravo/jake-povinnosti-vyplyvaji-pro-organy-verejne-moci-ze-zakona-o-kyberneticke-bezpecnosti-ii.>

SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.

Správa sítě: Co je kyberterorismus? [online], 2016. Praha: Aira GROUP, s.r.o. [cit. 2023-02-13]. Dostupné z: <https://www.sprava-site.eu/kyberterorismus/>.

SQL vs. XXS Injection Attacks Explained, 2018. Keirstenbrager [online]. [cit. 2023-03-03]. Dostupné z: <https://www.keirstenbrager.tech/sql-vs-xxs-injection-attacks-explained/>.

Útoky hackerů na nemocnice sílí. Umírají kvůli nim lidé - Seznam Zprávy. [online]. Copyright © Seznam Zprávy, a.s. [cit. 05.04.2023]. Dostupné z: <https://www.seznamzpravy.cz/clanek/fakta-utoky-hackeru-na-nemocnice-sili-umiraji-kvuli-nim-lide-217153>.

Uživatel jako nejslabší článek — Stay Secure — Forbes speciál. Stay Secure — Forbes speciál [online]. Dostupné z: <https://staysecure2020.forbes.cz/uzivatel-jako-nejslabsi-clanek>.

V. T. En and V. Selvarajah, "Cross-Site Scripting (XSS)," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-5, doi: 10.1109/ICMNWC56175.2022.10031815.

What is Dumpster Diving in Cybersecurity?. Free DMARC Analyzer | DMARC Monitoring Service [online]. Copyright © PowerDMARC is a registered trademark. [cit. 25.04.2023]. Dostupné z: <https://powerdmarc.com/dumpster-diving-in-cybersecurity/>.

What is Password Cracking?. Purchase Intent Data for Enterprise Tech Sales and Marketing -TechTarget [online].Dostupné z: <https://www.techtarget.com/searchsecurity/definition/password-cracker>.

Worm vs. Virus: What's the Difference and Does It Matter?. Avast Academy [online]. Prague: Avast Software, c1988-2021 [cit. 2023-01-03]. Dostupné z: <https://www.avast.com/c-worm-vs-virus>.

ZAVRŠNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.

Zero-Day Vulnerability, 2014. K SOOD, Aditya a Richard ENBODY. Targeted Cyber Attacks [online]. Syngress [cit. 2023-03-03]. ISBN 978-0-12-800604-7. Dostupné z: <https://www.sciencedirect.com/topics/computer-science/zero-day-vulnerability>.

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

2FA	Two-Factor Authentication (Dvou-faktorové ověření)
CD	Compact Disk (kompaktní disk)
CIA	Confidentiality Integrity and Availability (důvěrnost, integrita a dostupnost)
DDoS	Distributed Denial-of-Service (distribuované odepření služeb)
DoS	Denial of service (odepření služeb)
ENISA	Evropská agentura pro bezpečnost sítí a informací
ESCO	Evropská iniciativa pro kybernetickou bezpečnost
HTTP	Hypertext Transfer Protocol (hypertextový internetový protokol)
HTTPS	Hypertext Transfer Protocol Secure ( zabezpečený hypertextový internetový protokol)
IAM	Identity and Access Management – Správa identity a přístupu
ICMP	Internet Control Message Protocol
ICT	Information and Comunication Technologies (Informační a komunikačních technologie)
IP	Internet Protocol (internetový protokol)
ISP	Internet Service Provider - Poskytovatel internetového připojení
LTP	Licensed Penetration Tester (licencovaný penetrační tester)
NATO	Severoatlantická aliance
NDA	Non-disclosure agreement (dohoda o mlčenlivosti)
NFC	Near Field Comunication
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OO	Ochrana obyvatelstva
PDR	Preliminary Design Review
RAID	Redundant Array of Independent Disks
RFID	Radio Frequency Identification
SAN	Storage Area Network

---

SET	The Social-Engineer Toolkit
SMTP	Simple Mail Transfer Protocol
SQL	Strukturovaný dotazovací jazyk
SSH	Secure Shell
URL	Unifor Resource Locator
USB	Universal Serial Bus
VIS	Významný informační systém
VPN	Virtual Private Network
XSS	Cross-site Scripting
ZoKB	Zákon o kybernetické bezpečnosti

**SEZNAM OBRÁZKŮ**

Obrázek 1: Edukační obrazovka na konci phishingové kampaně (zdroj: vlastní).....	46
Obrázek 2: První stupeň obtížnosti phishingových emailů (zdroj: vlastní).....	48
Obrázek 3: Druhý stupeň obtížnosti phishingových emailů (zdroj: vlastní) .....	49
Obrázek 4: Třetí stupeň obtížnosti phishingových emailů (zdroj: vlastní).....	50
Obrázek 5: Phishingový email z kampaně pro nováčky (zdroj: vlastní) .....	52
Obrázek 6: Stránka zobrazená po kliknutí na odkaz (zdroj: vlastní) .....	53
Obrázek 7: Nedůvěryhodná URL adresa (zdroj: vlastní) .....	54
Obrázek 8: Edukační obrazovka na konci phishingové kampaně pro nováčky (zdroj: vlastní) .....	55
Obrázek 9: Umístění nástroje SET (zdroj: vlastní).....	61
Obrázek 10: Menu možností nástroje SET (zdroj: vlastní) .....	62
Obrázek 11: Nabídka webových útoků (zdroj: vlastní) .....	62
Obrázek 12: Výběr konkrétních metod (zdroj: vlastní) .....	63
Obrázek 13: Zadání IP adresy (zdroj: vlastní) .....	63
Obrázek 14: Vložení URL adresy stránky k naklonování (zdroj: vlastní) .....	64
Obrázek 15: Zadání cílové stránky (zdroj: vlastní) .....	65
Obrázek 16: Srovnání originální (vlevo) a falešné stránky (vpravo) (zdroj: vlastní).....	65
Obrázek 17: Údaje zadané do přihlašovacího formuláře falešné stránky (zdroj: vlastní) ...	66
Obrázek 18: Návrh phishingového emailu cílící obecně na zaměstnance nemocnice (zdroj: vlastní) .....	68
Obrázek 19: Návrh spear phishingového emailu cílící na konkrétní osobu (zdroj: vlastní) .....	69
Obrázek 20: Model procesu phishingového útoku (zdroj: vlastní).....	71

## SEZNAM GRAFŮ

Graf 1: Reakce respondentů (zdroj: zkoumaná společnost) .....	56
---------------------------------------------------------------	----

