Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Aplikace vybraných metod sociálního inženýrství v praxi

Diplomová práce

Autor: Bc. Stanislav Růžička
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Zuzana Němcová, Ph.D.

Hradec Králové 2020

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 12.8.2020 Bc. Stanislav Růžička

Poděkování:

Děkuji vedoucí diplomové práce Ing. Zuzaně Němcové, Ph.D. za metodické vedení práce, pomoc a cenné rady.

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2018/2019

Studijní program: Aplikovaná informatika
Forma studia: Kombinovaná
Obor/kombinace: Aplikovaná informatika (ai2-k)

Podklad pro zadání DIPLOMOVÉ práce studenta

Jméno a příjmení:	**Bc. Stanislav Růžička**
Osobní číslo:	**I1700326**
Adresa:	Národní 1009, Prachatice – Prachatice II, 38301 Prachatice, Česká republika
Téma práce:	Aplikace vybraných metod sociálního inženýrství v praxi
Téma práce anglicky:	Application of selected methods of social engineering in practice
Vedoucí práce:	Ing. Zuzana Němcová, Ph.D. Katedra informačních technologií

Zásady pro vypracování:

Práce bude vypracována dle metodických pokynů FIM UHK.
Cíl:
Cílem práce je prozkoumat problematiku sociálního inženýrství a aplikovat vybrané metody k testování zaměstnanců. Na základě analýzy výsledků navrhnout opatření pro zvýšení zabezpečení pracoviště.

Osnova:
1. Úvod
2. Sociální inženýrství
3. Metody sociálního inženýrství
4. Aplikace vybraných metod
5. Závěr a návrh opatření pro zvýšení zabezpečení pracoviště
6. Seznam použité literatury

Seznam doporučené literatury:

JAMES, Lance. *Phishing bez zábav*. Praha: Grada, 2007, 281 s. ISBN 978-80-247-1766-1
JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2
Kevin Mitnick, William L. Simon. The Art of Deception: Controlling the Human Element of Security (2003)
Kevin Mitnick a William SIMON, 2003. Umění klamu. B.m.: Helion S.A. ISBN 83-7361-210-6.

Podpis studenta: Datum:

Podpis vedoucího práce: Datum:

Anotace

Sociální inženýrství je téma, které se často stává předmětem mnoha diskuzí z důvodu snahy o zdokonalení zabezpečení informačních systémů. Jedná se o souhrn různých metod a prostředků k získání citlivých informací. Útoky prostřednictvím sociálního inženýrství představují bezpečnostní hrozbu, která spočívá v klamání. Zaměřují se na nejslabší článek zabezpečení v rámci každého informačního systému. Tímto nejslabším článkem daného systému je samotný uživatel.

V diplomové práci je definován pojem sociální inženýrství. Po seznámení s problematikou sociálního inženýrství následuje popis historie, legislativy, forem a cyklu útoku. Dále jsou detailně popsány metody útoku sociálního inženýrství a poté vybrané metody aplikovány k testování zaměstnanců městského úřadu. Závěr představuje návrhy bezpečnostních opatření, které by mohly v budoucnu zabránit útokům sociálního inženýrství nebo alespoň zmírnit jejich dopady.

Annotation

Title: Application of selected methods of social engineering in practice

Social engineering is a topic that is often discussed in order to improve security of information systems. There are various methods available to obtain sensitive information. Attacks through social engineering post a threat, counting in deception. It focuses on the weakest link in security within any information system. This weakest part in the system is the user himself.

Thesis defines the concept of social engineering. After getting acquainted with issues of social engineering, a description of the history, legislation and the cycle of attack follows. The next part precisely describes selected methods of attacks of social engineering, some of these methods are applied to test municipal employees. The end of thesis provides solution for security measures that could prevent from social engeering attacks or at least mitigate the impact of social engeering attacks.

Obsah

1. Úvod 1

2. Cíl práce 3

3. Sociální inženýrství 4

3.1. Historie 6

3.2. Terminologie 8

3.3. Formy útoků sociálního inženýrství 9

3.3.1. Komunikace přes e-mail 15

3.3.2. Komunikace přes sociální sítě 16

3.3.3. Neurolingvistické programování 16

3.4. Cyklus útoku sociálního inženýrství 17

3.4.1. Průzkum volných zdrojů informací 17

3.4.2. Budování vztahů a důvěry 18

3.4.3. Využití důvěry 18

3.4.4. Využití informace 19

3.5. Právní úprava v oblasti sociálního inženýrství 20

4. Metody sociálního inženýrství 25

4.1. Vishing 25

4.2. Phishing 26

4.3. Pharming 28

4.4. Baiting 30

4.5. Smishing 32

4.6. Trashing 34

4.7. Tailgating 35

4.8. Quid Pro Quo 35
4.9. Pretexting 36
5. Aplikace vybraných metod 47
5.1. Metoda phishing 47
5.2. Metoda baiting 51
5.3. Metoda pretexting 53
5.4. Metoda vishing 53
5.5. Metoda smishing 54
5.6. Metoda trashing 54
6. Dotazník na téma Sociální inženýrství 57
7. Návrh opatření pro zvýšení zabezpečení pracoviště 72
8. Závěr 79
9. Seznam použité literatury 81
Seznam obrázků 85
Seznam grafů 86
Seznam tabulek 86

1. Úvod

V současné době společnost stále více využívá informační technologie k usnadnění svého života. Za posledních několik let došlo k rychlému vývoji informačních a telekomunikačních technologií. Zmíněné technologie mohou pomoci například v osobním životě, při výkonu práce, ale také mohou posloužit jako určitý typ zábavy. Vzhledem k jednodušší dostupnosti a ceně si technologie dnes může pořídit téměř každá domácnost. Vývoj technologií bohužel představuje i negativní dopad. Dochází k růstu kybernetické kriminality. Rostoucí množství útoků má na svědomí mnohačetné škody nejen pro jednotlivce, ale i organizace.

Sociální inženýrství je téma, které se často stává předmětem mnoha diskuzí z důvodu snahy o zdokonalení zabezpečení informačních systémů. Jedná se o souhrn různých metod a prostředků k získání citlivých informací. Útoky prostřednictvím sociálního inženýrství představují bezpečnostní hrozbu, která spočívá v klamání. Útoky se zaměřují na nejslabší článek zabezpečení v rámci každého informačního systému. Nejslabším článkem daného systému je samotný uživatel. Útoky mohou být úspěšné díky porušení zásad zabezpečení. Bývají využity psychologické triky, díky nimž se stává útok obtížně rozpoznatelný a nelze se proti němu bránit. Útok sociálního inženýrství může mít fatální dopad. Následky mohou být likvidační vzhledem k tomu, že škody mohou představovat velkou finanční ztrátu.

Podle posledních provedených průzkumů vychází tvrzení, že dnešní antivirové programy a firewall jsou schopny dosáhnout takové kvalitní ochrany, že selhání je možné pouze u lidského faktoru. Z tohoto hlediska vyplývá, že nejjednodušším způsobem, jak získat chtěné citlivé informace, je si o ně rovnou říci.

V současné době lze útočníky označit za čím dál více vynalézavější a jejich útoky za promyšlenější a propracovanější. Z tohoto důvodu bychom si všichni měli dobře chránit své osobní údaje a být ostražití před těmito útoky. Přestože organizace investují své prostředky do nejlepších a nejdražších bezpečnostních technologií,

tato opatření nepředstavují stoprocentní ochranu a organizace budou stále zranitelné.

Ke zmírnění rizika provedení útoku sociálního inženýrství může také posloužit například školení zaměstnanců, nastolení vhodné bezpečnostní politiky nebo penetrační testování. Bezpečnostní opatření mohou představovat různá úskalí. Jestliže jsou bezpečnostní opatření zavedena neadekvátním způsobem, může to mít negativní dopad na výkon zaměstnanců a efektivnost organizace.

2. Cíl práce

Vzhledem k tomu, že nelze přesně stanovit mez, kdy se jedná o podvod a kdy o sociální inženýrství, cílem diplomové práce je prozkoumat problematiku sociálního inženýrství a aplikovat vybrané metody k testování zaměstnanců městského úřadu. Na základě analýzy výsledků budou navržena vhodná opatření pro zvýšení zabezpečení pracoviště.

Teoretická část je zaměřena na problematiku sociálního inženýrství. Definuje základní pojmy a popisuje historii, v níž jsou představeny nejznámější osobnosti spojené se sociálním inženýrstvím. Také se teoretická část zaměřuje na právní úpravu, která s touto problematikou úzce souvisí. Dále je popis možných forem útoku a cyklu útoku, který detailně popisuje získání citlivých informací. V neposlední řadě teoretická část popisuje metody sociálního inženýrství.

Praktická část se skládá ze dvou částí. První část představuje aplikaci vybraných metod sociálního inženýrství. Pro aplikaci byla vybrána organizace, kterou byl městský úřad. Cílem aplikace je zjistit, zda jsou zaměstnanci schopni odhalit možný útok sociálního inženýrství. Vzhledem k tomu, že si úřad nepřál být jmenován, je v diplomové práci využit pouze obecný název bez nutnosti fiktivního pojmenování. Druhá část zahrnuje dotazníkové šetření, jehož cílem je zjistit, zda zaměstnanci znají pojmy sociálního inženýrství. Dále je cílem porovnat výsledky dotazníkového šetření s výsledky metod aplikovaných na zaměstnance.

Závěr práce představuje návrhy opatření, které by mohly v budoucnu zabránit útokům sociálního inženýrství nebo alespoň zmírnit jejich dopady. S těmito útoky se mohou zaměstnanci setkat během každého pracovního dne.

3. Sociální inženýrství

Sociální inženýrství představuje souhrn metod a prostředků pro manipulaci s lidmi. Používá se za účelem získání důvěrných informací. Základním předpokladem pro získání informací je obvykle zneužití důvěry a nevědomosti oběti. Sociální inženýrství je díky médiím spojováno s kriminalitou v kybernetickém prostoru. Lidé si často pod tímto pojmem představují například lhaní, skrývání totožnosti nebo zmizení peněz z bankovních účtů. (WHAT IS SOCIAL ENGINEERING? EXAMPLES AND PREVENTION, 2019)

(HADNAGY, 2018) vysvětluje sociální inženýrství jako jednání, které vede člověka k jisté akci. Ta může být v jeho nejlepším zájmu, ale nemusí. Nevidí v sociálním inženýrství pouze negativum. Tvrdí, že se s ním lidé setkávají každý den na kterémkoliv místě. Příkladem mohou být rodiny s dětmi, kdy rodiče přesvědčují své děti, aby plnily jejich příkazy. Také při léčbě pacienta, kdy lékař potřebuje k určení diagnózy důležité informace. Zmíněné příklady jsou si podobné, ale přitom se výrazně odlišují ve výsledcích.

Podle (JIROVSKÝ, 2007): *„Existuje mnoho definic sociálního inženýrství, které jsou si více či méně podobné. Sociální inženýrství označováno za „umění, jak přimět ostatní lidi, aby splnili Vaše přání“ nebo za „psychologické triky hrané na oprávněné uživatele systému za účelem získání přístupu do tohoto systému“ apod. Obecně se však jedná o zneužití nejslabšího článku, o chytrou a promyšlenou manipulaci přirozené důvěřivosti člověka.“*

(MITNICK A SIMON, 2003) definují sociální inženýrství jako umění sociotechniky, které je založeno na psychologii a pokročilých počítačových znalostech. Spočívá v podvodné manipulaci, kdy se sociotechnik zaměřuje na méně zkušené nebo nezkušené uživatele. Cílem je vybudovat v člověku dojem, že situace je jiná, než skutečně je.

Sociální inženýrství nepředstavuje pouze záměr k podvodným účelům. Lidé se s ním běžně setkávají, aniž by si toho byli vědomi. Osoby, které využívají sociální inženýrství lze zařadit do následujících kategorií:

Hackeři

Snahou hackerů je prolomení již vybudovaných zabezpečení, například firemní počítačové sítě. Vzhledem k neustálému zlepšování a zdokonalování zabezpečení představují největší slabinu samotní uživatelé počítačových systémů. Z tohoto důvodu hackeři častěji využívají metody sociálního inženýrství.

Penetrační testeři

Penetrační testeři vylepšují stav zabezpečení prostřednictvím metod sociálního inženýrství. Informace, které získají, v tomto případě neslouží k jejich zneužití. Cílem je například testování zabezpečení firmy nebo hledání silných a slabých stránek v zabezpečení.

Špioni

Špioni využívají k aplikaci sociálního inženýrství i jiné dovednosti. Neustále se učí a zdokonalují své znalosti ve způsobu klamání lidí. Vzhledem k tomu, že si špioni zjišťují o oběti více informací, působí důvěryhodným dojmem.

Zloději identity

Zloději identity získávají citlivé informace (jméno, datum narození, adresu bydliště) odesíláním podvodného e-mailu oběti. V tomto případě oběť nemá o úniku informací nejmenší tušení.

Nespokojení zaměstnanci

Nespokojení zaměstnanci představují pro své zaměstnavatele určité riziko. Svou nespokojenost mohou dát najevo například smazáním důležitých dokumentů nebo vynášením informací mimo firmu. Mezi nespokojené zaměstnance patří převážně lidé, se kterými byla ukončena pracovní smlouva.

Výkonní náboráři

Výkonní náboráři musí umět nejen nalákat lidi, ale také je motivovat. Většinou se jedná o nábor na pozice v top managementu.

Prodejci

Existuje tvrzení, že dobrý prodejce se nesnaží zákazníky ovlivňovat ani manipulovat s nimi. Svých schopností využívá pouze ke zjištění, jaké jsou jejich potřeby. Cílem je uspokojit přání těchto zákazníků.

Sociální inženýrství využívají i lékaři, psychologové nebo právníci. (HADNAGY A EKMAN, 2014)

3.1. Historie

Umění manipulovat s lidmi a přelstít je existuje odjakživa. Pokaždé se objevil jedinec, který dokázal svou vychytralost využít ve svůj prospěch. Jedním z nich byl Viktor Lustig, který byl původem z Čech. Lustig byl velice inteligentní muž, mluvil pěti jazyky. Jako mladý se naučil mnoho karetních triků. V pozdějším věku propadl hazardním hrám. Lustig se proslavil díky prodeji Eiffelovy věže. Rozhodl se ji prodat v okamžiku, kdy se v novinách dočetl o problému s opravou věže. Domluvil schůzku se šesti obchodníky, kteří se zabývali likvidací kovového odpadu. Oznámil jim, že má na starost likvidaci věže, protože její údržba je příliš nákladná. Prodej věže se Lustigovi vydařil, inkasoval peníze za prodej včetně úplatku od jednoho obchodníka. Po čase se znovu pokusil o prodej věže, tentokrát byl ale neúspěšný. Lustig se pohyboval na hraně zákona do té doby, než byl odsouzen na patnáct let do vězení Alcatraz. Jeho život skončil po jedenácti letech za mřížemi, kde zemřel na zápal plic. (THE MAN WHO SOLD THE EIFFEL TOWER, 2019)

Dalším mužem, který proslavil sociální inženýrství, byl Kevin Mitnick (obrázek 1). Mitnick se narodil 6. října 1963 v San Fernando Valley, které se nachází v severozápadní části města Los Angeles. Od narození žil pouze se svojí matkou, neměl žádného sourozence. V dětství Mitnicka fascinovaly kouzelnické triky. Na základní škole se mu podařilo po několika rozhovorech s řidičem cestovat zadarmo autobusem. Když pochopil způsob tisku jízdenek, sehnal si děrovací strojek. Na střední škole se Mitnick poprvé setkal se sociotechnikou, kterou mu ukázal kamarád. Předvedl mu, jak se dostat do telefonních sítí. Postupem času se z Mitnicka stal nejobávanější hacker, který byl schopen dostat se do počítačových systémů největších obchodních společností. Často čelil obvinění ve věcech, které nespáchal

a byl několikrát přinucen se zříci svých práv. V době, kdy Mitnick dosáhl nejvyššího vrcholu, se stal nejhledanější osobou FBI. Byl několikrát odsouzen a uvězněn, přitom tvrdil, že získaná data nikdy nezničil a ani se na nich neobohatil. Dělal to jen proto, aby sám sobě dokázal, že je něčeho takového schopen. Během šesti let, které strávil ve vězení, měl přísně zakázáno používat počítač a telefon. Rozsudek soudu zněl: „Vyzbrojen klávesnicí je nebezpečím pro společnost.“ Pojmem hacker byli dříve nazýváni lidé, kteří se pokoušeli experimentovat s počítači a programy, vymýšleli efektivnější řešení problémů. V dnešní době jsou tito lidé označováni za zločince. Mitnick rozlišoval, kdo je podvodník a kdo sociotechnik. Podle něj byl podvodník ten, kdo lákal z lidí peníze. Ten, kdo z lidí lákal informace, byl sociotechnik. V roce 2002 Mitnick vydal svou první knihu „Umění klamu“. Při příležitosti uvedení knihy do českého knihkupectví navštívil v roce 2003 Českou republiku.

Obrázek 1: Kevin Mitnick
Zdroj: KEVIN MITNICK NET WORTH, 2020

V současnosti je Kevin Mitnick považován za specialistu v oblasti bezpečnosti počítačových systémů. Zabývá se bezpečností jak u firem, tak u soukromých osob.

„Má činnost byla způsobena zvědavostí – toužil jsem znát všechno, co se dalo, o tom, jak fungují telefonní sítě a vstupy a výstupy počítačových bezpečnostních systémů. Z dítěte fascinovaného kouzelnickými kousky jsem se stal nejhroznějším hackerem na světě, kterého se obává vláda i korporace. Když se probírám vzpomínkami posledních třiceti let mého života, musím přiznat, že jsem vedený zvědavostí, touhou po poznání technologií a uspokojováním intelektuálních výzev, učinil jsem několik velmi špatných rozhodnutí. Změnil jsem se. Dnes využívám svůj talent a své znalosti o bezpečnosti informací a sociotechnice, které se mi podařilo osvojit, abych pomáhal vládě, firmám i soukromým osobám při odhalování, prevenci a reagování na ohrožení bezpečnosti informací.“

Kevin Mitnick

3.2. Terminologie

Terminologie je nedílnou součástí sociálního inženýrství. Existuje několik základních pojmů, se kterými se lze v oblasti sociálního inženýrství setkat.

Cílený rozhovor

Cílený rozhovor představuje takový rozhovor, jehož cílem je zjistit nějakou konkrétní informaci. K úspěšnému zvládnutí cíleného rozhovoru jsou zapotřebí v určité míře verbální i neverbální zkušenosti použité v praxi. Za cílený rozhovor lze považovat například pohovor.

Zájmová osoba

Za zájmovou osobu se považuje osoba, která je předmětem zájmu. Například to může být osoba, která je podezřelá ze spáchání trestné činnosti. Může to být i osoba, jejíž postavení disponuje informacemi a je předmětem zájmu.

Vytěžování osob

Vytěžování osob je metoda, která se používá při detektivní činnosti. Jejím cílem je získat potřebné informace. Pro tuto metodu je nezbytně nutná schopnost

komunikovat a přizpůsobit se určité situaci. Protože se komunikace nikdy nevyvíjí podle očekávání, je nutné umět improvizovat. Rozdíl mezi metodou vytěžování osob a cíleným rozhovorem spočívá v navázání kontaktu a správném směrování rozhovoru k získání informací. Dále se liší délkou zjišťování informací o konkrétním jedinci. Metoda vytěžování osob může být vedena prostřednictvím předem vytvořených otázek.

Senzitivní informace

Obecně se informace definuje jako jednotné ucelené sdělení. To může mít písemnou nebo ústní podobu. Senzitivní informace je citlivá informace, která si žádá ochranu. Při jejím neoprávněném použití nebo zveřejnění může dojít ke způsobení škody. Škoda může vzniknout osobě nebo instituci, kterých se citlivá informace týká. Za senzitivní informaci lze považovat například osobní údaje nebo ekonomické údaje. (BRABEC, 2009)

3.3. Formy útoků sociálního inženýrství

Existuje několik forem útoků sociálního inženýrství. Mezi jednu z forem patří kontaktní sociální inženýrství, na které se obvykle zapomíná. Pro správné využití formy útoku je základním předpokladem znalost lidského chování a jeho vhodné použití. Velmi důležitá je i neverbální komunikace, která úzce souvisí s některými metodami sociálního inženýrství. Neverbální komunikaci je možné využít různými způsoby. Nejčastěji bývá využívána při čtení myšlenek ostatních lidí. Sociální inženýrství, které s neverbální komunikací úzce souvisí, umožnuje lidem vnutit pravdu, která nemusí být pravdou nebo umožnuje přinutit lidi, aby dělali to, co se od nich žádá. Neverbální komunikace umožnuje odhadnout reakci lidí, s využitím sociálního inženýrství je možné lidi ovlivnit tak, aby byli důvěřiví.

Neverbální komunikace

Představuje fyzická gesta beze slov, která lidé používají při komunikaci s lidmi. Mezi gesta patří například způsob, jak lidé sedí, mluví, navazují oční kontakt nebo jakou udržují vzdálenost od druhé osoby. Často dochází k tomu, že to, co lidé říkají,

neodpovídá reakci jejich těla. Jedná se o dvě odlišné věci. V tomto případě tedy záleží na každém jedinci, zda bude věřit mluvenému projevu nebo neverbální komunikaci.

- **Projevy neverbální komunikace**

Jak už bylo řečeno, neverbální komunikace se projevuje takovými fyzickými gesty, která nelze snadno skrývat. Existuje několik podob fyzických gest, která každého člověka určitým způsobem ovlivňují a jsou pro něj důležité.

Haptika je komunikace dotykem. Sdělení se realizuje prostřednictvím fyzického kontaktu. Takové sdělení bývá využíváno v řadě případů, například při náznaku přátelství, ale i nadvlády nad člověkem.

Kinezika představuje komunikaci skrze pohyb těla. Zahrnuje nejen jak se lidé pohybují, ale i jaká gesta používají při mluveném projevu. Existuje několik druhů interpretace řeči těla. Tyto druhy mohou být od sebe odlišné například na základě pohlaví nebo příslušné kultury.

Znaky jsou fyzická gesta, jejichž význam může spočívat v překladu slov. Například souhlas (obrázek 2) může být vyjádřen zdviženým palcem. Naopak nesouhlas lze vyjádřit palcem dolů. Pro nás typická fyzická gesta mohou v jiné kultuře představovat vulgarismy nebo mohou mít zcela jiný význam.

Obrázek 2: OK
Zdroj: HADNAGY A EKMAN, 2014

Ilustrátory jsou pohyby, které doprovází neverbální komunikaci. Pomáhají lidem usnadnit jejich vyjadřování. Je prokázáno, že se lidé díky pomoci svých rukou vyjadřují ve svém projevu snáze. Během projevu ilustrátory slouží například ke zdůraznění klíčového slova nebo přiblížení velikosti popisovaného objektu. Také mohou být ilustrátory využity ve snaze o zájem a pozornost při projevu. Ilustrátory jsou jednoduše čitelné. Existují typické pohyby, které člověk neovlivní, například ruce v pěst nebo překřížené ruce. Ruce v pěst mohou představovat obranu, případně útok. Překřížení rukou vyjadřuje nezájem nebo nesouhlas.

Projevy emocí vychází z neverbálních projevů těla a obličeje. Představují rozpoložení, ve kterém se lidé nachází. Typickým příkladem projevu těla může být výskok při chůzi. U takového gesta lze předpokládat, že je člověk šťastný. Naopak pomalá chůze, při které má člověk hlavu skloněnou dolů, může být projevem nešťastného člověka. U projevu obličeje lze považovat člověka, který se usmívá, za šťastného. Naopak člověka, který se mračí, lze označit za nešťastného. Projevy emocí u lidí bývají často spontánní a nelze je nijak ovlivnit.

Regulátory jsou doprovodem řeči. Při projevu mohou řídit, regulovat nebo napomáhat tomu, co se snaží člověk sdělit. Jako příklad lze uvést řečníka, který při ukončení projevu svěsí ruce dolů nebo může pokynutím ruky předat slovo kolegovi.

Adaptory představují projevy neverbální komunikace, které většina lidí nevnímá. Mezi typické adaptory patří prohrabávání vlasů, škrábání, upravování brýlí nebo cvakání psací potřebou. Jestliže se člověk cítí provinile, obvykle si rukama zakrývá oči a klopí hlavu dolů. Pokud trpí nějakými bolestmi, přikládá ruku na bolestivé místo. Díky těmto projevům lze snadno rozpoznat, jak se člověk v daný okamžik cítí.

Emoce bývají často označovány jako pocity. Zahrnují zážitky, které jsou spjaty s radostí, láskou, smutkem, strachem, nenávistí, zlostí, důvěrou nebo panikou. Představují určité reakce na různé události a jejich trvání je krátkodobé. Veškeré emoce jsou založené na subjektivních pocitech. Ty se dále projevují fyziologickými reakcemi. (HADNAGY A EKMAN, 2014)

Projevy emocí se sociálním inženýrstvím úzce souvisí. Útočníci často využívají k realizaci útoku emoce. Díky využití emocí se útočníci snaží vyvolat v oběti pocity,

aby se jim podařilo získat požadované informace. Útočníci dokáží v oběti vyvolat emoce i prostřednictvím telefonního rozhovoru.

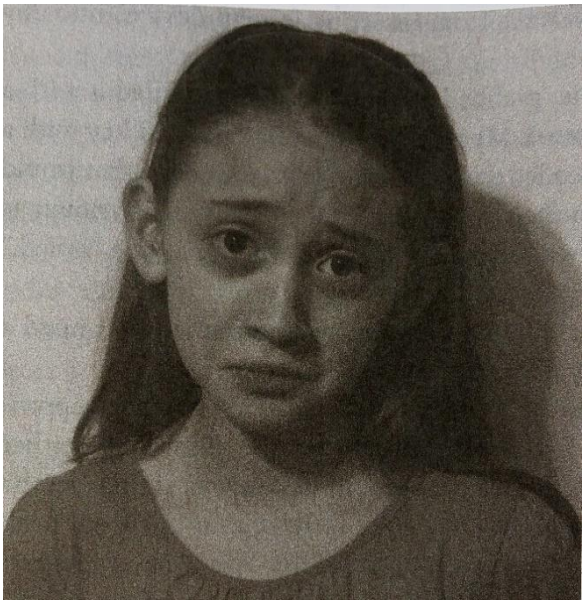
Podle (EKMAN A FRIESEN, 2015) existuje šest základních skupin emocí: radost, smutek, strach, překvapení, hněv, znechucení.

Radost je pozitivní emoce, kterou člověk cítí při prožívání příjemných událostí. Patří mezi základní emoce, které lze snadno rozpoznat. Radost se může stupňovat a nabývat na intenzitě. Vždy ji doprovází úsměv, který také může nabývat na intenzitě a v některých případech mohou radostí téct i slzy z očí.

Radost (obrázek 3) patří mezi emoce, která bývá používána k zakrývání jiné emoce. Také ji lze kombinovat s jinou emocí, například se strachem nebo překvapením. Typickým výrazem kombinace radosti a překvapení je úsměv a vykulené oči.

Obrázek 3: radost
Zdroj: HADNAGY A EKMAN, 2014

Smutek (obrázek 4) je negativní emoce, která se projevuje úzkostí. Příčina smutku spočívá v předešlém utrpení nebo ztrátě. Smutný může být člověk kvůli čemukoliv, nejčastěji však bývá při ztrátě blízkého člověka, promrhání životní šance nebo neopětované lásce. Jedná se o dlouhodobou emoci, která může mít tichou nebo hlasitou podobu. Hlasitá podoba je doprovázena pláčem. Součástí emoce bývají často výčitky nebo demotivace. Smutek lze kombinovat se strachem a hněvem.



Obrázek 4: smutek
Zdroj: HADNAGY A EKMAN, 2014

Hněv představuje emoci, která je přirozená a nelze ji snadno skrývat. Jedná se o jednu z nejintenzivnějších emocí. Může se stupňovat a nabírat na intenzitě. Příčinou hněvu může být nespravedlnost, kritika, výhružky nebo nebezpečí. Mezi mírné projevy hněvu patří například nelibost, podráždění nebo odpor. Existuje velké množství spouštěčů hněvu, které mohou být u každého člověka odlišné. Výraz v obličeji však mají všichni hněvající se lidé stejný.

Překvapení (obrázek 5) je označováno za nejkratší emoci, která je náhlá jak při jejím nástupu, tak i odezvě. Tuto emoci lze velice těžko oklamat. Jestliže má člověk prostor na posouzení, zda překvapený je nebo není, pak překvapený není. Skutečné překvapení má stejně rychlou odezvu jako její nástup. Za předpokladu, že je to nečekané, může být překvapením téměř vše. Vzhledem ke krátkému trvání překvapení přichází většinou další emoce. Jestliže se jedná o nemilé překvapení, může poté nastoupit smutek. Pokud jde o milé překvapení, může nastoupit radost.

Obrázek 5: překvapení
Zdroj: HADNAGY A EKMAN, 2014

Strach (obrázek 6) je definován jako nepříjemná a často velmi silná emoce. Bývá vyvolán očekáváním nějakého nebezpečí, které doprovází individuální psychický a fyzický projev. Může mít různou intenzitu. Ta závisí na předchozích zkušenostech nebo vyhodnocení konkrétní situace. Strach se často plete s překvapením. Tyto dvě emoce se od sebe odlišují emocionálním stavem, který doprovází typické fyziologické příznaky.

Obrázek 6: strach
Zdroj: HADNAGY A EKMAN, 2014

Znechucení je emoce, která bývá označována jako averze a vyvolává pocit opovržení či nevolnosti. Jestliže člověk cítí odpor, dostaví se silný vnitřní impuls vedoucí k vyhnutí se věci nebo situaci, která v člověku tento pocit vyvolala. Dále mohou vyvolat pocit znechucení například odpadky, nepříjemné pachy nebo neznámé chutě. Znechucení je ve srovnání s hněvem považováno za mírný emoční projev. (HADNAGY A EKMAN, 2014)

Další formou je sociální inženýrství bez fyzického kontaktu. S touto formou lze přijít do styku přes internet. Princip spočívá ve využití znalostí a zkušeností útočníka, díky kterým je útočník schopen dostat informace, které potřebuje. V současnosti je nejčastěji využívána komunikace přes sociální sítě. Lidé si mezi sebou sdělují prostřednictvím chatu důvěrné informace, a přitom zapomínají na možnost rizika zneužití informací.

Současná doba nám umožňuje vystupovat v anonymitě díky stále více využívané výpočetní technice. Osobní kontakt není považován za důležitý. (MITNICK A SIMON, 2003)

3.3.1. Komunikace přes e-mail

E-mail byl odjakživa terčem mnoha útoků. Představoval pro útočníky jednoduchý způsob, jak se nabourat do účtu oběti. Využitím techniky sociálního inženýrství jsou útočníci schopni zjistit přístupové údaje k e-mailu oběti. K údajům se mohou dostat i pomocí sofistikovaného softwaru neboli počítačového viru, který funguje na principu zaznamenávání každého úderu na klávesnici a jeho následného odeslání útočníkovi. Další možnou technikou, kterou se mohou pokusit uhádnout přístupové údaje, je útok hrubou silou (anglicky brute force attack). Útočník si může vytvořit program, který náhodně generuje přihlašovací údaje nebo může použít předem vytvořený seznam údajů, který je dostupný na internetu. Jestliže útočník pronikne do e-mailového účtu, může využít seznam kontaktů oběti a rozeslat jim podvodné e-maily, díky kterým získá důvěrné informace. Podvodné e-maily mohou mít různou podobu. E-mail může obsahovat odkaz na fiktivní stránku, která může být infikovaná. Dále mohou být obsahem e-mailu infikované přílohy. (SOCIAL ENGINEERING TECHNIQUES: 4 WAYS CRIMINAL OUTSIDERS GET INSIDE, 2019)

3.3.2. Komunikace přes sociální sítě

Sociální sítě představují nejjednodušší způsob, jak komunikovat mezi sebou. Umožňují sdílet například soukromé informace, fotografie, videa nebo i polohu, kde se momentálně nacházíme. Komunikace přes sociální sítě přináší i jistá rizika. Sdílené informace mohou být zneužity útočníkem. K tomu dochází, pokud má uživatel na sociální síti špatně nastavené soukromí, respektive kdo může vidět obsah jeho profilu. Díky tomu může být profil uživatele viditelný pro všechny uživatele sociální sítě a kdokoliv tak má možnost dostat se k informacím, které majitel účtu zveřejnil.

Vzhledem k tomu, že se sociální sítě řadí mezi nejrozsáhlejší a nejčastěji používané komunikační prostředky, představují pro uživatele velkou hrozbu ze strany útočníků. Jestliže se podaří útočníkovi nabourat do cizího účtu, může například ohrozit přátele oběti tím, že jim pošle odkaz na fiktivní internetovou stránku, která bude obsahovat malware. Pokud oběť na odkaz klikne, automaticky do počítače malware stáhne, aniž by o tom věděla. Díky tomu dostane útočník přístup do počítače oběti. Nebo může ke zprávě přidat infikovaný soubor a tím může dostat přítele oběti do problémů. (SOCIAL ENGINEERING TECHNIQUES: 4 WAYS CRIMINAL OUTSIDERS GET INSIDE, 2019)

3.3.3. Neurolingvistické programování

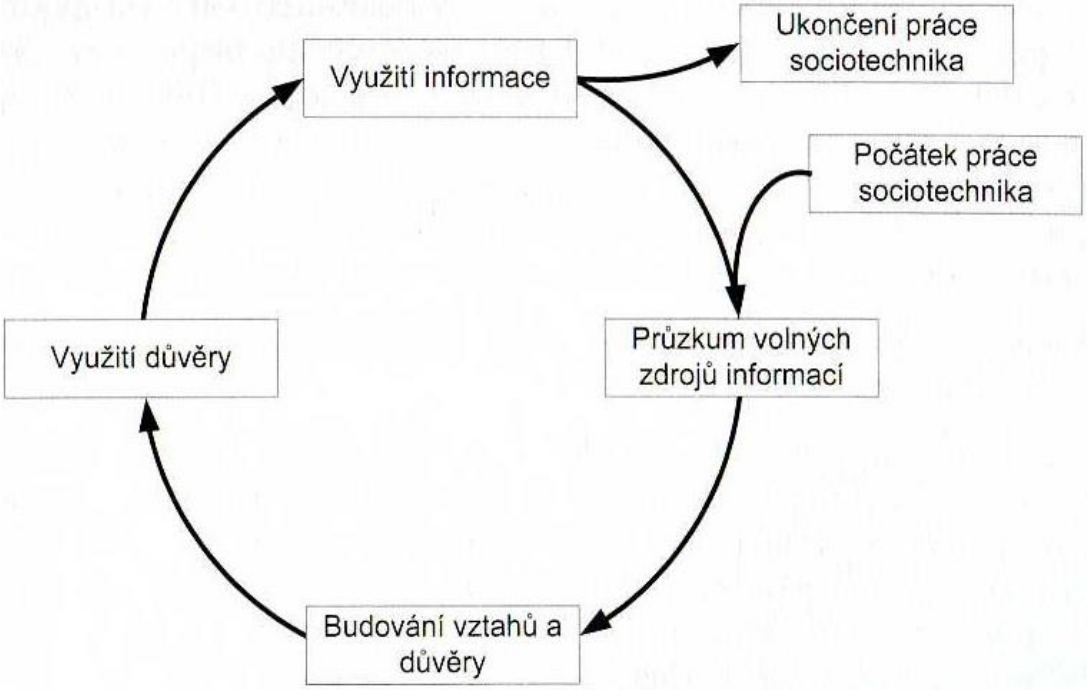
Neurolingvistické programování spočívá v přizpůsobování se konkrétnímu chování oběti, od které se snažíme získat důvěrné informace. Lze se dostat do podvědomí oběti, aniž by si to uvědomila.

Předpokladem úspěchu neurolingvistického programování je určitá míra všímavosti, empatie a sociálního vnímání. Opírá se o procesy, které podvědomě vykonává každý jedinec. Jedná se například o styl vyjadřování nebo o osvojené zvyky. Pro velký úspěch a účinnost se metoda rozrostla do více různých odvětví. Dnes je využívána manažery, policisty, vojáky, obchodníky i přes to, že použití metody v praxi je obtížné vzhledem k velkému množství faktorů, které je potřeba sledovat. (TOP 10 SOCIAL ENGINEERING TACTICS, 2019)

3.4. Cyklus útoku sociálního inženýrství

Cyklus útoku sociálního inženýrství se skládá z předem naplánovaného scénáře akcí, které musí sociotechnik postupně projít, aby získal potřebné informace. Je tvořen ze čtyř následujících kroků (obrázek 7):

1. Průzkum volných zdrojů informací
2. Budování vztahů a důvěry
3. Využití důvěry
4. Využití informace



Obrázek 7: Cyklus útoku sociálního inženýrství

Zdroj: JIROVSKÝ, 2007

3.4.1. Průzkum volných zdrojů informací

Průzkum volných zdrojů informací představuje pro sociotechnika začátek celého cyklu. Spočívá v hledání informací, které jsou volně dostupné. Informace se mohou využít i v dalších krocích. Jedná se o volné zdroje, jejichž obsah nemá pro majitele obvykle žádný význam. Nepovažují informace za důležité, a proto dochází k jejich

volnému šíření bez jakéhokoliv zabezpečení. Mezi volné zdroje informací patří například webové stránky firem. Útočník se zaměřuje především na hledání struktury firmy, jmen zaměstnanců a případná volná pracovní místa. (JIROVSKÝ, 2007)

3.4.2. Budování vztahů a důvěry

V této fázi cyklu je nutné zvážit všechny možné situace, které mohou nastat. Je třeba si dopředu připravit seznam otázek. Sociotechnik si je plně vědom, že jeho práce je časově náročná a že nesmí před svou obětí vyvolat podezření, že se jedná o podvod. Z tohoto důvodu probíhá komunikace obvykle vícekrát. Většinou první komunikace směřuje k tématu každodenních běžných věcí.

Strategie komunikace se dělí do třech základních přístupů (JIROVSKÝ, 2007):

- **Oficiální komunikační strategie** – Nepřipouští se familiární tón. Komunikace probíhá působivě a seriózně. Sociotechnik nezná osobní údaje cílové osoby. Klíč úspěchu spočívá v zachování profesionality.
- **Familiární komunikační strategie** – Je nutné znát některé osobní údaje a rysy cílové osoby. V komunikaci se používají žertovné nebo flirtující fráze. Strategie vyžaduje orientaci v prostředí cílové osoby. Je dobré mít určité herecké vlohy.
- **Úzce osobní komunikační strategie** – Princip spočívá ve vyvolání přesvědčení u cílové osoby, že se znají déle. Komunikace vyžaduje znalost detailních informací o cílové osobě. Strategie patří mezi nejsložitější. Hrozí odhalení při neznalosti několika detailů nebo minimální přesvědčivosti.

3.4.3. Využití důvěry

Jakmile sociotechnik naváže s cílovou osobou vřelé vztahy a vyvolá v ní pocit důvěry, přichází okamžik, kdy ji požádá o potřebné informace. Z důvodu opatrnosti, aby cílová osoba nenabyla jakéhokoliv podezření, nepadá otázka na potřebnou informaci v úvodu komunikace. Většinou začíná komunikace v přátelském duchu a nezávazně.

Ke zjištění, zda je cílová osoba ochotna poskytnout citlivé informace, bude položen osobní dotaz. Pokud znejistí a nechce odpovědět, může to znamenat varovný signál neúspěchu sociotechnika.

Po položení dotazu a získání citlivé informace sociotechnik pokračuje v komunikaci. Vede s cílovou osobou další nezávaznou komunikaci, aby odvedl pozornost od vyzrazené informace.

3.4.4. Využití informace

Využití informace je konečnou fází cyklu. Pokud jsou získané informace úplné, není potřeba zjišťovat další informace. Jestliže máme k dispozici část potřebných informací, je nutné celý cyklus sociálního inženýrství zopakovat. Informace lze využít pro jednodušší budování důvěry.

Existuje šest základních lidských vlastností, které přispívají ke zvýšení efektivnosti útoků. Mezi lidské vlastnosti patří autorita, sympatie, vzájemnost, důslednost, společenský souhlas a zvláštní příležitost. Rozlišují se dva typy autority, neformální (přirozená) a formální. Neformální autoritu představují rodiče. V pozdějším věku jsou to učitelé ve škole a výše postavení zaměstnanci v práci. Vzhledem k tomu, že bývají autority uznávané, útočník tohoto faktu využívá a vydává se před obětí například za nadřízeného. Oběť si nedovolí nadřízenému nesdělit informace, protože se obává možné hrozby výpovědi.

Útočník se může snažit budovat vztah s obětí přes vzájemné sympatie. Lidé se během svého života obklopují lidmi, kteří v nich vzbuzují jisté sympatie a mají společné zájmy, koníčky nebo názory. Útočník může díky vybudování důvěry získat od oběti potřebné citlivé informace.

Vzájemnost spočívá v prvotním poskytnutí služby oběti, která v ní vyvolá pocit zavázanosti. Snaha oběti na oplátku vykonat dobrý skutek umožňuje manipulaci s obětí podle potřeby útočníka.

Společenský souhlas představuje činnost, kterou už dříve vykonali jiní lidé. Typickým příkladem může být vyplnění dotazníku, který již vyplnili kolegové oběti.

V dotazníku je nutné vyplnit osobní údaje. Díky lidské vlastnosti, jako je zvědavost, je pravděpodobné, že útočník získá potřebné citlivé informace.

Za zvláštní příležitost lze považovat například akční lákavou nabídku, která je distribuovaná prostřednictvím informační technologie. Útočník má možnost získat od oběti přístupové údaje. (MITNICK A SIMON, 2003)

3.5. Právní úprava v oblasti sociálního inženýrství

Od samého prvopočátku, kdy se objevily nežádoucí činnosti prováděné prostřednictvím informačních a komunikačních technologií, existovala snaha o právní úpravu a postih těchto činností. Kybernetická kriminalita se velmi značně odlišovala od ostatních typů trestné činnosti. Vzhledem k rychlosti vývoje muselo docházet k okamžité změně legislativy, ať už byl odhalený útok úspěšný nebo neúspěšný.

Podle (KOLOUCH, 2016): „Před vlastní analýzou stávající platné a účinné legislativy v oblasti kyberkriminality je třeba podotknout, že nejen v rámci Evropské unie je zřetelná snaha po implementaci účinnějších právních nástrojů, které by byly schopné včas a adekvátně reagovat na kyberkriminalitu. Dochází tak k postupnému odstraňování rozporů a nedostatků v právních normách členských států EU a dalších států, které se rozhodly aktivně zapojit do boje s kybernetickou trestnou činností.“

Mezi prvotní dokumenty, které se zabývaly problematikou kybernetické kriminality a byly přijaty na mezinárodní úrovni, patřil Manuál OSN o prevenci a kontrole trestných činů spojených s počítači, přijatý v Havaně v roce 1990. V roce 2001 došlo na mezinárodní úrovni k přijetí Úmluvy o kybernetické kriminalitě a dodatkového protokolu. Jednalo se o dva nejvýznamnější právní dokumenty, které sloužily k usnadnění ochrany společnosti. Dokumenty definovaly základní okruh kybernetických trestných činů a představovaly možnosti, jak tuto činnost odhalit. V České republice byly dokumenty přijaty v roce 2005.

V České republice existují zákony, které se zabývají problematikou sociálního inženýrství. Zákony jsou sepsány například v trestním zákoníku nebo zákonu o kybernetické bezpečnosti.

Trestní zákoník

Zákony trestního práva upravuje trestní zákoník č. 40/2009 Sb. Novela trestního zákoníku vstoupila v platnost 1. ledna 2010. Kybernetická kriminalita, která se vztahuje k informačním a komunikačním technologiím, se dělí na trestnou činnost, kdy jsou technologie využité ke spáchání trestné činnosti a na trestnou činnost, kdy technologie představují cíl útoku. K problematice sociálního inženýrství se vztahují tyto paragrafy:

§ 120 Uvedení někoho v omyl a využití něčího omylu prostřednictvím technického zařízení

„Uvést někoho v omyl či využít něčího omylu lze i provedením zásahu do počítačových informací nebo dat, zásahu do programového vybavení počítače nebo provedením jiné operace na počítači, zásahu do elektronického nebo jiného technického zařízení, včetně zásahu do předmětů sloužících k ovládání takového zařízení, anebo využitím takové operace či takového zásahu provedeného jiným.“ (40/2009 SB. TRESTNÍ ZÁKONÍK, 2020)

Během testování zaměstnanců městského úřadu by mohla nastat situace, kdy se útočník v kanceláři zaměstnance ocitne sám se spuštěným počítačem. Útočník by mohl využít příležitosti a pokusit se získat citlivé informace. V tomto případě by se jednalo o trestný čin.

§ 181 Poškození cizích práv

(1) „Kdo jinému způsobí vážnou újmu na právech tím, že

a) uvede někoho v omyl, nebo

b) využije něčího omylu,

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.“ (40/2009 SB. TRESTNÍ ZÁKONÍK, 2020)

U metody vishing se útočník během telefonického rozhovoru vydává za někoho jiného a snaží se získat od zaměstnance citlivé informace. Takové jednání je v rozporu se zákonem.

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

(1) „Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a

a. neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

d. neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní i jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci.“ (40/2009 SB. TRESTNÍ ZÁKONÍK, 2020)

V rámci phishingu útočník rozesílá podvodné e-mailové zprávy, které obsahují odkaz na falešnou stránku. Po otevření odkazu je zaměstnanec vyzván například ke změně hesla vyplněním svých přístupových údajů. Takový čin lze považovat za trestný, protože útočník v případě vyplnění mohl získat citlivé informace.

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) „Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a. zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b. počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části, bude potrestán odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti.“ (40/2009 SB. TRESTNÍ ZÁKONÍK, 2020)

U metody baiting může být například na USB flash disk vytvořen a nahrán skript, který po vložení do počítače odešle přístupové údaje oběti na útočníkem zvolený server. V jiném případě by mohl skript umožnit vzdálený přístup do počítače oběti. Toto jednání je v rozporu se zákonem.

Zákon o kybernetické bezpečnosti

Právní úprava, která se týká kybernetické bezpečnosti v České republice, je obsažena v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Souvislost s problematikou sociálního inženýrství je popsána v paragrafu 7.

§ 7 Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

(1) „Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.

(2) Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.“ (181/2014 SB. O KYBERNETICKÉ BEZPEČNOSTI A O ZMĚNĚ SOUVISEJÍCÍCH ZÁKONŮ, 2020)

V případě kybernetické bezpečnosti, za použití různých metod útoků sociálního inženýrství, by mohlo dojít například k poškození databáze nebo havárii systému.

4. Metody sociálního inženýrství

Existuje několik metod sociálního inženýrství. Metody jsou založeny na chybném lidském úsudku, který představuje zdroj pro získání potřebných citlivých informací. Lidé často dělají chyby, aniž by si jich byli vědomi.

V současné době se už téměř žádný útok neobejde bez informačních a komunikačních technologií. Mezi metody sociálního inženýrství patří například vishing, phishing, pharming, baiting, smishing, trashing, tailgating, quid pro quo a pretexting.

4.1. Vishing

Metoda vishing je složena ze dvou slov, voice a phishing. S metodou phishing jsou si podobné, ale existuje mezi nimi určitý rozdíl. Metoda phishing využívá ke zjišťování citlivých informací elektronickou komunikaci, kdežto metoda vishing představuje zjišťování informací prostřednictvím telefonických hovorů. Cílem je například dostat z oběti potřebné informace nebo ji přimět dobrovolně přeposlat peníze na jiný účet. Vishing se soustřeďuje převážně na oběti, které lze považovat za zranitelné díky svému věku, intelektu a nejsou schopny hrozbu odhalit.

Všechny telefonické rozhovory jsou založeny na vypočítavosti volajícího. Volající zná telefonní číslo oběti, jméno, adresu bydliště a někdy i informace o bankovním účtu. Na začátku rozhovoru se představí jako zástupce společnosti, informuje oběť o nějakém problému s tím, že ihned ochotně nabídne společné vyřešení daného problému. (VISHING AND SMISHING: THE RISE OF SOCIAL ENGINEERING FRAUD, 2019)

Telefonickému rozhovoru může předcházet zaslání e-mailové zprávy oběti. Zpráva je sepsána tak, aby působila důvěryhodně a oběť neměla žádné podezření, že se jedná o podvod. Zpráva budí dojem, že pochází ze společnosti, kterou oběť využívá a dobře ji zná. Při uskutečnění hovoru se ozývá nahraná hlasová zpráva. Obsahem zprávy bývá většinou žádost o vyřešení určitého případu prostřednictvím kontaktování telefonní linky společnosti.

Metoda je v současné době stále více využívána. Důvodem je vyšší zabezpečení elektronické pošty (antispam, blacklist) a rozšíření volání přes internet. Internet nám umožňuje volání z kterékoliv části světa, která má dostatečnou internetovou konektivitu.

Technologie VoIP (Voice over Internet Protocol) přispívá k vyššímu počtu útoků pomocí vishingu. Na druhé straně linky může být například počítač, který lze snadněji zneužít než klasickou telefonní přípojku. Jedná se o službu, která nám umožňuje telefonický rozhovor přes internet. Zdigitalizovaný hlas se přenáší po síti díky paketům a oběť tak nemůže poznat, že se nejedná o klasický hovor, ale o hovor prostřednictvím VoIP. Existuje několik možností rozhovoru. Lze volat ze stolního či mobilního telefonu, počítače, notebooku nebo tabletu. (VOIP PHISHING AND THE WAY IT WORKS, 2020)

4.2. Phishing

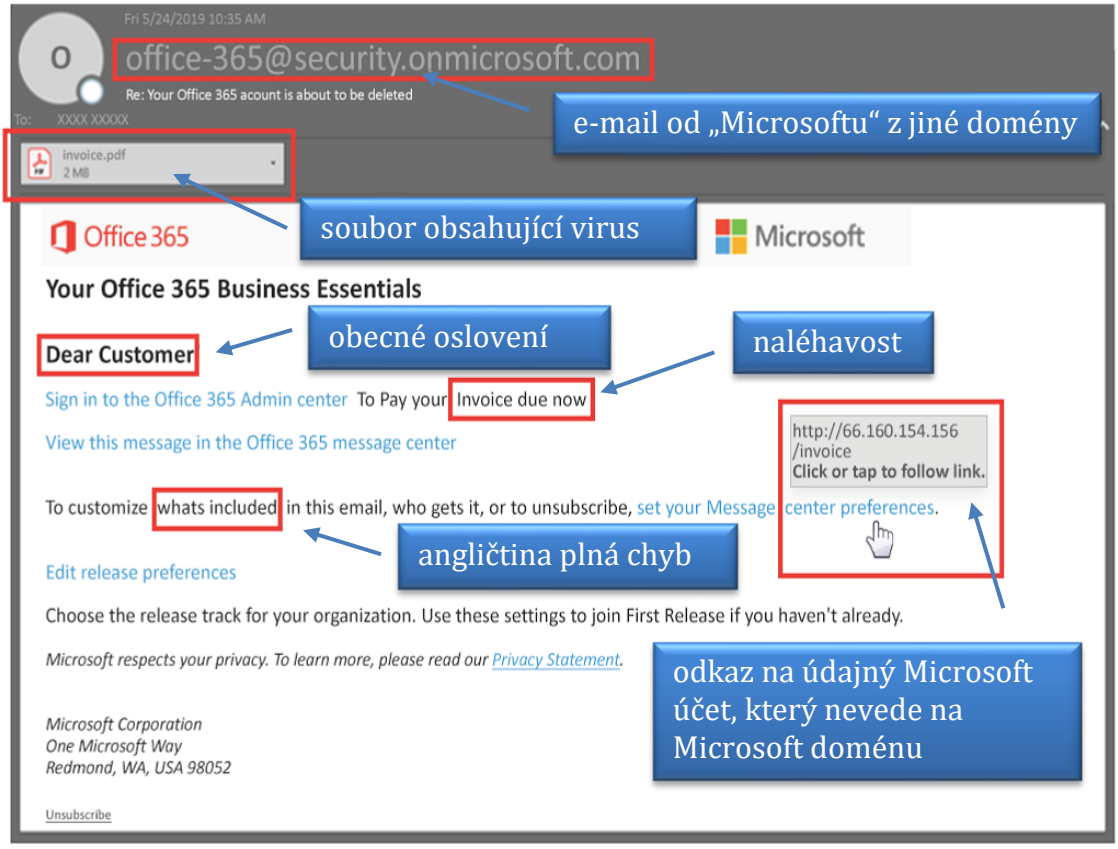
Metoda slouží k získávání citlivých informací (například uživatelská jména, hesla, čísla kreditních karet) za účelem zneužití. Útočník se díky těmto informacím může na síti vydávat za někoho jiného. Metoda probíhá prostřednictvím elektronické komunikace.

V roce 1995 se objevila první zmínka o phishingu. Došlo k napadení klientů společnosti American Online. Společnost v té době patřila mezi největšího poskytovatele internetového připojení v USA. Útok byl proveden prostřednictvím komunikačního systému společnosti. V současné době se útoky neustále zdokonalují a k jejich provedení je využita elektronická komunikace. (JAMES, 2007)

Phishing představuje homonymum ke slovu fishing, což znamená v českém překladu rybaření. Phishing a fishing mají podobný význam. Nahodí se návnada a čeká se, kdo nebo co se na ni chytne. (WHAT IS SOCIAL ENGINEERING? EMPLOYEES ARE YOUR WEAKEST LINK, 2019)

Prostřednictvím phishingového e-mailu se lze dostat například k citlivým informacím. Obsahem e-mailu (obrázek 8) mohou být odkazy na webové stránky, které jsou předem infikované. Nebo může e-mail obsahovat odkaz na webovou

stránku, která vizuálně vypadá stejně jako stránka oficiální a vyzývá oběť k vyplnění svých přístupových údajů. Údaje poté přijdou na e-mail útočníkovi. (HADNAGY A FINCHER, 2015)



Obrázek 8: Příklad podvodného e-mailu

Zdroj: TIPS FOR DETECTING A PHISHING EMAIL, VLASTNÍ ZPRACOVÁNÍ

Při aplikaci phishingu představuje velkou výhodu nesoustředěnost obětí. Přitom tento typ útoku je každý člověk schopen odhalit. Důležité je být obezřetný a vždy si zkontrolovat název domény i přes to, že podvodná stránka vypadá na první pohled stejně jako stránka skutečná. I sebemenší odlišnost v názvu stránky nás může upozornit na možnou nepravost stránky. Například může být odlišnost mezi seznam.cz a sezam.cz.

Dalším handicapem uživatelů může být neznalost problematiky sociálního inženýrství. Tento handicap se snaží zmírňovat média nebo instituce, které rozesílají informace o možné hrozbě útoku. Poskytují rady, jak je možné útoku předejít.

Jednou z doporučených rad je dodržování zlatého pravidla, kdy by se uživatelé neměli důvěrně svěřovat s citlivými informacemi. (JIROVSKÝ, 2007)

Mezi další phishingovou metodu patří útok pomocí vyskakovacího okna. *„V rámci metody vyskakovacího okna nastavíme náš phishingový server tak, aby otevřel vyskakovací okno ve chvíli, kdy přesměrovává oběť na skutečný cíl. Tento postup je dnes nejneobvyklejším typem útoku, protože nástroje blokující vyskakovací okna jsou velmi rozšířené a jsou dokonce standardně vestavěné do většiny prohlížečů na trhu, čímž snižují šanci této metody na úspěch. V našem případě vyřadíme jeden nástroj blokující vyskakovací okna, abychom mohli tuto techniku předvést.“* (JAMES, 2007)

4.3. Pharming

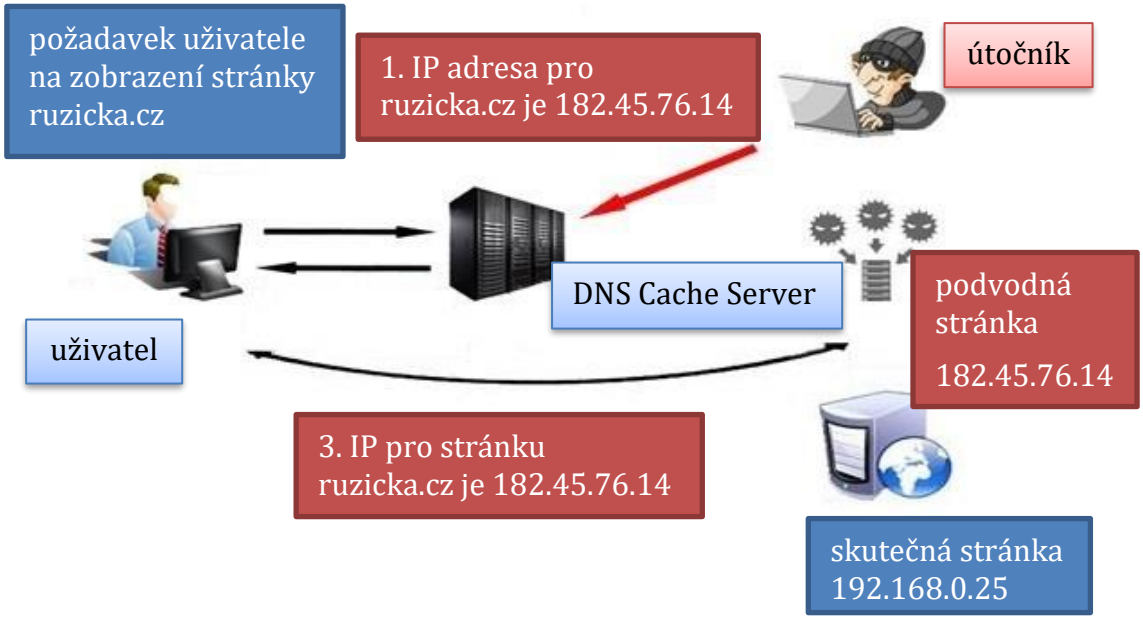
Metoda pharming je podobná metodě phishing. Často dochází k záměně těchto dvou metod. Phishing funguje na principu lákání oběti prostřednictvím podvodného e-mailu nebo odkazu. U pharmingu dochází k přesměrování na podvodnou webovou stránku i přesto, že oběť zadá správnou webovou adresu. Metoda je, na rozdíl od phishingu, obtížně odhalitelná. Nevzniká podezření, že by se mohlo jednat o podvod. Výhoda útočníka spočívá v tom, že si nemusí nic vymýšlet a vytvářet scénáře pro klamání oběti. (PHARMING, 2020)

Počítač, který se připojí do sítě, získá svou vlastní IP adresu. Tuto IP adresu je možné si představit jako telefonní číslo. Aby si uživatel mohl zapamatovat internetové stránky a nemusel si pamatovat IP adresy těchto stránek, byl vytvořen DNS systém (anglicky Domain Name Systém). Tento DNS systém slouží k přiřazování doménových jmen k jednotlivým IP adresám internetových stránek. Uživateli umožňuje zadávat do prohlížeče název stránky, kterou chce zobrazit bez nutnosti zapamatování si IP adresy pro jednotlivou internetovou stránku. (CZ.NIC – O DOMÉNÁCH A DNS, 2020)

Při aplikaci metody pharming dochází k záměně adres, kdy podvodná URL adresa má stejnou podobu jako adresa původní stránky. Po zadání URL adresy do prohlížeče dojde k přesměrování na podvodnou IP adresu. Vzhledem k tomu, že se zadává pravá URL adresa, lze metodu pharming považovat za jeden z nejhůře

zjistitelných útoků. Obrana před touto metodou je velmi komplikovaná. (PARSONS A OJA, 2014)

Útok metodou pharming je znázorněn na obrázku 9:



Obrázek 9: Hrozba DNS cache poisoning

Zdroj: ATTACKS OVER DNS, VLASTNÍ ZPRACOVÁNÍ

Z obrázku 9 je patrné, že se jedná pro uživatele o obtížně zjistitelný útok. Při tomto útoku je napaden DNS server. DNS server obsahuje seznam webových stránek s přidělenou IP adresou. Jakmile se do prohlížeče zadá adresa webové stránky, automaticky se odešle dotaz DNS serveru na IP adresu, kde je možné se na stránku připojit. Princip DNS cache poisoning spočívá ve vytvoření podvodné webové stránky s určitou IP adresou. Útočník napadne DNS server poskytovatele internetu, u kterého je oběť připojená. Na serveru změní nebo vloží vlastní DNS záznam. V tomto záznamu dochází ke změně IP adresy oficiální stránky na podvodnou. Podvodné stránky jsou zpracované tak, že jsou nerozeznatelné od původních. (CLOUDFLARE, 2020)

U metody nedochází k infikování počítače, jelikož se přesměrování odehrává na serveru. Existuje mnoho způsobů, jak DNS server napadnout. Napadení DNS serveru

neodhalí antivirová ochrana oběti, protože se uskutečňuje mimo operační systém počítače.

Metoda pharming umožňuje zaměření na velké množství uživatelů v krátkém časovém horizontu. Ochrana proti těmto útokům je záležitostí síťové bezpečnosti. Ochrana DNS serverů závisí na jednotlivých poskytovatelích internetu. (BROWN, 2010)

4.4. Baiting

Další metodou sociálního inženýrství je baiting. Název je odvozený z anglického slova „bait“, což v českém překladu znamená návnada. Metoda využívá jako svoji návnadu přenosná datová média.

Princip baitingu spočívá v zanechání infikovaného přenosného datového média na takovém místě, aby oběť médium nalezla a použila. Útočník může požádat jinou osobu, aby médium umístila místo něj. Přenosným datovým médiem může být například USB flash disk, CD nebo DVD. Úspěšnost metody lze zvýšit pomocí vhodně nadepsaného média tak, aby bylo pro oběť zajímavé a nebála se ho použít. (SOCIAL ENGINEERING: WOULD YOU TAKE THE BAIT?, 2019)

Přenosné datové médium (obrázek 10) lze infikovat softwarem, který se při připojení nahraje do počítače oběti a útočníkovi tak umožní vzdálený přístup k citlivým informacím. Jestliže je počítač připojen do interní sítě firmy, útočník má možnost dostat se i do jiných počítačů, které jsou ve stejné síti. (BAITING, WHAT IS IT? HOW TO DEFEND YOURSELF FROM SOCIAL ENGINEERING, 2020)

Obrázek 10: Příklad nastraženého CD

Zdroj: VLASTNÍ ZPRACOVÁNÍ

Vzhledem k tomu, že se musí útočník pohybovat v cílové oblasti, kam se rozhodl umístit infikované přenosné datové médium, existuje vysoké riziko jeho prozrazení. (CROSS A SHIMONSKI, 2014)

U metody baiting dochází v dnešní době k postupnému vývoji. Díky smartphonům a technologii QR kódů se vyskytl nový způsob útoku. Většina dnešních smartphonů má aplikaci pro čtení QR kódů, proto se může jejich uživatel jednoduše stát obětí a narazit na návnadu uloženou v QR kódu. Tento QR kód může obsahovat odkaz na adresu webové stránky, která je infikovaná útočníkem. Aplikace smartphonu webovou adresu automaticky otevře. (ALCORN, FRICHOT A ORRÚ, 2014)

Útoky, které jsou typické baitingu, se neustále zdokonalují a soustřeďují na moderní technologie a zařízení. Jsou směřovány na využití výhod útočníka nad svými oběťmi. Uživatelé, kteří používají QR kódy, si většinou neuvědomují riziko, že by QR kód mohl obsahovat infikovanou adresu webové stránky a oni se tak mohli stát obětí útoku.

4.5. Smishing

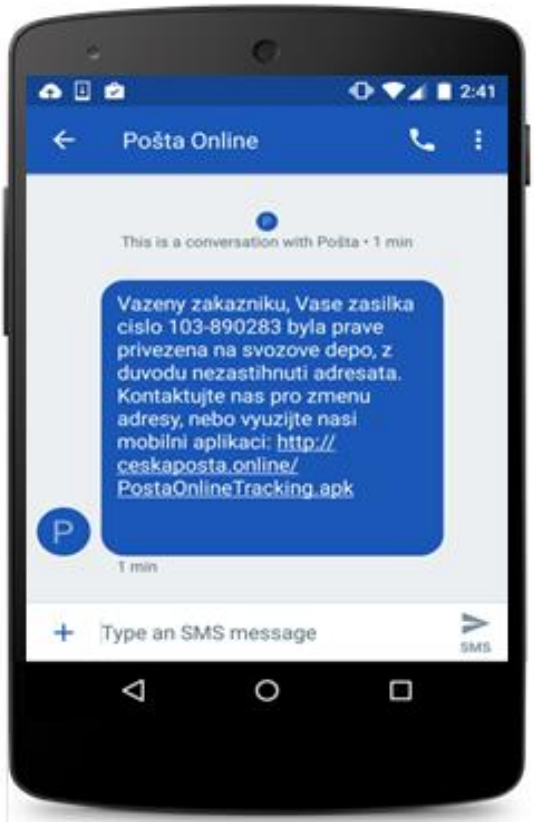
Smishing (SMS phishing) je metoda podobná vishingu. U obou metod probíhá útok prostřednictvím mobilního telefonu. Citlivé informace jsou zjišťovány pomocí SMS zpráv. Metoda funguje na principu odesílání odkazů nebo ověřovacích kódů. Jestliže SMS vyzývá k otevření odkazu, který oběti přišel na mobilní telefon, není možné odkaz vždy otevřít. Telefon musí mít k dispozici připojení na internet. Po kliknutí na odkaz se oběti zobrazí vytvořená podvodná stránka, která je podobná skutečné stránce společnosti. Útočník se ve zprávě například vydává za společnost, kterou oběť dobře zná. Útočník může ve zprávě žádat o opis ověřovacího kódu a zpětné zaslání. (WHAT IS SMISHING?, 2019)

Další možností je odesílání SMS zpráv, které obsahují telefonní číslo. Při uskutečnění hovoru se většinou ozve telefonní automat. SMS zprávy mohou být odesílány například prostřednictvím webových serverů, které umožňují hromadné odesílání zpráv. Také mohou být SMS zprávy odeslány přes servery, které nabízí bezplatné odesílání zpráv. (DUNHAM, 2009)

U útoku, který prostřednictvím SMS zprávy vyzývá ke zpětnému zavolání, nezáleží na typu mobilního telefonu oběti. Útok lze provést i na telefonu, který nemá k dispozici nebo nevyužívá internetové připojení.

Rozesílání podvodných SMS zpráv každým rokem přibývá. Největší podíl nese vznik vícefaktorové autentizace. Z hlediska bezpečnosti je potřeba počítat s tím, že útočník zná přístupové údaje oběti (první faktor – znalost), proto se následně využívá například mobilní telefon pro zaslání ověřovacího kódu (druhý faktor – vlastnictví). (CO JE TO 2FA A PROČ VÍCEFAKTOROVOU AUTENTIZACI POUŽÍVAT, 2019)

Během útoku je možné do mobilního zařízení stáhnout škodlivý software. Útočník odešle oběti z podvodného telefonního čísla textovou zprávu, která obsahuje škodlivý odkaz. Typický příklad odesílané SMS zprávy je znázorněn na obrázku 11.



Obrázek 11: Smishing na klienty České pošty

Zdroj: THE SMISHING THREAT, 2019

V současné době používá převážná většina lidí smartphone, přes který si vyřizují osobní i pracovní záležitosti, například e-mailovou korespondenci nebo komunikaci na sociálních sítích. Také přes smartphone využívají služby internetového bankovnictví. (HOW TO AVOID BECOMING THE VICTIM OF A SMISHING SCAM, 2019)

Další možností, která souvisí s metodou smishing, je využití MMS zprávy místo zprávy SMS. Rozdíl mezi těmito dvěma typy zpráv spočívá v jejich zobrazení. MMS zpráva umožňuje lepší grafické zobrazení, například logo firmy. Díky tomuto zobrazení může působit na oběť důvěryhodněji. Způsob provedení útoku a jeho následky prostřednictvím MMS zprávy je shodný s útokem přes SMS zprávu.

Vzhledem k tomu, že lidé více důvěřují textovým zprávám než elektronické poště, lze považovat metodu za efektivní.

4.6. Trashing

Metoda trashing je odvozena od slova „trash“, což v českém překladu znamená odpad. Někdy bývá označována jako dumpster diving. Metoda sociálního inženýrství představuje prohledávání kontejnerů s odpadem pro získání potřebných informací. V kontejnerech lze najít dokumenty, které oběť nepovažuje za důležité. Pro útočníka to mohou být naopak cenné informace, které mohou posloužit k plánovanému útoku. Nepříjemností je pohyb v zapáchavém prostředí a špíně. Získávání informací může být zdlouhavé a může vyžadovat vynaložení většího úsilí. Jestliže útočník získá data, pro které útok plánoval, nemusí dále pokračovat.

Kontejnery s odpadem představují pro útočníka bohatý zdroj informací, kde může nalézt například schéma společnosti, bezpečnostní dokumenty, marketingové plány, CD, zdrojové kódy, přihlašovací údaje, hesla nebo telefonní seznam. V telefonním seznamu lze najít jména zaměstnanců a kontakt na ně. To umožňuje útočníkovi zaútočit přímo. (HOW INTRUDERS GAIN ACCESS TO NETWORK USING SOCIAL ENGINEERING, 2019)

Jelikož útočník nepřichází do kontaktu s obětí, lze tuto metodu považovat za bezpečný způsob získání potřebných informací. Veškeré informace jsou získávány z kontejnerů a popelnic, které jsou určené pro odpad. Vzhledem k minimální hrozbě nebezpečí a vyšší efektivnosti, je metoda oblíbená především u mladistvých, začínajících útočníků. K prohledávání kontejnerů a popelnic nejsou potřebné technické znalosti ani dovednosti. (MITNICK A SIMON, 2003)

Mezi nástroje, které útočník potřebuje, patří rukavice a svítilna. Typickou barvou oblečení je černá. Bývají využity i obleky úklidové nebo popelářské služby. (BOSWORTH, KABAY A WHYNE, 2014)

Proti útoku existuje jednoduchá obrana. Stačí pouze veškeré dokumenty a digitální nosiče informací před vhozením do kontejneru nebo popelnice znehodnotit.

4.7. Tailgating

Jednou z metod sociálního inženýrství je tailgating. Používá se tehdy, když se neoprávněná osoba potřebuje dostat do oblasti s omezeným přístupem. Předpokladem úspěchu metody je držení se v těsné blízkosti oprávněné osoby. Typickým příkladem může být kurýr, který potřebuje doručit zásilku do budovy podniku. Čeká, až se objeví zaměstnanec s oprávněným přístupem. Poté, co zaměstnanec projde zabezpečovacím systémem, požádá kurýr o podržení dveří, aby mohl také projít.

V současné době není metoda příliš efektivní. U většiny podniků existuje několik identifikačních prvků, bez kterých se neoprávněná osoba do budovy nedostane. Příkladem mohou být přepážky pro vstup, u kterých je potřeba identifikační karta zaměstnance.

Existuje podobná metoda, která se nazývá piggybacking. Metoda spočívá ve snaze útočníka připojit se ke skupině lidí a dostat se tak do oblasti s omezeným přístupem. Aby se útočník vyhnul případnému podezření, snaží se navázat nezávazný rozhovor s jedincem ze skupiny. Musí vyvolat dojem, že se zná velmi dobře s jedincem, který má oprávněný vstup do oblasti. (5 SOCIAL ENGINEERING ATTACKS TO WATCH OUT, 2019)

4.8. Quid Pro Quo

Quid Pro Quo znamená v českém překladu „něco za něco“. Metoda funguje na principu výměny služby za jinou protislužbu. Může jít i o výměnu informací. Očekává se, že oběť bude důvěřivá a útočník bude schopen ovlivnit oběť tak, aby si myslela, že výměna informace nebo služby je pro obě strany výhodná.

S touto metodou se lze nejčastěji setkat v případě, kdy se útočník vydává za IT specialistu. Obvolává zaměstnance podniku tak dlouho, dokud se neobjeví někdo, kdo pomoc potřebuje. Za poskytnutí pomoci vyžaduje útočník informaci nebo přístup do systému. Jestliže útočník oběti namluví, že k vyřešení problému potřebuje vzdálený přístup k počítači, oběť v domnění, že mu chce útočník pomoci, přístup zajistí. Útočník se díky tomuto přístupu dostane nejen do počítače oběti, ale

i do ostatních počítačů v síti podniku. (5 SOCIAL ENGINEERING ATTACKS TO WATCH OUT FOR, 2019)

4.9. Pretexting

Pretexting spočívá v získávání citlivých informací pomocí předem vymyšleného scénáře. Je důležité, aby oběť vymyšlenému scénáři uvěřila a dobrovolně poskytla potřebné informace. Využívá se předešlého průzkumu, při kterém je zjištěna určitá informace. Ta se poté zakomponuje do scénáře a slouží k tomu, aby v oběti vyvolala pocit důvěry. Pokud oběť scénáři uvěří, je velká pravděpodobnost, že nám bude ochotna sdělit potřebné informace. Pretexting lze využít v přímé i nepřímé komunikaci. (5 SOCIAL ENGINEERING ATTACKS TO WATCH OUT, 2019)

Úkolem útočníka je přesvědčit oběť, že jde o někoho jiného než ve skutečnosti. Důležitou roli hraje nachystaná řeč a intonace. Jestliže jde o osobní setkání, je potřeba, pro podporu důvěryhodnosti, zvolit vhodné oblečení, případně si obstarat falešnou dokumentaci. Aby útočníkův projev nepůsobil jako herecký výkon a vyhnul se odhalení, volí si raději roli, se kterou má jisté zkušenosti. Scénáře bývají situovány tak, aby vyvolaly u oběti zvědavost a zájem.

Nejčastěji používaným prostředkem pro nepřímou komunikaci je stolní nebo mobilní telefon. V současné době lze prostřednictvím telefonického rozhovoru vyřídit čím dál více záležitostí. Například banka umožňuje svým klientům přes telefon uzavírání smluv nebo změnu osobních údajů. Pro ověření totožnosti volajícího stačí znát své rodné číslo, bezpečnostní otázky nebo aktuální zůstatek účtu. (SUCCESSFUL PRETEXTING, 2020)

Prostředí, které lze považovat za ideální k tvorbě efektivního útoku, získáme propojením sociálního inženýrství s informační a komunikační technologií. Rozlišení jednotlivých metod útoků napomáhá při obraně nebo prevenci před samotným útokem. Útočníci využívají osvědčené metody útoků, které se neustále opakují. Přesto oběti nedokáží útoky odhalit a ponaučit se z nich.

Ochrana před sociálním inženýrstvím

Vzhledem k tomu, že jsou jednotlivé metody sociálního inženýrství založeny na chybném lidském úsudku, bojovat proti nim je velmi obtížné. Pravděpodobnost, že se podaří zamezit útokům, bývá velmi nízká. Základním předpokladem ochrany před sociálním inženýrstvím je dodržování určitých zásad a využívání znalostí. Jednou ze zásad je nikomu nedůvěřovat. Například v každé online komunikaci je nezbytně nutné si ověřit, zda se jedná o osobu, za kterou se účastník komunikace vydává.

Ochrana v online prostředí

V současné době, v souvislosti s rozšiřováním pokrytí internetu, začalo stále častěji docházet k okrádání uživatelů skrze elektronickou poštu a internet. Toto prostředí umožňuje útočníkovi jistou anonymitu, u které se neočekává, že by mohl mít uživatel nějaké pochybnosti a byl nedůvěřivý. U těchto případů je nezbytně nutná správnost nastavení počítače, která zajistí bezpečnou ochranu uživatele. (MCCARTHY A WELDON-SIVIY, 2013)

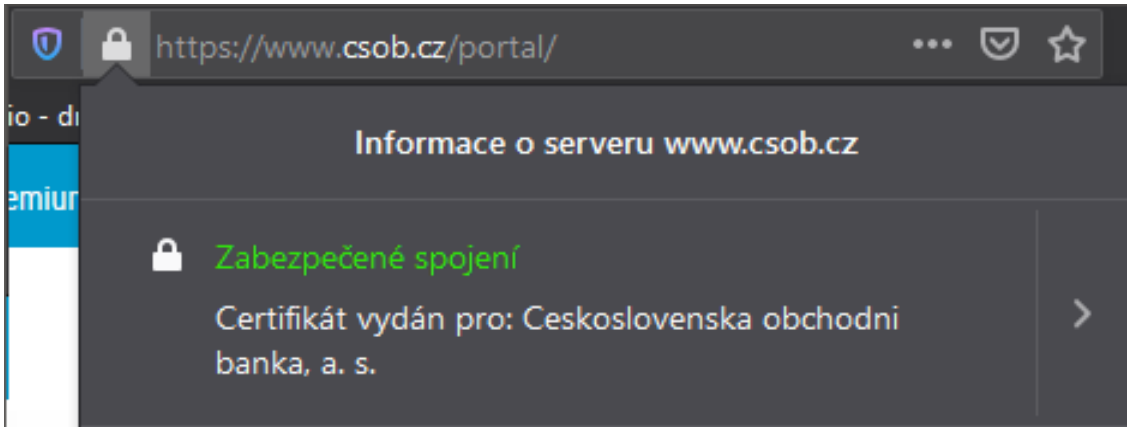
Správnost nastavení počítače

V první řadě je nutné na počítači nastavit firewall a zkontrolovat, jestli je zapnutý. Firewall slouží k filtrování veškeré komunikace, která probíhá po síti a mezi zařízeními. Součástí systému Windows je předem nainstalovaný firewall. Například u systému Windows 10 je předem nainstalovaný Windows Defender. Jeho zapnutí nebo vypnutí lze provést přímo v nastavení systému, konkrétně v položce Aktualizace a zabezpečení. Dále zvolíme Zabezpečení Windows a nakonec vybereme Firewall a ochrana sítě. Veškerá ochrana spočívá v předem nastavených pravidlech. Pravidla mohou být kdykoliv přidána, upravena nebo odebrána. Lze je nastavit pro jakoukoliv aplikaci, službu či port.

Přesto, že je firewall u Windows 10 předem nainstalovaný, uživatel ho nemusí využívat. Existuje několik verzí firewallů. Mezi placené patří například ESET, AVG, Avast a mezi zdarma poskytované ZoneAlarm, Comodo Firewall.

Protokoly SSL

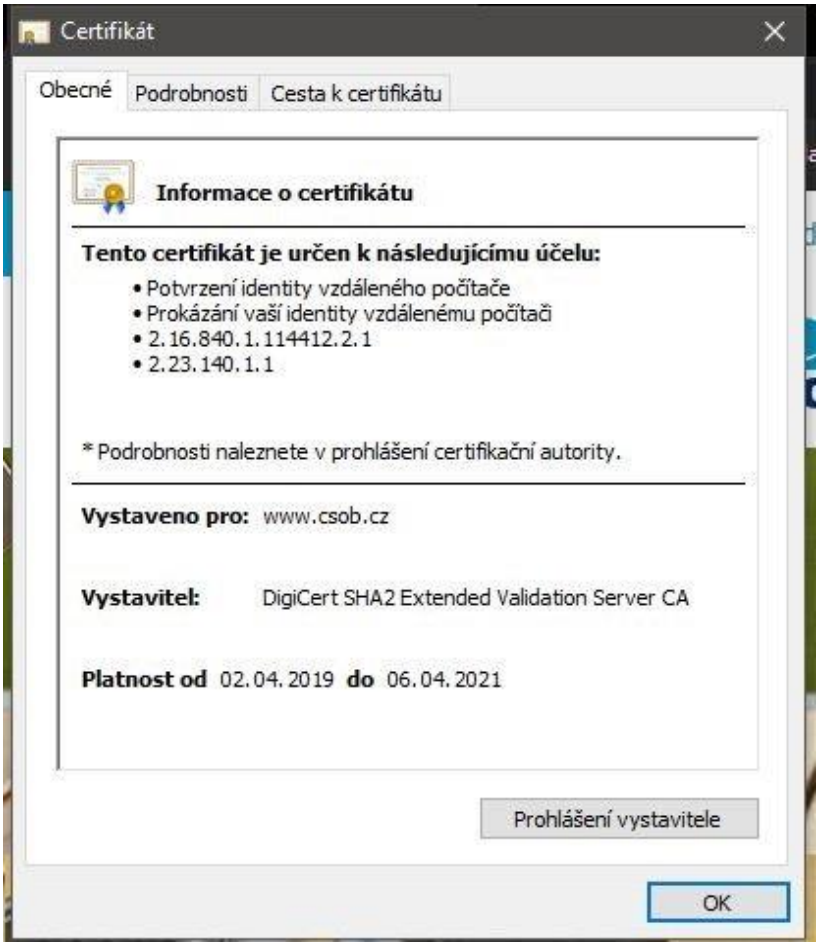
Protokoly SSL slouží k identifikaci klienta a serveru. Při jejich využití dochází k šifrování komunikace mezi nimi. Využití těchto protokolů je snadno rozpoznatelné. Vedle adresního řádku je zeleným písmem zobrazený protokol, o který se jedná. V adresním řádku vyhledávače je běžná zkratka http nahrazena zkratkou https. Ukázka adresního řádku s protokolem je na obrázku 12.



Obrázek 12: Adresní řádek s protokolem

Zdroj: ČSOB, VLASTNÍ ZPRACOVÁNÍ

Protokoly nepředstavují pro klienta jistotu bezpečí. Představují pouze značení, že je komunikace zašifrována a chráněna před odposloucháváním. Protokoly využívají certifikáty (obrázek 13), které jsou klíčovým prvkem pro bezpečnou komunikaci. Obsahují bezpečnostní prvky, které zabraňují jejich falšování. Dále obsahují datum vydání, datum expirace a informace, k jakému serveru patří. Při otevírání různých webových stránek je důležité ověřovat informace z certifikátu. Dosáhne se tak vyšší bezpečnosti.



Obrázek 13: Podrobnosti SSL certifikátu

Zdroj: ČSOB, VLASTNÍ ZPRACOVÁNÍ

Prověření příloh, odkazů

Jestliže přijde uživateli neočekávaný e-mail s přílohou, uživatel by měl nejprve přílohu stáhnout do počítače a vložit do antivirového skeneru. Jedním z nejznámějších online skenerem, který slouží k testování souborů, je Virustotal.com. Na tomto online skeneru prověří soubor více než čtyřicet antivirových programů.

V případě, že přijde uživateli neočekávaný e-mail s odkazem na webovou stránku, pro ověření tohoto odkazu je možné využít sandbox. Ten představuje prostředí, ve kterém lze izolovaně spustit program, například internetový prohlížeč. Do prohlížeče uživatel vloží odkaz na webovou stránku. Pokud byl odkaz infikovaný,

nedojde díky sandboxu k infikování zařízení. K těmto účelům je nejčastěji používán program Sandboxie.

Podvodná e-mailová adresa

V současné době téměř každý uživatel používá svou e-mailovou adresu například pro jednorázové nákupy na e-shopech, registraci ke službám nebo si uživatel zveřejní e-mail na svých vlastních webových stránkách. Díky tomu může být e-mailová adresa snadno zneužita spamery. Spameři vyhledávají na internetu pomocí web crawler typické znaky, například @. Tento znak obsahuje každá e-mailová adresa. Spameři provedou sběr všech dostupných adres a dále je nabízí společnostem, které je od nich vykupují. Z tohoto důvodu je pro uživatele vhodné založit si podvodnou e-mailovou adresu. Potřebné e-maily si může nechat prostřednictvím filtru automaticky přeposílat na svou primární e-mailovou adresu. Díky tomuto opatření se uživatel vyhne velkému počtu spamů.

Výběr případů zaznamenaných útoků sociálního inženýrství v rámci České republiky

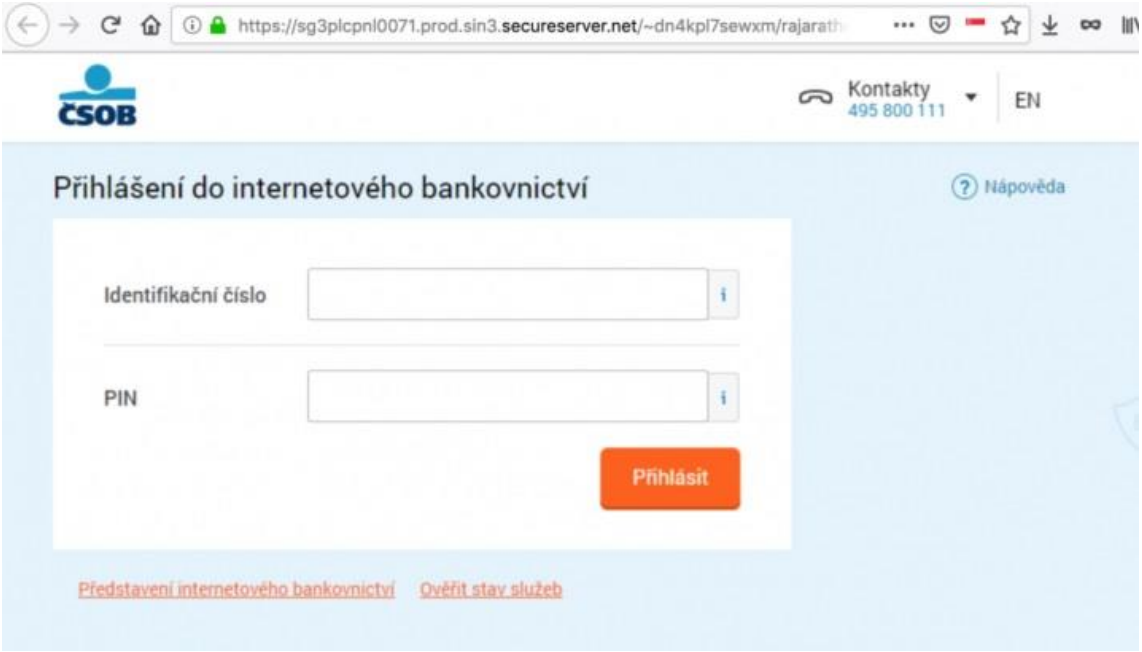
Kapitola je věnována několika vybraným případům zaznamenaných útoků sociálního inženýrství v rámci České republiky.

V roce 2019 se útočníci zaměřili na některé klienty Československé obchodní banky, a. s. (ČSOB), a poslali jim podvodnou e-mailovou zprávu (obrázek 14). Zpráva měla informovat o neobvyklé aktivitě na jejich klientském účtu. E-mail obsahoval hypertextový odkaz, který měl přesměrovat klienta na webovou stránku banky.

Obrázek 14: Podvodný e-mail ČSOB

Zdroj: ČSOB, 2020

Z obrázku 14 je patrné, že se jedná o podvodnou e-mailovou zprávu. Obsahuje nevhodné oslovení a chybnou češtinu. Zpracování e-mailové zprávy a použitý hypertextový odkaz působí velmi nevěrohodně.

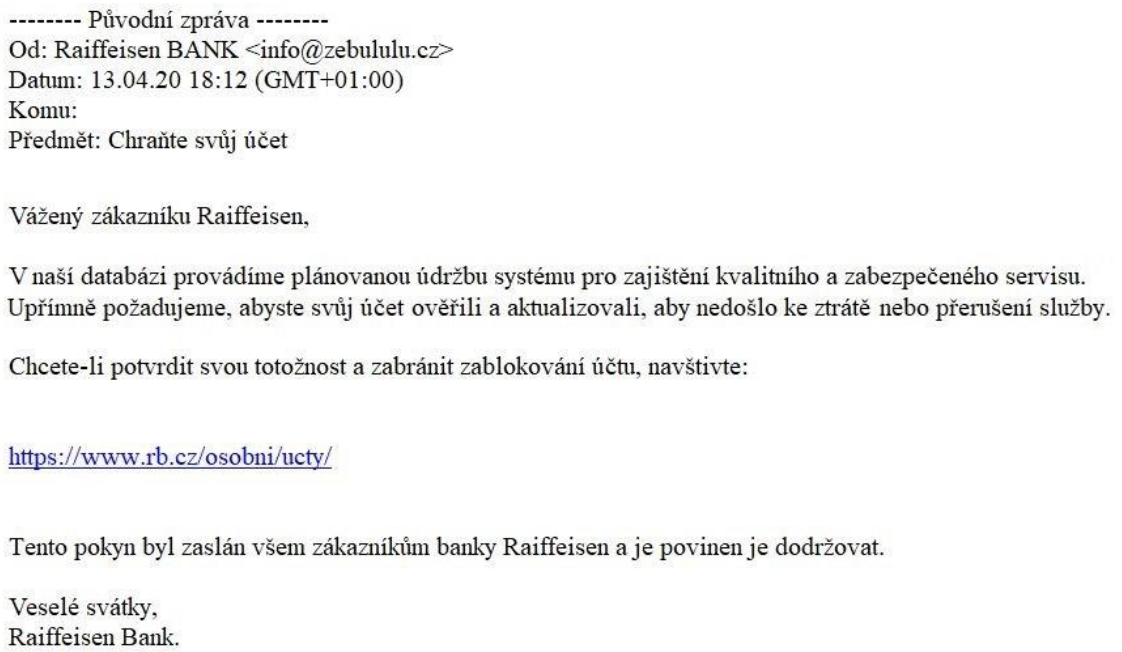


Obrázek 15: Podoba podvodné webové stránky ČSOB

Zdroj: ČSOB, 2020

Podvodná webová stránka (obrázek 15) vypadala na první pohled jako oficiální, ale ve skutečnosti šlo o stránku podvodnou. Zásadní rozdíl mezi oficiální a podvodnou stránkou spočíval v adresním řádku. U podvodné stránky byla využita jiná doména. Po přesměrování byl klient požádán o vyplnění svých přihlašovacích údajů pro vstup do internetového bankovnictví. Pokud klient své přihlašovací údaje vyplnil a potvrdil je ověřovacím SMS kódem, zobrazilo se chybné hlášení. Útočníci tak získali všechny potřebné údaje pro vstup do internetového bankovnictví klienta.

Dalším případem zaznamenaného útoku v České republice byla e-mailová zpráva (obrázek 16), která se vydávala za společnost Raiffeisenbank. Text zprávy obsahoval informaci o plánované údržbě systému banky a prosbu o ověření účtu klienta, aby nedošlo k případné ztrátě nebo přerušení služby. E-mailová zpráva obsahovala hypertextový odkaz, který vypadal, že odkazuje na oficiální stránky banky, přitom po kliknutí na odkaz byl přesměrován na podvodnou webovou stránku. (PHISHING|RAIFFEISENBANK, 2020)



-------- Původní zpráva --------
Od: Raiffeisen BANK <info@zebululu.cz>
Datum: 13.04.20 18:12 (GMT+01:00)
Komu:
Předmět: Chraňte svůj účet

Vážený zákazníku Raiffeisen,

V naší databázi provádíme plánovanou údržbu systému pro zajištění kvalitního a zabezpečeného servisu.
Upřímně požadujeme, abyste svůj účet ověřili a aktualizovali, aby nedošlo ke ztrátě nebo přerušení služby.

Chcete-li potvrdit svou totožnost a zabránit zablokování účtu, navštivte:

https://www.rb.cz/osobni/ucty/

Tento pokyn byl zaslán všem zákazníkům banky Raiffeisen a je povinen je dodržovat.

Veselé svátky,
Raiffeisen Bank.

Obrázek 16: Podvodný e-mail Raiffeisenbank

Zdroj: PHISHING|RAIFFEISENBANK, 2020

Jiný případ byl zaměřen na vrácení daní za rok 2019. Obsahem e-mailové zprávy (obrázek 17) byla informace o vrácení daně a odkaz, který měl přesměrovat oběť na

stránky Ministerstva financí České republiky (MFCR). Vzhledem k tomu, že šlo o útok sociálního inženýrství, oběť přesměroval na podvodnou webovou stránku. Na podvodné stránce se nacházel formulář, který požadoval vyplnění identifikačních údajů a následně údaje o platební kartě. (MFCR VARUJE PŘED PODVODNÝMI E-MAILOVÝMI ZPRÁVAMI, 2020)


Ministerstvo financí
České republiky

Po kontrole všech daní zaplacených od roku 2019 se společnost MFCR rozhodla,

že jste elegantní, abyste dostali vrácení daně ve výši 6 841,25 Kč.
Chcete-li požádat o vrácení daně online, musíte vyplnit formulář žádosti
s požadovanými informacemi.
Podrobnosti:
Kód opakování: #CZ-86B5-2019
Částka, která má být vrácena: 6841,25 Kč

Můžete požádat zde:
https://adiseet.mfcr.cz/auth/LoginPage.faces

Platba může být zpožděna z různých důvodů, jako je předložení neplatných
záznamů o platnosti po termínu 31. května 2020.

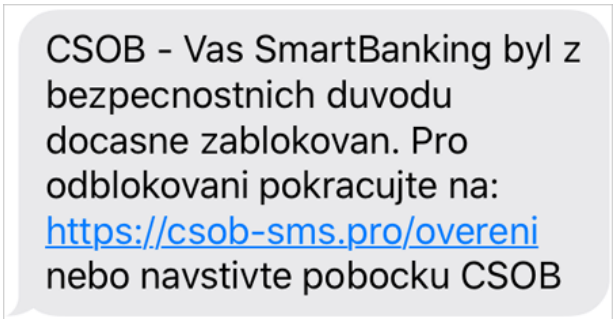
Pozdravy,
MFCR © 2020.

Obrázek 17: Podvodný e-mail MFCR

Zdroj: MFCR VARUJE PŘED PODVODNÝMI E-MAILOVÝMI ZPRÁVAMI, 2020

SMS zprávy

Klienti Československé obchodní banky, a. s. (ČSOB), neobdrželi pouze podvodné e-mailové zprávy, ale přicházely jim i podvodné SMS zprávy (obrázek 18). Obsahem SMS zprávy byla informace o dočasném zablokování internetového bankovnictví. Dále obsahovala hypertextový odkaz, který měl problém se zablokováním vyřešit. Odkaz ale klienta přesměroval na podvodnou webovou stránku, která se velmi podobala oficiální stránce internetového bankovnictví. Webová stránka požadovala po uživateli vyplnění všech dat z platební karty. (KROMĚ PHISHINGOVÝCH E-MAILŮ POSÍLAJÍ ÚTOČNÍCI TAKÉ SMS, 2020)



Obrázek 18: Podvodná SMS zpráva ČSOB

Zdroj: KROMĚ PHISHINGOVÝCH E-MAILŮ POSÍLAJÍ ÚTOČNÍCI TAKÉ SMS, 2020

S podvodnými SMS zprávami se setkali i zákazníci Apple zařízení. Obsah SMS zprávy (obrázek 19) byl velmi podobný té, kterou obdrželi klienti ČSOB (obrázek 18). Z toho vyplývá, že se útočníci v obou případech pokoušeli dostat z obětí informace o jejich platební kartě, včetně CVC kódu (obrázek 20). Tento kód se nachází na zadní straně platební karty. Jestliže se útočníkům podaří získat informace o platební kartě oběti, mohou s kartou zaplatit například v e-shopech, které nepoužívají 3D Secure zabezpečení. (ČESKÉ UŽIVATELE APPLE PRODUKTŮ OHROŽUJE NOVÝ PHISHING, 2020)

Obrázek 19: Podvodná SMS zpráva APPLE

Zdroj: ČESKÉ UŽIVATELE APPLE PRODUKTŮ OHROŽUJE NOVÝ PHISHING, 2020

Obrázek 20: Podoba podvodné stránky APPLE

Zdroj: ČESKÉ UŽIVATELE APPLE PRODUKTŮ OHROŽUJE NOVÝ PHISHING, 2020

Dalším zaznamenaným útokem v České republice byla fiktivní soutěž (obrázek 21). V soutěži došlo ke zneužití jména a loga společnosti Česká pošta, s. p., když útočníci vytvořili podvodnou Facebookovou stránku se jménem společnosti. Na stránce byla zveřejněna klamavá reklama. Předmětem výhry fiktivní soutěže byl mobilní telefon. Jednalo se o telefon značky Apple. Podmínkou pro jeho získání bylo odeslat členský poplatek.

Obrázek 21: Fiktivní výhra

Zdroj: MANIPULÁTOŘI, 2020

Text k fiktivní soutěži:

„Všichni noví zákazníci se zúčastňují losování cen zobrazeného produktu kampaně. Pokud jste šťastným výhercem, budete kontaktováni přímo prostřednictvím e-mailu. Tato speciální nabídka přichází s 4 dny trvající zkušební dobou přidělené předplacené služby, po které bude měsíční členský poplatek (70 EUR) odečten z Vaší kreditní karty. Pokud nejste z jakéhokoli důvodu spokojeni se službou, můžete svůj účet zrušit do 4 dnů. Služba bude obnovována měsíčně až do zrušení. Tato kampaň vyprší 31. prosince 2020.“ (ČESKÁ POŠTA VARUJE PŘED PODVODNOU SOUTĚŽÍ O IPHONE 11, 2020)

5. Aplikace vybraných metod

Cílem aplikace vybraných metod sociálního inženýrství je ukázat, jak je možné v praxi získat citlivé informace od zájmových osob.

Pro aplikaci vybraných metod útoků sociálního inženýrství byl vybrán městský úřad, ve kterém autor pracuje. V diplomové práci nebylo dovoleno městský úřad jmenovat, proto byl použit pouze obecný název bez nutnosti fiktivního pojmenování. V současné době zaměstnanci neskartují veškeré dokumenty, které obsahují citlivé informace. Dále zaměstnanci využívají pracovní e-mail nejen pro pracovní, ale i soukromé účely. U příchozích e-mailových zpráv zaměstnanci ne vždy prověřují odkazy, které e-mailové zprávy obsahují. Během pracovní doby zaměstnanci navštěvují webové stránky, které nesouvisí s jejich náplní práce. Při odchodu z kanceláře zaměstnanci neodhlašují počítač a nechávají na pracovním stole položené nosiče, které mohou obsahovat citlivé informace. Dále si zaměstnanci ukládají v počítači přístupové údaje a také si údaje s kolegy mezi sebou sdělují. Na základě tohoto současného stavu byly k aplikaci vybrány určité metody. Metody byly předem zkonzultovány a schváleny vedením městského úřadu. Zaměstnanci o této skutečnosti nebyli informováni. Z důvodu bezpečnosti a ochrany osobních údajů nebyla při aplikaci metod použita jména zaměstnanců. Zaměstnanci tak zůstali po celou dobu v anonymitě.

Vybrané metody byly aplikovány v reálných podmínkách. Pro aplikaci metod bylo potřeba zjistit jména zaměstnanců, jejich e-mailové adresy a telefonní čísla. Potřebné informace byly čerpány z oficiálních stránek městského úřadu.

5.1. Metoda phishing

Metoda phishing umožňuje získat citlivé informace (například uživatelská jména, hesla) za účelem zneužití. Pro aplikaci metody byl využit phishingový e-mail. Jednalo se o podvodnou e-mailovou zprávu, která byla rozeslána zaměstnancům městského úřadu. Phishingový e-mail obsahoval odkaz, který při jeho otevření přesměroval zaměstnance na vytvořenou podvodnou webovou stránku. Webhosting a název domény byly zvoleny tak, aby působily co nejdůvěryhodněji. Webová stránka měla

kromě nepatrných rozdílů podobu oficiální webové stránky. Jejich odlišnost umožnila zaměstnancům vyvolat podezření, že se jednalo o podvod. Rozdíly mezi stránkami jsou zobrazeny na obrázcích 22 a 23.

Obrázek 22: Pravá podoba webové stránky
Zdroj: VLASTNÍ ZPRACOVÁNÍ

Obrázek 23: Podvodná podoba webové stránky
Zdroj: VLASTNÍ ZPRACOVÁNÍ

Na podvodné webové stránce bylo zabudované počítadlo, které zaznamenávalo počet přístupů. Jestliže zaměstnanec vyplnil své přístupové údaje, bylo zaznamenáno pouze uživatelské jméno. Po vyplnění přístupových údajů byl

zaměstnanec přesměrován na webovou stránku, která obsahovala upozornění možné hrozby phishingového útoku. Upozornění je zobrazeno na obrázku 24.

Obrázek 24: Upozornění o možné hrozbě phishingového útoku

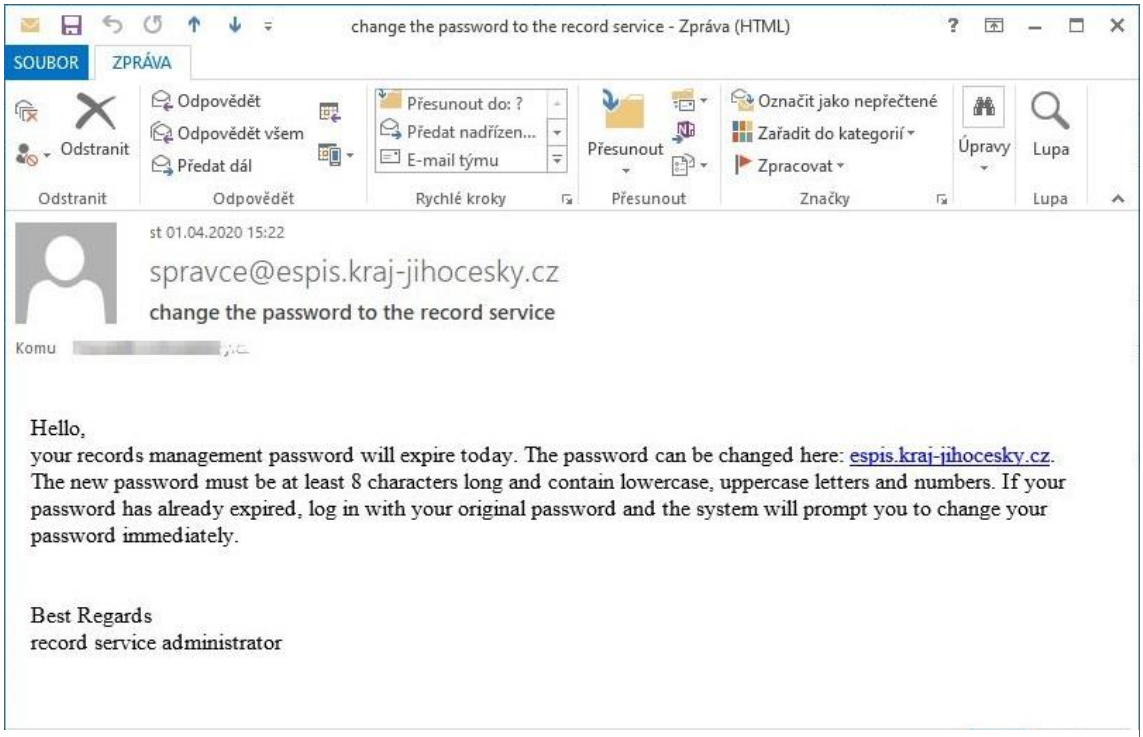
Zdroj: VLASTNÍ ZPRACOVÁNÍ

K rozeslání phishingového e-mailu zaměstnancům byl využit vlastní webhosting. Jako podvodná adresa odesílatele byla zvolena spravce@espis.kraj-jihocesky.cz. U adresy bylo důležité, aby působila na zaměstnance co nejdůvěryhodněji a nestalo se, že by příchozímu e-mailu nevěnovali žádnou pozornost a okamžitě ho smazali.

Obsahem phishingového e-mailu byla informace o vypršení platnosti přístupového hesla a jeho změně prostřednictvím přiloženého odkazu. Vzhledem k tomu, že se jednalo o změnu hesla u služby, kterou používají zaměstnanci, obsah e-mailu byl pro všechny stejný.

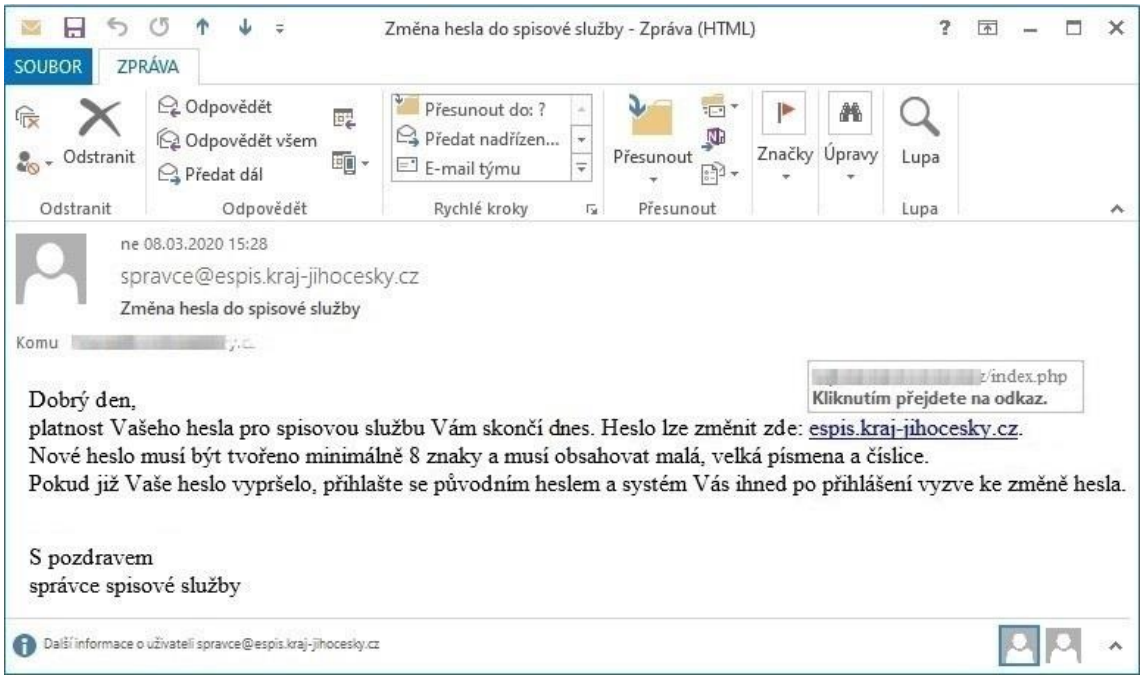
Phishingový e-mail byl vytvořen v různých variantách. Jednotlivé varianty e-mailu byly rozeslány postupně s odstupem jednoho týdne třiceti zaměstnancům, kteří ke své práci využívali počítač. Cílem bylo zneužít nevědomost zaměstnanců k získání citlivých informací.

Text u první varianty phishingového e-mailu (obrázek 25) byl napsaný v anglickém jazyce a neobsahoval žádné gramatické ani stylistické chyby.



Obrázek 25: První varianta phishingového e-mailu
Zdroj: VLASTNÍ ZPRACOVÁNÍ

U druhé varianty phishingového e-mailu (obrázek 26) byl text zprávy napsaný v českém jazyce bez gramatických a stylistických chyb.



Obrázek 26: Druhá varianta phishingového e-mailu
Zdroj: VLASTNÍ ZPRACOVÁNÍ

Text u třetí varianty phishingového e-mailu byl napsaný v českém jazyce, ale do textu byly záměrně zaneseny nápadné gramatické a stylistické chyby. Místy byl v textu záměrně zaměněn český výraz slova za slovenský. Čtvrtá varianta phishingového e-mailu obsahovala žádost o instalaci připojeného zazipovaného souboru z důvodu zvýšení zabezpečení. Text e-mailu byl napsaný v českém jazyce, neobsahoval gramatické ani stylistické chyby.

Fiktivní adresa odesílatele musela být u výše zmíněných čtyř variant e-mailu nepatrně pozměněna. Pokud by zaměstnancům přišlo více zpráv z jedné e-mailové adresy, mohlo by to v nich vyvolat podezření, že se jedná o podvod a obdržené e-mailové zprávy by si nemuseli více všímat.

U poslední páté varianty phishingového e-mailu byla zneužita e-mailová adresa IT technika městského úřadu. E-mailová adresa IT technika byla dostupná na oficiálních stránkách úřadu. Obsahem e-mailu byla prosba IT technika o ověření přístupových údajů zaměstnance v přiloženém odkaze.

5.2. Metoda baiting

Metoda baiting funguje na principu zanechání přenosného datového média tam, kde může zájmová osoba médium nalézt a použít. Cílem útoku je získat citlivé informace od zájmové osoby.

K aplikaci vybrané metody byla použita dvě přenosná datová média, USB flash disk a CD-ROM.

USB flash disk

Dříve bylo možné po vložení USB flash disku do počítače použít soubor autorun.inf, který dokázal například automaticky přesměrovat na vybranou webovou stránku nebo otevřít aplikaci. V současné době u operačního systému Windows 10 je v základním nastavení zakázané automatické načtení souboru autorun.inf. Vzhledem k tomu, že počítače městského úřadu měly nainstalovány operační systém Windows 10, nebylo možné tímto způsobem metodu aplikovat.

Metoda baiting byla aplikována pomocí tří USB flash disků. Z důvodu možného odhalení útoku byly USB flash disky ponechány během jednoho dne ve třech kancelářích zaměstnanců městského úřadu. Na každém USB flash disku byl vytvořen skript, který nesl název mzdy. Skript měl za úkol získat údaje o přihlášeném uživateli. Jestliže po vložení USB flash disku do počítače oběť spustila skript s názvem mzdy, došlo k získání uživatelského jména přihlášené osoby a jeho následnému odeslání na předem vytvořený server. Každý skript obsahoval jednorázový token, který se společně s uživatelským jménem odeslal a sloužil jako pojistka, která by v případě odhalení zabránila možnému zahlcení serveru množstvím nežádoucích dat.

CD-ROM

Pro aplikaci metody baiting prostřednictvím CD-ROM nosiče bylo potřeba nejprve vymyslet název, který by u zaměstnanců městského úřadu vzbudil pozornost. Vzhledem k tomu, že byly k aplikování metody použity dva CD-ROM nosiče, byly pro nosiče vybrány dva názvy, Firemní večírek 2019 – fotky a Mzdy 2020. Na oba nosiče byl pomocí počítače vypálen skript.

Jestliže po vložení CD-ROM nosiče do počítače oběť spustila skript s názvem mzdy nebo firemni_vecirek, došlo k automatickému otevření webové stránky a získání uživatelského jména přihlášené osoby. Uživatelské jméno bylo následně odesláno na předem vytvořený server. Na webové stránce bylo poučení o sociálním inženýrství a zabudované počítadlo, které zaznamenávalo počet přístupů na webovou stránku.

Důležité bylo pro nosiče vymyslet vhodné místo k umístění. Jelikož městský úřad navštěvovala široká veřejnost a aplikace metody byla směřována výhradně na zaměstnance městského úřadu, nebylo možné umístit CD-ROM nosiče na chodbu. Jediným možným místem, kam neměla přístup široká veřejnost, byly místnosti vyhrazené pouze pro zaměstnance městského úřadu. První místnost se nacházela v přízemí, druhá místnost se nacházela v prvním patře budovy. CD-ROM nosiče byly jedenkrát v průběhu týdne ponechány v jedné ze dvou místností. Místnost v přízemí byla využita k umístění CD-ROM nosiče s názvem Mzdy 2020. Nosič s názvem

Firemní večírek 2019 – fotky byl umístěn do místnosti v prvním patře budovy. Útok byl po čtrnácti dnech ještě jednou zopakován s opačným umístěním CD-ROM nosičů.

5.3. Metoda pretexting

Pretexting spočívá v získávání citlivých informací pomocí předem vymyšleného scénáře. Je důležité, aby oběť vymyšlenému scénáři uvěřila a dobrovolně poskytla potřebné informace.

Pro aplikaci metody byla oslovena osoba, která měla za úkol sehrát roli útočníka. Při výběru osoby bylo důležité, aby byla pro všechny zaměstnance městského úřadu neznámá. Před aplikací metody byl vytvořen možný scénář, díky kterému se měl pokusit útočník získat od zaměstnance citlivé informace. Úkolem útočníka bylo jít v době nepřítomnosti IT technika na ekonomické oddělení a vydávat se za servisního technika účetního programu. Na začátku rozhovoru se útočník zaměstnanci představil jako servisní technik, který měl s IT technikem domluvenou kontrolu programu. Útočník po zaměstnanci požadoval přístupové údaje pro vstup do programu. Během rozhovoru se útočník snažil u zaměstnance vyvolat pocit důvěry tím, že se choval přátelsky, profesionálně a nevykazoval známky nervozity.

5.4. Metoda vishing

Metoda vishing představuje získávání citlivých informací prostřednictvím telefonického rozhovoru se zájmovou osobou. V současné době je metoda stále více využívána.

Pro aplikování metody bylo náhodně vybráno dvanáct zaměstnanců městského úřadu. Kontakt na zaměstnance byl veřejně dostupný na oficiálních webových stránkách městského úřadu. Pro aplikování metody byla potřeba předplacená karta s telefonním číslem, které bylo pro zaměstnance městského úřadu neznámé. Také byla důležitá příprava na samotný telefonický rozhovor. Byl dopředu sepsán přibližný scénář, jakým směrem se měl rozhovor ubírat. Na začátku každého telefonického rozhovoru s jedním ze zaměstnanců úřadu se volaný představil jako administrátor spisové služby. Důvodem volání byla žádost o pomoc. Kvůli předstírané interní chybě potřeboval spolupráci zaměstnance pro uvedení spisové

služby do původního stavu. Administrátor potřeboval od zaměstnance zjistit, zda je schopen přihlásit se do spisové služby. Když zaměstnanec zjistil, že s přihlášením do spisové služby není problém, administrátor předstíral, že přihlášení nevidí a poprosil zaměstnance, zda by mohl ověřit přihlášení u sebe. Poprosil tedy zaměstnance o přístupové údaje.

Všechny telefonní rozhovory byly cíleně uskutečněny během jednoho měsíce, a to vždy před polední přestávkou, kdy se zaměstnanci snažili rozhovory uspíšit a vyřešit co nejrychleji. Cílem bylo během telefonních rozhovorů získat od zaměstnanců jejich přístupové údaje.

5.5. Metoda smishing

Metoda smishing funguje na principu rozesílání podvodných SMS zpráv za účelem získání citlivých informací od zájmových osob.

K aplikaci vybrané metody byla potřeba předplacená karta s telefonním číslem, které nikdo ze zaměstnanců městského úřadu neznal. Z předplacené karty byla prostřednictvím mobilního telefonu hromadně rozeslána SMS zpráva. Zpráva byla adresována osmi zaměstnancům, kteří měli k dispozici služební mobilní telefon. Jejich čísla byla veřejně dostupná na oficiálních webových stránkách městského úřadu. Obsahem SMS zprávy byl odkaz s průvodním textem, který informoval, že z důvodu zvýšení bezpečnosti spisové služby bylo nově potřeba vyplnit telefonní číslo v uživatelském účtu zaměstnance. Pro přihlášení do uživatelského účtu bylo potřeba otevřít odkaz a vyplnit přístupové údaje. Jestliže zaměstnanec odkaz otevřel, byl přesměrován na podvodnou webovou stránku, která měla zabudované počítadlo přístupů. V případě vyplnění přístupových údajů bylo zaznamenáno uživatelské jméno.

5.6. Metoda trashing

Metoda sociálního inženýrství představuje prohledávání kontejnerů s odpadem pro získání potřebných informací.

Metoda trashing byla aplikována během jednoho týdne. Cílem aplikace metody bylo nalézt dokumenty s citlivými informacemi. Kontejnery byly umístěny za budovou městského úřadu, kde se v blízkosti nacházel prostor vyhrazený pro kouření. Na začátku týdne bylo potřeba zjistit, kdy se poblíž kontejneru nikdo nevyskytoval. Vzhledem k tomu, že se zaměstnanci městského úřadu stravovali každý den o polední pauze mimo budovu, byla aplikace metody provedena v tomto čase.

Analýza výsledků aplikace vybraných metod

Jednou z aplikovaných metod sociálního inženýrství byla metoda phishing. Phishingový e-mail byl vytvořen v různých variantách, které byly rozeslány třiceti zaměstnancům městského úřadu. Součástí e-mailu byl odkaz, který přesměroval zaměstnance na podvodnou webovou stránku. Text první varianty e-mailu byl v anglickém jazyce bez gramatických a stylistických chyb. Útok byl neúspěšný, jelikož nebyl zaznamenán žádný přístup na podvodnou webovou stránku. Důvodem neúspěchu mohl být text e-mailu, který byl napsaný v anglickém jazyce. U druhé varianty phishingového e-mailu byl text napsaný v českém jazyce bez gramatických a stylistických chyb. Útok byl úspěšný, protože u osmi zaměstnanců nevyvolal e-mail podezření, že se jednalo o podvod a prostřednictvím přiloženého odkazu podvodnou webovou stránku zobrazili. Na zobrazené stránce vyplnilo přístupové údaje šest zaměstnanců. U třetí varianty phishingového e-mailu byl útok neúspěšný. V českém textu byly úmyslně zaneseny nápadné gramatické a stylistické chyby. Nápadné chyby mohly být důvodem, proč u žádného zaměstnance nedošlo k zobrazení podvodné webové stránky. Čtvrtá varianta phishingového e-mailu obsahovala žádost o instalaci připojeného souboru. Vzhledem k tomu, že nedošlo ani jednou ke spuštění souboru, útok byl neúspěšný. Důvodem neúspěchu mohla být medializace tohoto typu útoku. U páté varianty phishingového e-mailu byla zneužita e-mailová adresa IT technika. Obsahem e-mailu byla prosba IT technika o ověření přístupových údajů zaměstnance prostřednictvím přiloženého odkazu. Přes přiložený odkaz zobrazilo podvodnou webovou stránku šestnáct zaměstnanců. Útok byl úspěšný, jelikož u sedmi z šestnácti zaměstnanců došlo k vyplnění přístupových údajů. Přehled výše zmíněných výsledků variant phishingového e-mailu je znázorněn v tabulce 1.

Phishingový e-mail	Počet zaměstnanců, kteří vyplnili přístupové údaje	Hodnocení útoku
První varianta	žádný	neúspěšný
Druhá varianta	šest	úspěšný
Třetí varianta	žádný	neúspěšný
Čtvrtá varianta	žádný	neúspěšný
Pátá varianta	sedm	úspěšný

Tabulka 1: Přehled výsledků variant phishingového e-mailu
Zdroj: VLASTNÍ ZPRACOVÁNÍ

Další aplikovanou metodou byla metoda baiting. Pro tuto metodu byla využita dvě přenosná datová média, USB flash disk a CD-ROM. K realizaci útoku byly potřeba tři USB flash disky a dva CD-ROM nosiče. USB flash disky byly ponechány v jeden den ve třech kancelářích zaměstnanců městského úřadu. Útok prostřednictvím USB flash disků byl neúspěšný, protože na vytvořeném serveru nebylo zaznamenáno žádné uživatelské jméno a všechny USB flash disky byly odevzdány IT technikovi. CD-ROM nosiče byly jedenkrát v průběhu týdne ponechány v jedné ze dvou místností určené pouze pro zaměstnance. Po čtrnácti dnech byl útok ještě jednou zopakován. Útok prostřednictvím CD-ROM nosiče, který nesl název Mzdy 2020, byl neúspěšný, protože nebyl na webové stránce zaznamenán žádný přístup. Druhý CD-ROM nosič nesl název Firemní večírek 2019 – fotky. Jelikož na vytvořeném serveru bylo zaznamenáno jedno uživatelské jméno, útok byl úspěšný.

Aplikaci metody pretexting předcházelo vytvoření scénáře, díky kterému měl útočník získat od zaměstnance městského úřadu citlivé informace. Úkolem útočníka bylo jít na ekonomické oddělení a vydávat se za servisního technika účetního programu. Útočník po zaměstnanci požadoval přístupové údaje pro vstup do programu. Útok byl úspěšný, jelikož zaměstnanec při rozhovoru s útočníkem nepojal podezření podvodného jednání a požadované přístupové údaje útočníkovi sdělil.

K útoku sociálního inženýrství byla využita metoda vishing. Pro aplikování metody bylo náhodně vybráno dvanáct zaměstnanců městského úřadu. Útočník se v telefonním rozhovoru pokaždé vydával za administrátora spisové služby.

Důvodem volání bylo zjistit, zda je zaměstnanec schopen přihlásit se do spisové služby. Provedený útok byl úspěšný, protože čtyři zaměstnanci útočníkovi do telefonu sdělili přístupové údaje. Šest zaměstnanců přístupové údaje nesdělilo, ale bylo ochotno přepojit hovor na IT oddělení. Zbylí dva zaměstnanci na žádost o pomoc odpověděli, že přístupové údaje neznají, protože se přihlašují automaticky.

Další aplikovanou metodou byla metoda smishing. SMS zpráva byla hromadně rozeslána osmi zaměstnancům městského úřadu. Obsahem SMS zprávy byl odkaz se žádostí o doplnění telefonního čísla v uživatelském účtu spisové služby. Útok pomocí metody byl neúspěšný, jelikož na podvodné webové stránce nedošlo k vyplnění přístupových údajů do uživatelského účtu. Neúspěch mohlo zapříčinit časté varování před takovýmto typem útoku. Z tohoto důvodu nebyla vytvořena další varianta SMS zprávy. S největší pravděpodobností by vedla ke stejnému výsledku. Mnoho lidí je díky častým varováním opatrnější.

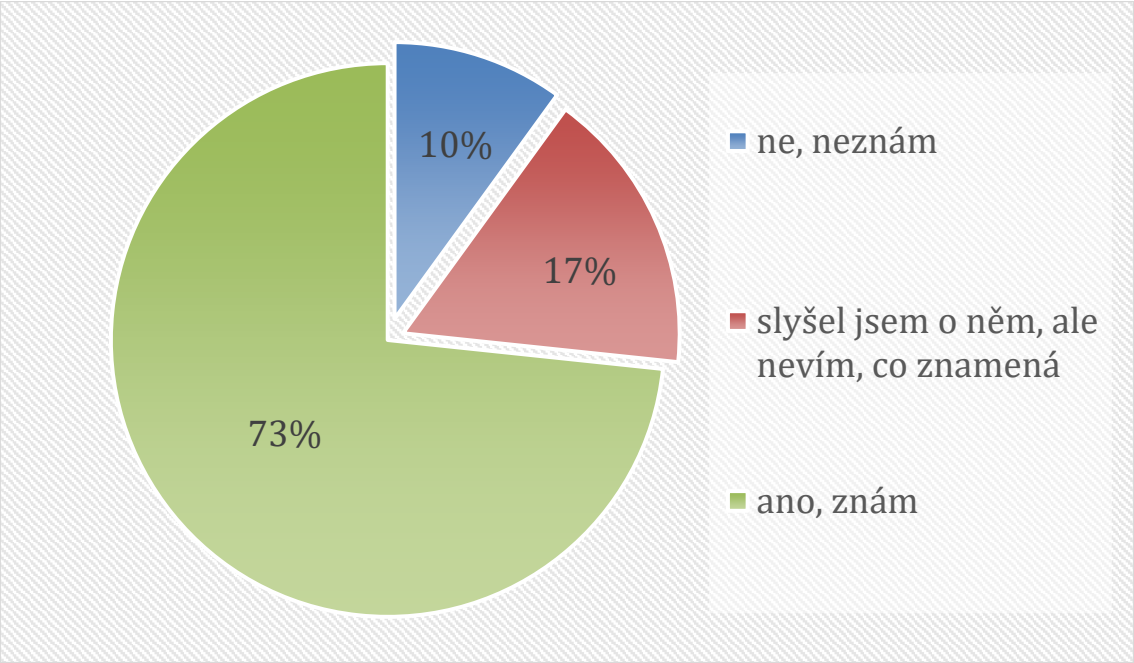
Poslední aplikovanou metodou byla metoda trashing. Cílem bylo nalézt dokumenty s citlivými informacemi. Při prohledání kontejnerů bylo zjištěno, že zaměstnanci městského úřadu veškeré dokumenty s citlivými informacemi neskartují. Útok byl úspěšný, protože byl v kontejneru nalezen například telefonní seznam se soukromými čísly zaměstnanců nebo utržený kus papíru, na kterém byly napsané přístupové údaje.

6. Dotazník na téma Sociální inženýrství

Existuje několik způsobů, jak prozkoumat znalost lidí v konkrétní problematice. V rámci diplomové práce byl vytvořen dotazník na téma Sociální inženýrství, jehož cílem bylo prozkoumat znalost zaměstnanců městského úřadu v této oblasti. Dotazník byl vytvořen pomocí volně dostupného Google formuláře. V úvodu vytvořeného dotazníku byli zaměstnanci informováni, pro jaký účel budou jejich odpovědi využity a jak s nimi bude naloženo. Po aplikaci vybraných metod útoků sociálního inženýrství byl dotazník rozeslán třiceti zaměstnancům, kteří ke své práci využívali počítač. Dotazník byl rozeslán na jejich pracovní e-mailové adresy.

Dotazník vyplnilo všech třicet zaměstnanců. Vyhodnocení jednotlivých otázek dotazníku je níže popsáno a znázorněno pomocí výsečových grafů. Odpovědi jsou uvedeny v procentech.

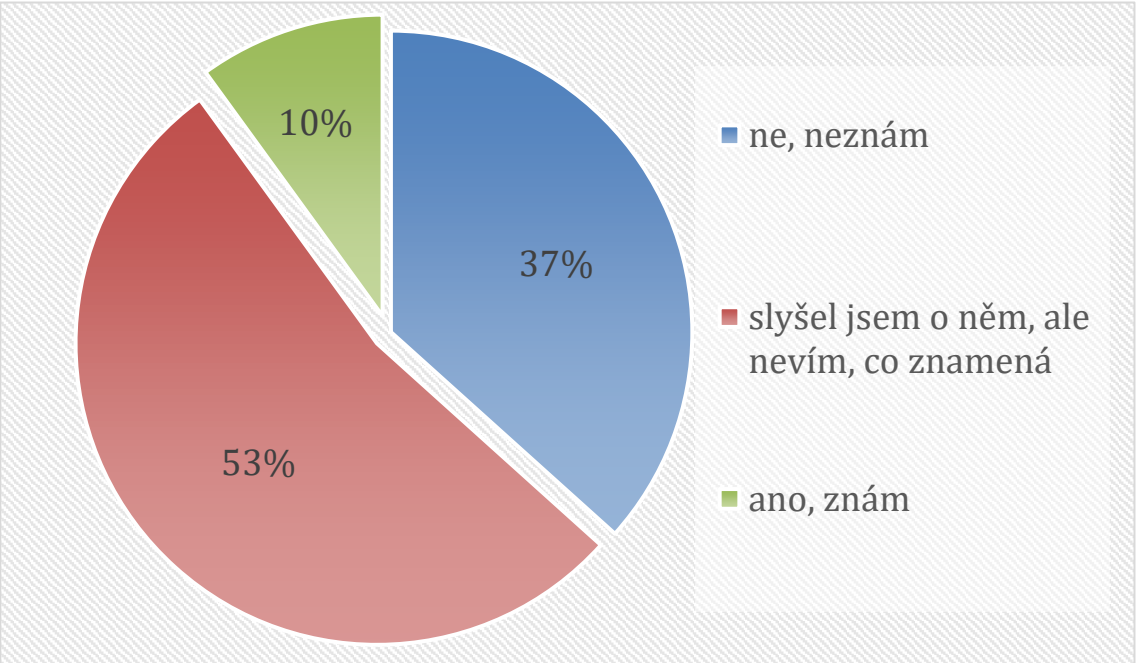
Otázka č. 1: Znáte pojem sociální inženýrství?



Graf 1: Vyhodnocení odpovědí k otázce č. 1

Úkolem otázky č. 1 bylo zjistit, jestli je zaměstnancům známý pojem sociální inženýrství. Na základě odpovědí bylo zjištěno, že 73 % zaměstnanců pojem zná. Dalších 17 % zaměstnanců odpovědělo, že pojem slyšelo, ale neví, co znamená. Zbylých 10 % zaměstnanců odpovědělo, že pojem neznají.

Otázka č. 2: Znáte pojem phishing?

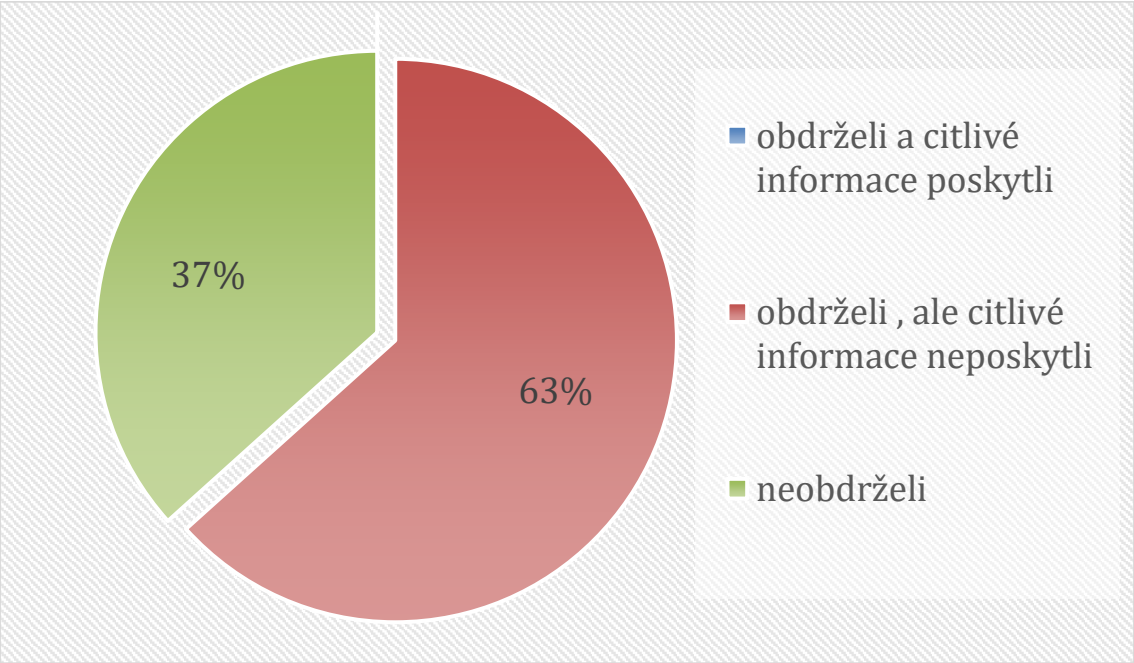


Graf 2: Vyhodnocení odpovědí otázky č. 2

Otázka č. 2 byla zaměřena na znalost zaměstnanců pojmu phishing. Z odpovědí v dotazníku vyplynulo, že více než polovina zaměstnanců o pojmu slyšela, ale neví, co znamená. Dalších 37 % zaměstnanců odpovědělo, že pojem nezná a zbylých 10 % zaměstnanců odpovědělo, že pojem znají.

Metoda phishing patří mezi jednu z nejčastěji využívaných metod útoku. Přesto si většina zaměstnanců pod pojmem phishing nepředstaví podvodný e-mail, který se snaží získat citlivé informace.

Otázka č. 3: Obdrželi jste někdy e-mail, který se od Vás pokusil získat citlivé informace?

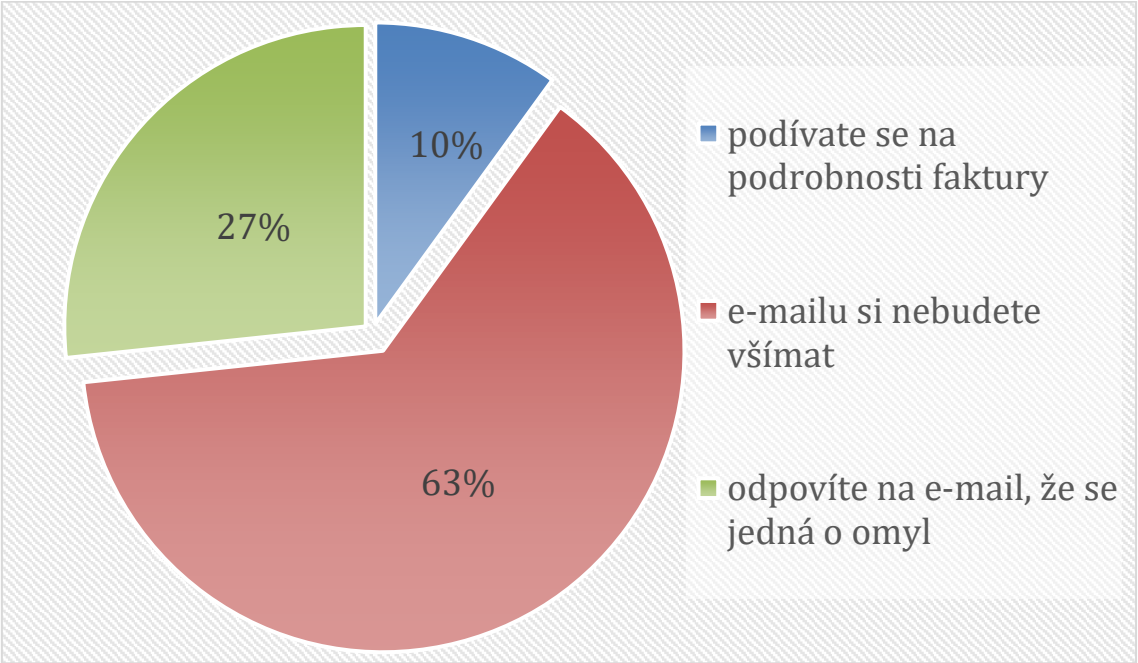


Graf 3: Vyhodnocení odpovědí otázky č. 3

Otázka č. 3 měla zjistit, jestli zaměstnanci někdy obdrželi e-mail, který se od nich pokusil získat citlivé informace. Z odpovědí bylo zjištěno, že 63 % zaměstnanců e-mail obdrželo, ale citlivé informace neposkytlo. Dále bylo zjištěno, že 37 % zaměstnanců e-mail požadující citlivé informace nikdy neobdrželo. Odpověď, že e-mail obdrželi a citlivé informace poskytli, nezvolil žádný zaměstnanec.

Z odpovědí v dotazníku vyplývá, že více než polovina zaměstnanců je schopna podvodný e-mail odhalit a zabránit úniku citlivých informací. Vzhledem k tomu, že jsou útoky promyšlenější a propracovanější, zaměstnanci, kteří odpověděli, že e-mail požadující citlivé informace neobdrželi, nemuseli poznat, že se stali obětí útoku.

Otázka č. 4: Přijde Vám prostřednictvím e-mailu faktura za službu, kterou jste si neobjednali. Co uděláte?

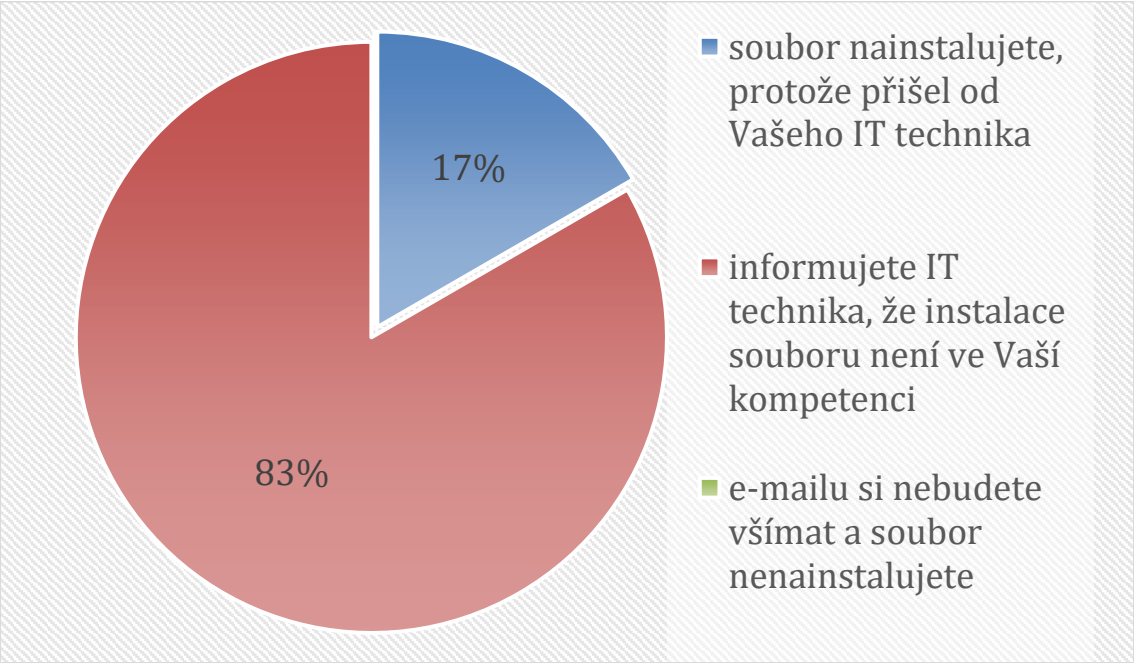


Graf 4: Vyhodnocení odpovědí otázky č. 4

Otázka č. 4 byla zaměřena na reakci zaměstnanců, jak by se zachovali při obdržení faktury za službu, kterou si neobjednali. Na základě odpovědí vyplynulo, že 63 % zaměstnanců by si e-mailu nevšímalo. Dalších 27 % zaměstnanců by na příchozí e-mail odepsalo, že se jedná o omyl. Zbylých 10 % zaměstnanců by se podívalo na podrobnosti faktury.

Z odpovědí vyplývá, že více než polovina zaměstnanců by v případě útoku zabránila úniku citlivých informací. Část zaměstnanců by odpověděla na e-mail, že se jedná o omyl, přitom na většinu podvodných e-mailů odpovědět nelze. Cílem e-mailu útočníka není získat odpověď, ale otevření přílohy. U zaměstnanců, kteří by se podívali na podrobnosti faktury, by v případě útoku došlo k úniku citlivých informací. Zaslaná příloha může obsahovat spustitelný kód, který odcizí například citlivé informace.

Otázka č. 5: Od Vašeho IT technika obdržíte e-mail s přílohou, která obsahuje zazipovaný soubor. V e-mailu prosí o instalaci přiloženého souboru. Jak se zachováte?

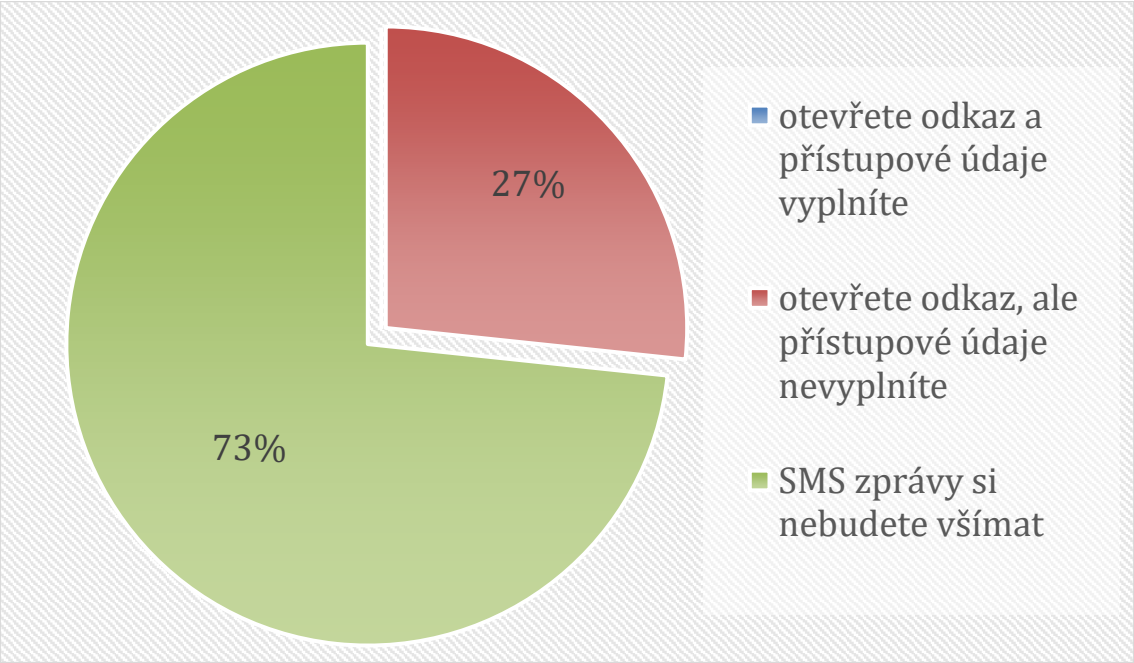


Graf 5: Vyhodnocení odpovědí otázky č. 5

Cílem otázky č. 5 bylo zjistit reakci zaměstnanců na příchozí e-mail od IT technika. Z odpovědí bylo zjištěno, že 83 % zaměstnanců by informovalo IT technika, že instalace souboru není v jejich kompetenci. Zbylých 17 % by soubor nainstalovalo, protože je o to požádal IT technik. Odpověď, že e-mailu si nebudete všímat a soubor nenainstalujete, nezvolil žádný zaměstnanec.

Vzhledem k tomu, že by většina zaměstnanců informovala IT technika, že instalace souboru není v jejich kompetenci, IT technik by se mohl dozvědět o možném útoku dříve, než by mohlo dojít k úniku citlivých informací. U ostatních zaměstnanců by v případě útoku došlo k úniku citlivých informací. Zaměstnanci by si neověřili, že obdržená e-mailová zpráva byla skutečně od IT technika.

Otázka č. 6: Přijde Vám SMS zpráva, která informuje o nutnosti ověření Vašich údajů uvedených u bankovního účtu. V SMS zprávě bude přiložen odkaz pro přihlášení do účtu. Jak se zachováte?

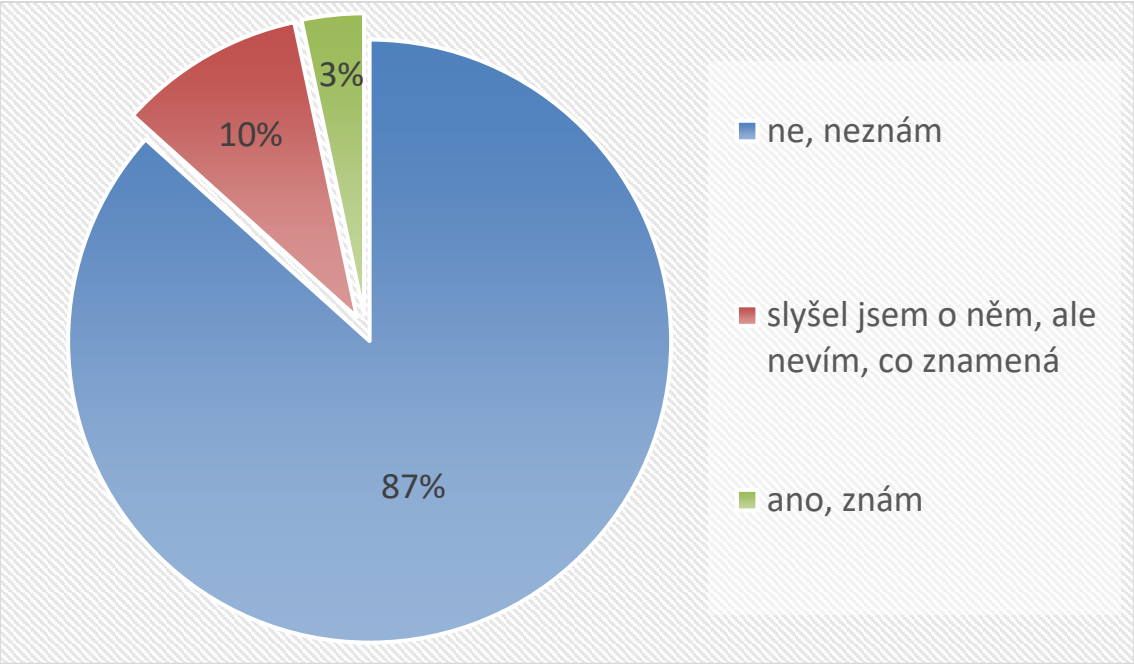


Graf 6: Vyhodnocení odpovědí otázky č. 6

Otázka č. 6 měla zjistit, jak by se zaměstnanci zachovali v případě obdržení SMS zprávy se žádostí o ověření údajů uvedených u bankovního účtu. Na základě odpovědí bylo zjištěno, že 73 % zaměstnanců by si SMS zprávy nevšímalo. Dalších 27 % zaměstnanců by otevřelo odkaz, ale přístupové údaje nevyplnilo. Mezi zaměstnanci nebyl nikdo, kdo by otevřel odkaz a vyplnil přístupové údaje.

Z odpovědí v dotazníku bylo zjištěno, že by v případě útoku prostřednictvím SMS zprávy většina zaměstnanců útok odrazila a zabránila úniku citlivých informací. Zaměstnanci, kteří odkaz otevřeli, ale přístupové údaje nevyplnili, by se v případě útoku mohli stát obětí. K infikování mobilního telefonu může dojít při pouhém otevření webové stránky pomocí přiloženého odkazu.

Otázka č. 7: Znáte pojem baiting?

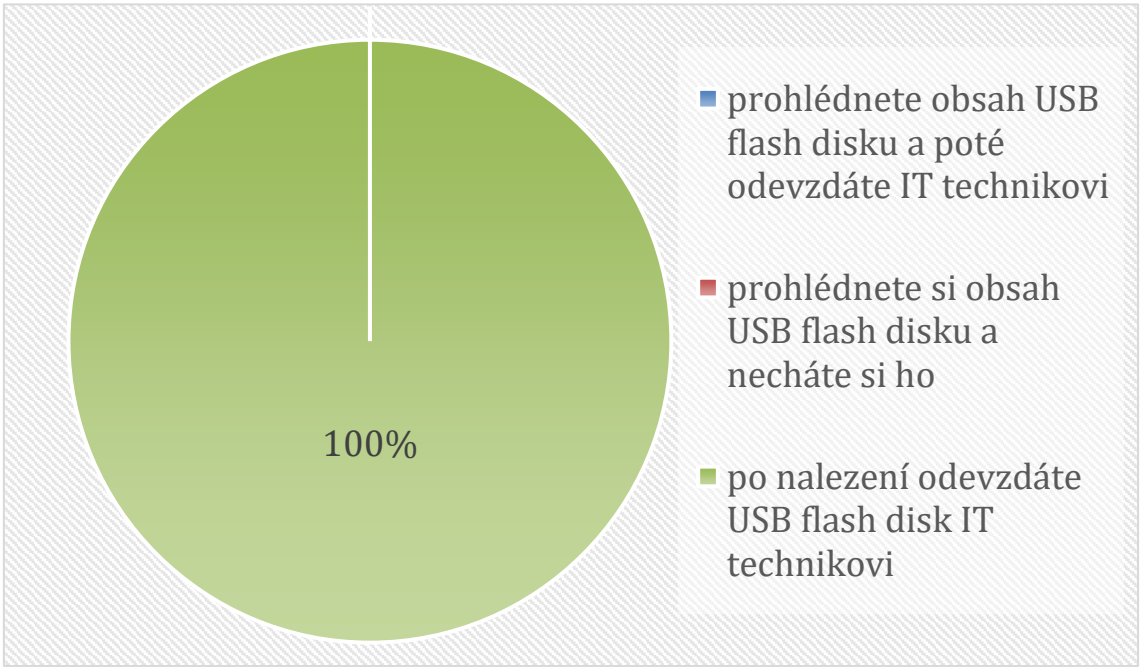


Graf 7: Vyhodnocení odpovědí otázky č. 7

Otázka č. 7 měla prověřit, jestli zaměstnanci znají pojem baiting. Z odpovědí vyplynulo, že pro 87 % zaměstnanců je pojem neznámý. Dalších 10 % zaměstnanců odpovědělo, že pojem slyšeli, ale neví, co znamená. Pouze u 3 % zaměstnanců byla zvolena odpověď, že pojem baiting znají.

Z odpovědi v dotazníku vyplývá, že převážná většina zaměstnanců pojem baiting nezná a ani o pojmu neslyšela.

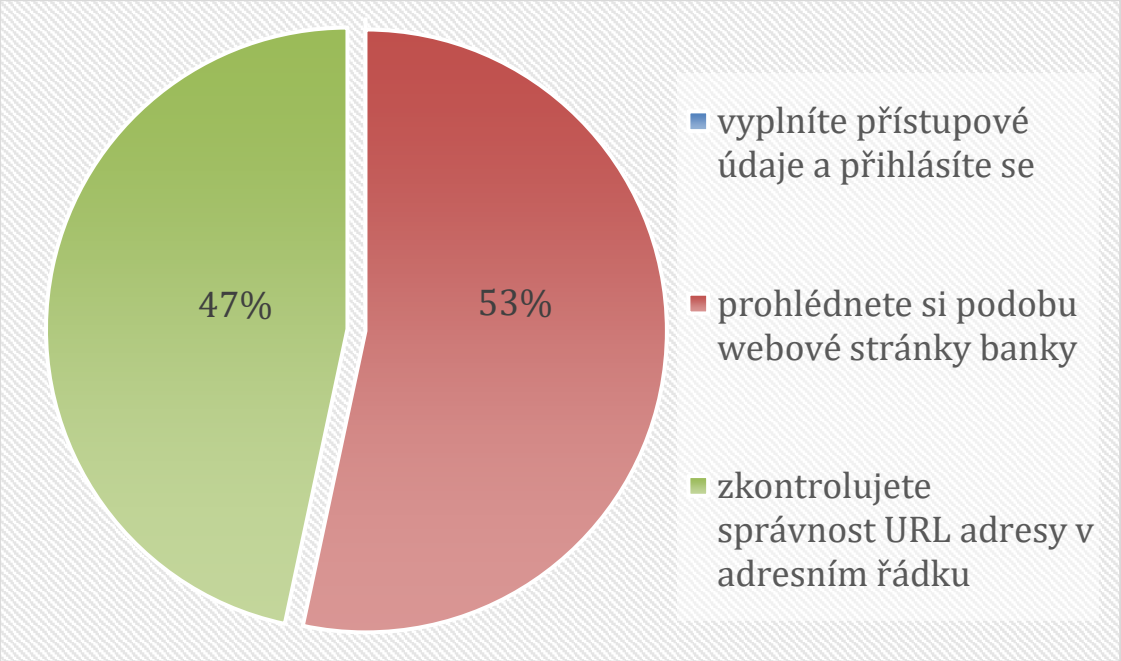
Otázka č. 8: V budově městského úřadu naleznete neznámý USB flash disk. Co s ním uděláte?



Graf 8: Vyhodnocení odpovědí otázky č. 8

Otázka č. 8 byla zaměřena na reakci zaměstnanců při nálezu neznámého USB flash disku. Na základě odpovědí zaměstnanců bylo zjištěno, že v případě nálezu neznámého USB flash disku by všichni zaměstnanci USB flash disk odevzdali IT technikovi, aniž by si prohlédli jeho obsah. Mezi zaměstnanci se nenašel nikdo, kdo by si v případě nálezu neznámého USB flash disku prohlédl jeho obsah nebo by si USB flash disk ponechal.

Otázka č. 9: Webovou stránku Vašeho internetového bankovnictví navštívíte prostřednictvím odkazu obsaženého ve zprávě. Jak se zachováte?

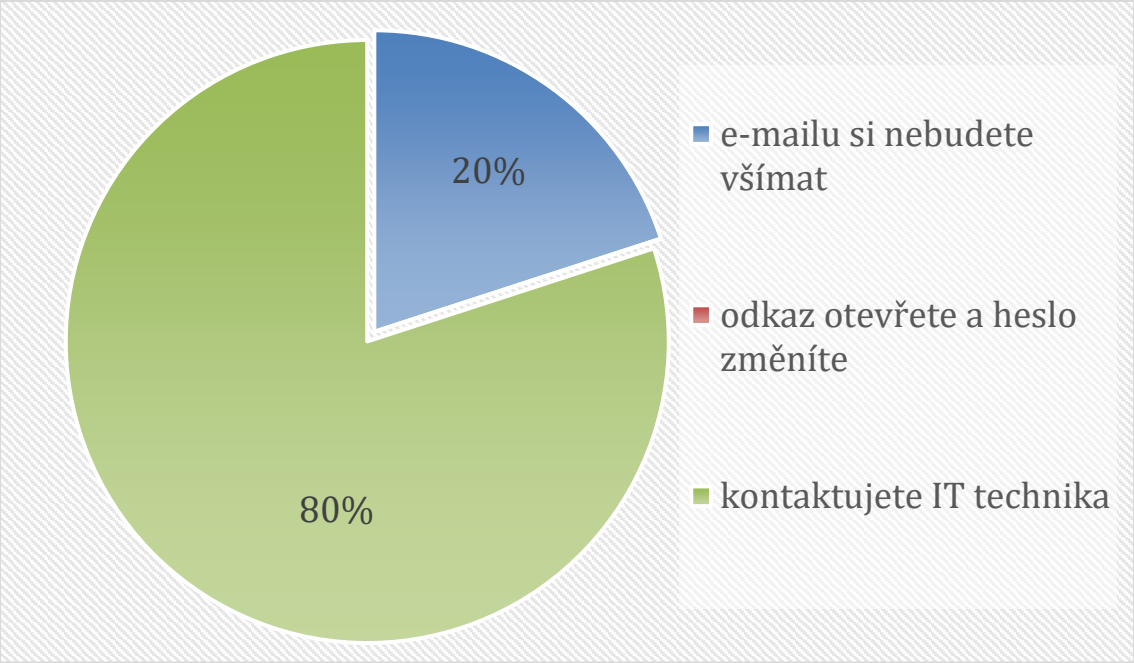


Graf 9: Vyhodnocení odpovědí otázky č. 9

Úkolem otázky č. 9 bylo zjistit, jak by se zaměstnanci zachovali v případě zobrazení webové stránky bankovnictví prostřednictvím odkazu přiloženého ve zprávě. Z odpovědí vyplynulo, že 53 % zaměstnanců by si prohlédlo podobu webové stránky banky. Ostatních 47 % zaměstnanců by zkontrolovalo správnost URL adresy v adresním řádku.

V současné době je velmi obtížné na první pohled rozpoznat podvodnou webovou stránku od stránky oficiální. Základem úspěšného útoku je vytvořit podvodnou webovou stránku, která je od originálu téměř k nerozeznání. Zaměstnanci, kteří by si pouze prohlédli podobu webové stránky banky, by se v případě útoku mohli stát obětí. Tento způsob ověření důvěryhodnosti webové stránky je v současné době nedostatečný. Pro rozpoznání podvodné webové stránky od stránky oficiální je nutné zkontrolovat správnost URL adresy v adresním řádku internetového prohlížeče.

Otázka č. 10: Obdržíte e-mail, který Vás žádá o změnu hesla do spisové služby z důvodu vypršení platnosti. E-mail byl zaslán z legitimní e-mailové adresy. Obsahem e-mailu je odkaz, přes který je možné změnit heslo. Jak se zachováte?

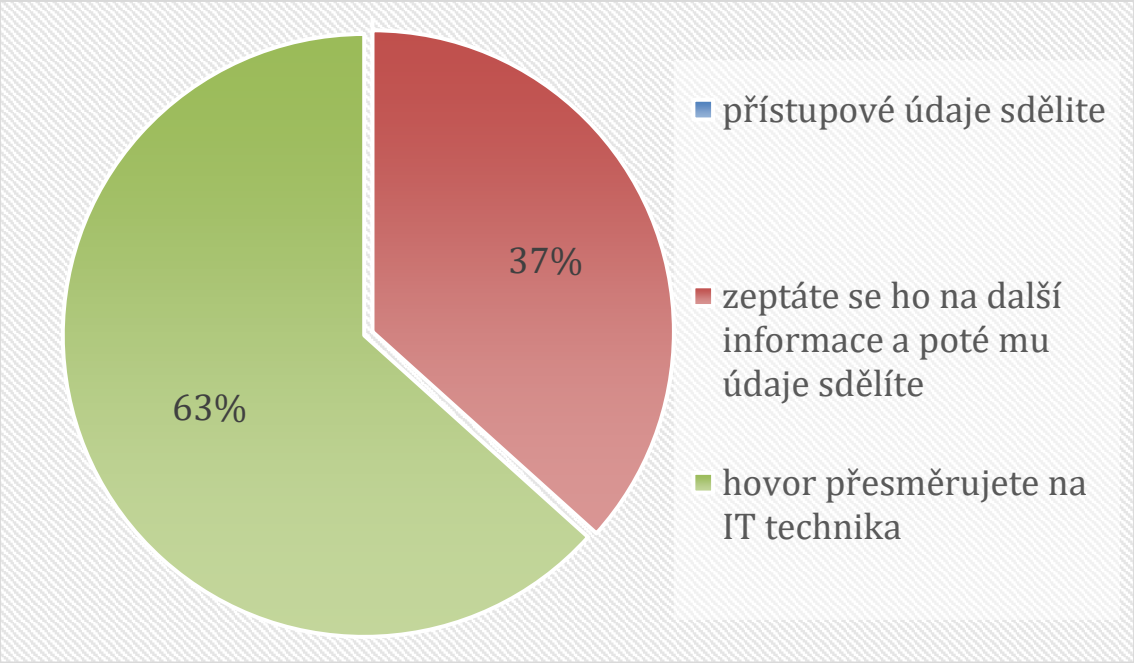


Graf 10: Vyhodnocení odpovědí otázky č. 10

Otázka č. 10 měla zjistit, jak by se zaměstnanci zachovali v případě obdržení e-mailové zprávy, která žádá o změnu hesla do spisové služby prostřednictvím odkazu. Na základě odpovědí bylo zjištěno, že 80 % zaměstnanců by kontaktovalo IT technika. Odpověď, že e-mailu by si nevšímali, zvolilo 20 % zaměstnanců. Mezi zaměstnanci nebyl nikdo, kdo by otevřel přiložený odkaz a změnil heslo.

Z odpovědí v dotazníku vyplynulo, že více než polovina zaměstnanců by informovala IT technika o příchozím e-mailu žádající změnu hesla. V tomto případě by mohl IT technik možný útok odvrátit a zabránit úniku citlivých informací. Díky správné reakci zaměstnanců by mohl IT technik včas varovat před možným útokem i ostatní zaměstnance. Zaměstnanci, kteří by si e-mailu nevšímali, by také v případě útoku zabránili úniku citlivých informací. Může ovšem nastat situace, kdy půjde o skutečný požadavek o změnu hesla. V tomto případě by spisová služba zaměstnance nejspíše opět kontaktovala.

Otázka č. 11: Zavolá Vám člověk, který má na starost provoz služby, kterou ke své práci využíváte. Kvůli interní chybě nastal problém s Vaším účtem. Pro ověření funkčnosti žádá o přístupové údaje do služby. Jak zareagujete?

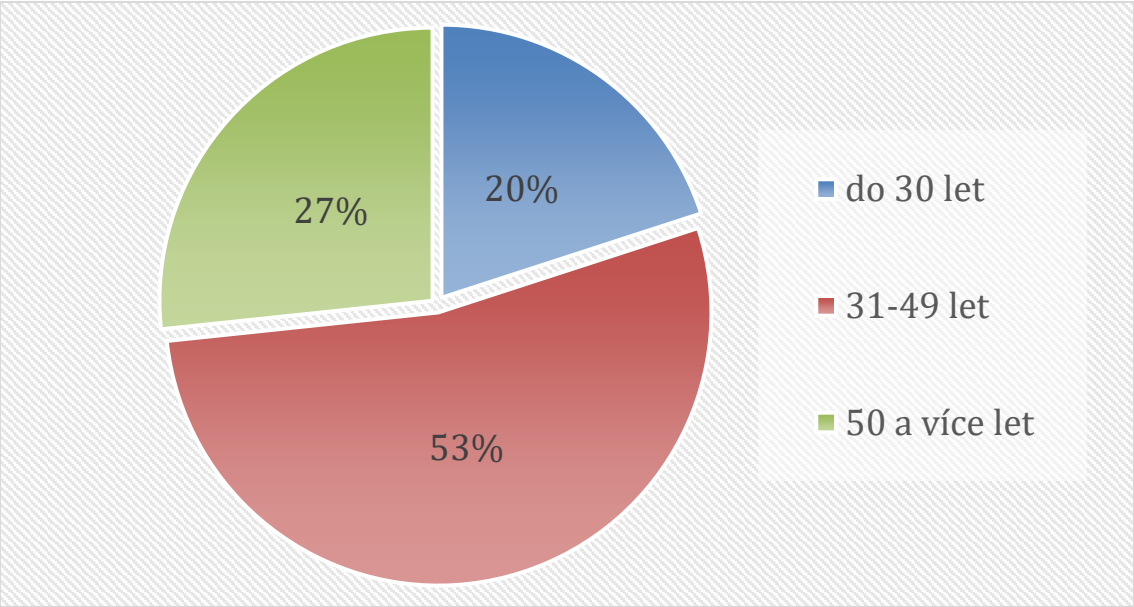


Graf 11: Vyhodnocení odpovědí otázky č. 11

Otázka č. 11 byla zaměřena na reakci zaměstnanců v případě telefonního rozhovoru s pracovníkem služby, který žádal o sdělení přístupových údajů pro ověření funkčnosti služby. Na základě odpovědí v dotazníku bylo zjištěno, že 63 % zaměstnanců by přesměrovalo hovor na IT technika. Zbylých 37 % zaměstnanců by se pracovníka služby zeptalo na další informace a poté by mu údaje sdělilo. Dále bylo zjištěno, že mezi zaměstnanci nebyl nikdo, kdo by na základě telefonního rozhovoru přístupové údaje sdělil, aniž by požadoval od volajícího více informací.

Vzhledem k tomu, že funkčnost služeb a programů na městském úřadě má na starost výhradně IT technik, zaměstnanci by v případě útoku zareagovali správně, když by hovor přesměrovali na IT technika. Zaměstnanci, kteří by se zeptali na další informace a poté volajícímu údaje sdělili, by se v případě útoku mohli stát obětí. Útočník před samotným útokem shromažďuje dostatek informací, aby oběť neměla šanci útočníka odhalit.

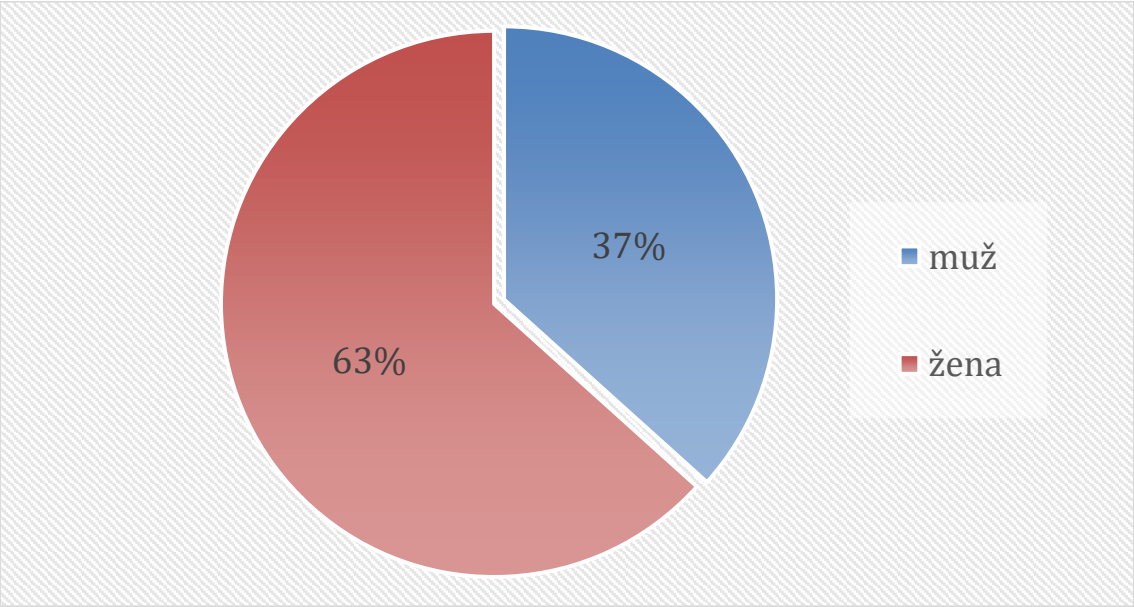
Otázka č. 12: Jaký je Váš věk?



Graf 12: Vyhodnocení odpovědí otázky č. 12

U otázky č. 12 bylo zjištěno, v jakém věkovém rozmezí se dotazovaní zaměstnanci nacházeli. Nejvyšší podíl zaměstnanců byl ve věkovém rozmezí 31-49 let, jednalo se o 53 % zaměstnanců. Ve věku do 30 let se nacházelo 20 % zaměstnanců. Ostatních 27 % zaměstnanců se nacházelo ve věku 50 a více let.

Otázka č. 13: Jaké je Vaše pohlaví?



Graf 13: Vyhodnocení odpovědí otázky č. 13

Otázka č. 13 měla zjistit zastoupení pohlaví mezi dotazovanými zaměstnanci. Z odpovědí bylo zjištěno, že mezi zaměstnanci převládal počet žen. Podíl žen představoval 63 % zaměstnanců, podíl mužů představoval 37 %.

Výsledky dotazníku mohou vzbuzovat otázku k zamyšlení, zda zaměstnanci problematiku sociálního inženýrství znají nebo do jaké míry se v problematice skutečně orientují. Tato otázka zůstane bohužel nezodpovězena.

Porovnání výsledků dotazníku s výsledky aplikace vybraných metod

V porovnání výsledků dotazníku s výsledky aplikace vybraných metod bylo zjištěno, že některé odpovědi zaměstnanců městského úřadu se neztotožňovaly s jejich reakcí na zrealizovaný útok sociálního inženýrství.

metoda baiting

Výsledkem aplikace metody baiting bylo odevzdání všech nalezených USB flash disků, které byly použity k realizaci útoku, IT technikovi. Výsledkem dotazníku byla jednotná odpověď všech zaměstnanců, že by v případě nálezu neznámého USB flash disku odevzdali nalezený USB flash disk IT technikovi. Při porovnání výsledků aplikace metody s výsledky dotazníku byla zaznamenána shoda.

metoda vishing

U aplikace metody vishing bylo výsledkem získání přístupových údajů prostřednictvím telefonického rozhovoru od 33 % z celkového počtu dvanácti zaměstnanců. Zaměstnanci útočníkovi sdělili přístupové údaje, aniž by od volajícího požadovali více informací. Z výsledku dotazníku vyplývá, že by žádný ze zaměstnanců nesdělil přístupové údaje přímo, ale 37 % z celkového počtu třiceti zaměstnanců by se nejprve útočníka zeptalo na další informace a poté by sdělilo přístupové údaje.

metoda phishing

Výsledek metody phishing představoval získání přístupových údajů od 20 % z celkového počtu třiceti zaměstnanců. Na základě výsledku dotazníku by žádný z třiceti zaměstnanců neposkytl přístupové údaje. U této metody byl zaznamenán mezi aplikací metody a výsledkem dotazníku největší rozdíl.

Rozdíly mezi aplikacemi vybraných metod a výsledky dotazníku mohly zapříčinit odpovědi zaměstnanců v dotazníku, které nemusely být vždy pravdivé. Přesto, že zaměstnanci věděli, jak by se v případě útoku zachovali, z důvodu nesprávnosti nechtěli takové jednání prezentovat a raději mohli zvolit jinou odpověď. Dalším důvodem rozdílnosti odpovědí mohl být odlišný pohled na práci v klidném prostředí a na práci v časové tísni. Lépe se zaměstnanci rozhodují v klidném prostředí, kdy vědí, co je správné. Při práci v časové tísni mohou reagovat jinak, což v konečném výsledku může znamenat úspěšný útok a únik citlivých informací.

7. Návrh opatření pro zvýšení zabezpečení pracoviště

Stanovení bezpečnostních opatření představuje ochranu před možnými útoky sociálního inženýrství. Pečlivě stanovená pravidla, která musí zaměstnanci povinně dodržovat, představují pro útočníky komplikaci.

Při navrhování bezpečnostních opatření je nutné mít na paměti, že zabezpečení může negativně ovlivnit pracovní výkon jednotlivých zaměstnanců. Slabé bezpečnostní opatření představuje vyšší riziko možného útoku sociálního inženýrství. Pokud je bezpečnostní opatření příliš silné, může mít negativní vliv na produktivitu práce zaměstnanců.

Navrhovaná opatření

Veškeré vytvořené návrhy opatření slouží k zabránění neoprávněnému nakládání s citlivými informacemi městského úřadu a jsou stanoveny v přiměřené míře. Návrhy opatření jsou také navrženy jako součást připravované bezpečnostní směrnice. Rozsah navrhovaných opatření je zaměřen na všechny zaměstnance, kteří pracují s citlivými informacemi a ke své práci potřebují výpočetní techniku.

Pro zvýšení zabezpečení pracoviště městského úřadu byla navržena tato opatření:

Likvidace dat

U dokumentace v papírové podobě musí zaměstnanci městského úřadu likvidovat data prostřednictvím skartace. Musí skartovat veškeré dokumenty, které obsahují citlivé informace. Za citlivé informace jsou považovány například ručně psané poznámky, různá hesla nebo telefonní čísla. Ke skartaci by bylo vhodné, aby zaměstnanci používali kvalitnější skartovací zařízení, které udělá z papírové dokumentace drť. U dokumentace, která má po skartaci podobu pruhů, hrozí riziko, že může být při troše snahy znovu složena.

Likvidace dat u digitálních médií je komplikovanější. V dnešní době je pouhé odstranění dat nedostačující. Existují různé způsoby, jak odstraněná data získat zpět. Proto je nutné například u pevných disků řešit likvidaci přes specializovanou

firmu, která se zabývá likvidací těchto zařízení. Nosič jako je CD nebo DVD musí zaměstnanci zlikvidovat pomocí skartovacího zařízení.

Pracovní e-mail

Každý zaměstnanec je povinen používat pracovní e-mail výhradně pro pracovní účely. Zaměstnanci nesmí pracovní e-mail zneužívat a nesmí zveřejňovat své pracovní e-maily na jiných než oficiálních webových stránkách městského úřadu.

Zaměstnanci jsou povinni u každého příchozího e-mailu prověřit e-mailovou adresu odesílatele. Pokud by e-mailová zpráva obsahovala odkaz, musí být zkontrolován zaměstnancem, zda opravdu směruje na stránky instituce, která je pod zprávou podepsaná. V případě jakékoliv pochybnosti u e-mailové zprávy by měl zaměstnanec kontaktovat IT technika. Pokud dojde k zobrazení webové stránky přes odkaz obsažený v e-mailové zprávě, zaměstnanec je povinen zkontrolovat i URL stránky v adresním řádku webového prohlížeče, kam byl odkazem přesměrován. Naopak při odesílání e-mailové zprávy musí zaměstnanci důkladně zkontrolovat, komu e-mailovou zprávu posílají. Je důležité zamezit tomu, aby se e-mailová zpráva s citlivými informacemi dostala do rukou neoprávněných osob.

Jestliže zaměstnancům přijde na pracovní e-mail jakákoliv poplašná zpráva, zaměstnanci jsou povinni neprodleně informovat IT technika.

Využívání internetu při práci

Městský úřad by měl omezit zaměstnancům využívání internetu při práci. Využívání internetu by mělo být povoleno pouze k výkonu práce, nikoliv k soukromým nebo jiným účelům. Zaměstnanci mají zakázáno stahovat z internetu jakýkoliv software a multimediální obsah. Zaměstnanci musí být poučeni o bezpečném chování na internetu a možných hrozbách, které by mohly při nesprávném chování na internetu ohrozit data a systém městského úřadu. Také musí být poučeni o možných rizicích spojených s otevíráním neznámých příloh u nedůvěryhodných e-mailů. Pokud by chtěl zaměstnanec odeslat přílohu nebo sdílet dokumenty větší velikosti, nesmí používat online úložiště, jako je například uschovna.cz, ke kterému má přístup široká veřejnost. Potřebné úložiště by měl zaměstnancům poskytnout městský úřad.

Pokud je i přesto potřeba poslat větší dokument přes veřejnou síť, musí dojít u každé odesílané přílohy či dokumentu k přenosu v zašifrované podobě.

Přístup do počítače

Každý zaměstnanec má pro přístup do počítače své přístupové údaje, uživatelské jméno a heslo. Přístupové údaje slouží jako překážka proti neoprávněnému přístupu do systému. Zaměstnanci nesmí přístupové údaje nikde zveřejňovat, sdělovat ani zapisovat. Zaměstnanec má zakázáno sdílet své přístupové údaje s kolegy. Pod přístupovými údaji zaměstnanec odpovídá za vše, co se na počítači vykonalo. Zaměstnanec má pouze taková práva, jaká potřebuje pro výkon své práce. Při zadávání přístupových údajů si zaměstnanci musí dát pozor, jestli nejsou pozorováni jinou osobou. Pokud by měli podezření, že jejich heslo bylo odhaleno, musí heslo neprodleně změnit a nahlásit tuto skutečnost IT technikovi.

Pro práci s počítačem a systémy je stanovený způsob tvorby přístupových hesel. Přístupové heslo musí obsahovat minimálně 10 znaků. Dále musí heslo obsahovat kombinaci čísel, velkých a malých písmen a speciálních znaků. Aby nebylo heslo jednoduše zjistitelné, zaměstnanci by neměli používat například vlastní jména, přezdívky, data narození nebo rodná čísla. Pro zajištění vyšší bezpečnosti je nutné vždy heslo po devadesáti dnech změnit. U zaměstnaneckých účtů dojde po třech neúspěšných pokusech o přihlášení k zablokování. Zaměstnanci by neměli používat stejné heslo do více systémů. Heslo by nemělo být shodné s heslem do soukromého počítače zaměstnance. Dále zaměstnanci nesmí využívat funkci zapamatování hesla. Pokud je to možné, zaměstnanci by se měli vyvarovat ručnímu zapisování hesel. V případě, že má zaměstnanec více hesel a není schopen je uchovat ve své paměti, je důležité, aby byla zapsaná hesla uložena na bezpečném místě, kam nemají přístup jiné osoby. Jestliže má zaměstnanec podezření, že došlo k prolomení hesla nebo k prolomení hesla skutečné došlo, musí dojít k okamžité změně hesla a informování IT technika.

V případě potřeby zástupu zaměstnance musí IT technik vytvořit zastupujícímu zaměstnanci přístupové údaje.

Pořádek na pracovišti

Zaměstnanci jsou vždy povinni před odchodem ze svého pracoviště uložit veškerou dokumentaci, písemnosti, razítka nebo paměťová úložiště na místo, které je nepřístupné pro neoprávněné osoby. Takovéto opatření je důležité proto, aby se předešlo odcizení, zneužití či poškození výše zmíněných věcí.

Přístup k datům

Každý zaměstnanec musí mít přístup pouze k datům, která nezbytně potřebuje k plnění svých pracovních povinností. Zaměstnanec musí zpracovávat data výhradně v pracovních zařízeních, poskytnutých městským úřadem. Zaměstnanec nesmí otevírat ani měnit soubory jiných zaměstnanců.

Na pracovních zařízeních není dovoleno shromažďování soukromých dat a využívání pracovních programů pro osobní účely.

Pracovní počítač, práce s počítačem

U všech pracovních počítačů musí účet administrátora spravovat výhradně IT technik městského úřadu. Instalace jakéhokoliv softwaru je možná pouze pod administrátorským účtem. Veškerý software musí být instalován z originálních medií. Dále u všech pracovních počítačů musí být pravidelně aktualizovaný operační systém a mělo by být zavedeno monitorování všech pokusů o přihlášení do systému. Každý pracovní počítač musí obsahovat antivirový program, který je nutné pravidelně aktualizovat. Na všech pracovních počítačích musí být povoleno v průzkumníku Windows zobrazení přípon souborů. Jednotlivé pracovní počítače musí být nastaveny tak, aby v síti nebyly mezi sebou vzájemně zjistitelné.

Zaměstnanci mají zakázáno provádět úkony, které nejsou předmětem jejich pracovní náplně. Dále mají zaměstnanci zakázáno instalovat do pracovního počítače jakýkoliv software, připojovat neznámé nosiče CD, DVD nebo USB flash disk. Zaměstnanci nesmí měnit nastavení počítače, počítačové sítě a služeb.

Při každém krátkodobém opuštění pracoviště musí zaměstnanec uzamknout svůj pracovní počítač, například použitím kombinací kláves (Win+L) nebo

Ctrl+Alt+Delete a volby Uzamknout. V případě odchodu zaměstnance z pracoviště na dobu delší, než dvě hodiny musí zaměstnanec počítač vypnout.

Hlášení bezpečnostních incidentů

Jestliže dojde k narušení zabezpečení pracoviště, je důležité mít přesně stanovený postup, jak se v takové situaci zachovat. Postup by měl být stanoven co nejjednodušeji, aby se jím zvládl řídit každý zaměstnanec. Veškeré incidenty musí být hlášeny IT technikovi městského úřadu, který je díky těmto hlášením schopen lépe odhadnout, kam budou směřovat například další útoky sociálního inženýrství. Může tak varovat ostatní zaměstnance ještě dříve, než by k útoku mohlo dojít. Incidenty je potřeba evidovat z důvodu možného opakování útoku.

V rámci školení zaměstnanců je nutné vždy poukázat na důležitost hlášení nebezpečných incidentů, i když se později ukáže, že se nejednalo například o útok sociálního inženýrství. Hlášení veškerých podezřelých incidentů snižuje riziko možného negativního dopadu na pracoviště.

Školení zaměstnanců

Útoky sociálního inženýrství jsou cílené primárně na člověka. Schopnost člověka odhalit útok sociálního inženýrství závisí nejen na bezpečnostním opatření, ale i na znalostech problematiky. Mezi jedno z nejdůležitějších opatření proti útokům sociálního inženýrství patří vytvoření školícího programu. Jestliže je člověk řádně proškolen, měl by být schopen útok odhalit a zabránit úniku citlivých informací. Snižuje se tak riziko možnosti stát se obětí útoku sociálního inženýrství.

Cílem školení by mělo být rozšíření znalostí zaměstnanců o problematice sociálního inženýrství a možných útocích. Také by mělo školení přispět ke zvýšení schopnosti zaměstnanců k odhalení útoků a jejich možné obraně. Školení by nemělo být pouze teoretické, ale mělo by obsahovat i praktickou část.

I když se zdají být cíle jasné, aplikovat je v praxi bývá často velmi komplikované. Problémy školení spočívají v jejich proveditelnosti. Školení často přistupují k problematice povrchně. Zaměstnanci nejsou během školení nijak zainteresováni. Školení bývají prováděna pomocí prezentací, poučných videí nebo knih. Vzhledem

k tomu, že útočníci mají přehled o konceptu prováděných školení, taková školení lze považovat za neefektivní.

Jedním z problémů může být motivace zaměstnanců řídit se navrženými bezpečnostními opatřeními. Často dochází k tomu, že zaměstnancům nejsou blíže vysvětleny důvody, proč by se opatřeními měli řídit. Díky tomu zaměstnanci považují pravidla za zbytečná a dochází ke snaze je obejít.

Městskému úřadu bych doporučil, aby bylo absolvování školení pro zaměstnance povinné, a to vždy alespoň jednou ročně. Nově příchozí zaměstnanec musí mít přístup k výpočetní technice až po absolvování školení. Pro lepší koncentraci zaměstnanců bych doporučil školení krátké a výstižné. Školení by nemělo mít pouze oznamovací charakter, ale zaměstnanci by si měli odnést i potřebné informace, které by se měly stát později zvykem. Dále bych doporučil k teoretické části školení přidat i praktické příklady konkrétních situací, které mohou nastat na městském úřadě. Za nedodržování bezpečnostních opatření musí čekat zaměstnance postih.

Přesto, že se může stát obětí útoku sociálního inženýrství i proškolený zaměstnanec, školení by mělo přispět alespoň k ochraně před jednoduchými útoky, kterých je v současné době nejvíce.

Kontrola dodržování bezpečnostních opatření

Městský úřad může kontrolovat své zaměstnance v dodržování bezpečnostních opatření. Z tohoto důvodu bylo doporučeno, aby městský úřad informoval zaměstnance o možné kontrole. To by mohlo přispět ke zvýšení jejich motivace při dodržování bezpečnostních opatření. Je doporučeno provádět kontrolu minimálně jednou ročně, ideálně v krátké době po proškolení zaměstnanců. To umožní zhodnotit efektivnost školení.

Veřejně dostupné informace

Městský úřad je veřejnou institucí vykonávající veřejnou správu. Na oficiálních webových stránkách má uveden telefonní seznam zaměstnanců, kteří se na výkonu správy určitým způsobem podílejí. Také má na webových stránkách organizační strukturu instituce. Zveřejněné údaje představují z pohledu bezpečnosti informací

riziko, že se útočník může dostat snadno ke jménům jednotlivých zaměstnanců, jejich telefonním číslům a e-mailovým adresám. Z organizační struktury může útočník snadno vyčíst postavení jednotlivých zaměstnanců na úřadě. Vzhledem k tomu, že městský úřad musí mít na webových stránkách zveřejněn telefonní seznam a organizační strukturu, mělo by být nastoleno odpovídající bezpečnostní opatření.

Přesto, že je na webových stránkách městského úřadu uveden telefonní seznam zaměstnanců, není nutné uvádět například zaměstnance z oddělení informačních a komunikačních technologií. Zaměstnanci z oddělení informačních a komunikačních technologií se žádným způsobem nepodílí na výkonu veřejné správy, jejich náplň práce spočívá v zajišťování plynulého chodu informačních systémů na úřadě. Z tohoto důvodu není potřeba veřejnosti sdělovat jména zaměstnanců a jejich kontakty. V případě potřeby kontaktování zaměstnanců z oddělení informačních a komunikačních technologií je možné se nechat na zaměstnance přepojit.

8. Závěr

Cílem diplomové práce bylo aplikovat vybrané metody sociálního inženýrství k testování zaměstnanců a navrhnout bezpečnostní opatření pro konkrétní instituci, vedoucí ke zmírnění možných útoků. Sociální inženýrství představuje nebezpečí pro každého z nás. Terčem útoku se mohou stát jak malé a velké podniky, tak i fyzická osoba. Vzhledem k tomu, že se jedná o celosvětový problém a dochází k rychlému rozvoji informačních a komunikačních technologií, je potřeba si uvědomit, zda jsme schopni se ubránit takovýmto útokům a případně podniknout určité kroky, které by hrozbu útoků minimalizovaly.

V současné době se i přes rostoucí nebezpečí útoků sociálního inženýrství o této problematice stále moc nemluví. I když je zabezpečení počítačů připojených k síti nebo internetu na vysoké úrovni, neexistuje žádný program, který by zabránil útokům sociálního inženýrství. Slabé místo totiž nespočívá v softwaru, ale v uživateli.

Teoretická část diplomové práce byla věnována definování základních pojmů, které souvisí se sociálním inženýrstvím. Byla popsána historie, formy a cyklus útoku. Dále bylo potřeba zmínit legislativu, která je spjata se sociálním inženýrstvím. Legislativa, která by se týkala pouze problematiky sociálního inženýrství, dodnes neexistuje. V této části byly také popsány možné metody útoků sociálního inženýrství. V současné době je hojně využíváno phishingových útoků z důvodu, že phishingové e-maily a podvodné webové stránky často působí důvěryhodným dojmem. Podoba phishingových e-mailů a podvodných webových stránek je na první pohled velmi obtížně rozpoznatelná od podoby oficiální. V tomto případě málo komu dojde, že se stal obětí útoku sociálního inženýrství.

V praktické části diplomové práce bylo provedeno testování zaměstnanců městského úřadu. K testování byly využity vybrané metody sociálního inženýrství. Dále se praktická část zabývala návrhy bezpečnostních opatření pro městský úřad. Při navrhování opatření bylo potřeba zohlednit možnost negativního dopadu na pracovní výkon zaměstnanců. Smysl bezpečnostních opatření spočíval ve zlepšení zabezpečení pracoviště. V praktické části byl zahrnut i dotazník na téma Sociální

inženýrství. Cílem dotazníku bylo zjistit, jaké mají zaměstnanci znalosti v této oblasti a jak si myslí, že by se zachovali, kdyby se stali obětí útoku sociálního inženýrství. Výsledky dotazníku byly následně porovnány s výsledky vybraných aplikovaných metod. Z dotazníku vyplynulo, že by mohl zaměstnanec znát problematiku spojenou se sociálním inženýrstvím a při možném útoku by správně zareagoval a útok odrazil. Přitom při aplikaci metody zaměstnanec útoku podlehl.

V budoucnu lze předpokládat přibývání útoků pomocí sociálního inženýrství, proto bude potřeba této problematice věnovat větší pozornost. Lze předpokládat nápor na organizace z důvodu zvýšení ochrany před možnými útoky. Proto je na závěr doporučeno vzdělávání zaměstnanců formou školení, které povede k pochopení problematiky spojené s možnými útoky sociálního inženýrství.

9. Seznam použité literatury

[1] *What is Social Engineering? Examples and Prevention Tips | Webroot [online]. [citace 2019-10-28]. Dostupné z: https://www.webroot.com/au/en/resources/tips-articles/what-is-social-engineering*

[2] *HADNAGY, Christopher.* Social engineering: the science of human hacking*. Second edition. Indianapolis, IN: Wiley, 2018. ISBN 978-1-119-43338-5.*

[3] *JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007, ISBN 978-80-247-1561-2.*

[4] *HADNAGY, Christopher a EKMAN, Paul. Unmasking the Social Engineer: The Human Element of Security. Indianapolis, IN: Wiley, 2014. ISBN 978-1-118-60857-9.*

[5] *Kevin MITNICK a William SIMON, 2003. Umění klamu. B.m.: Helion S.A. ISBN 83-7361-210-6.*

[6] *EKMAN, Paul a Wallace V. FRIESEN. Emoce pod maskou: poznám, co si myslíš, podle toho, jak se tváříš. I. vydání. Brno: BizBooks, 2015. ISBN 978-80-265-0422-1.*

[7] *The Man Who Sold the Eiffel Tower. Twice [online]. [citace 2019-10-31]. Dostupné z: https://www.smithsonianmag.com/history/man-who-sold-eiffel-tower-twice-180958370/*

[8] *Kevin MITNICK [online]. [citace 2020-04-20]. Dostupné z: https://www.wealthypersons.com/kevin-mitnick-net-worth-2020-2021/*

[9] *BRABEC, František. Technologie detektivních činností. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-780-4.*

[10] *MCCARTHY, Linda a Denise WELDON-SIVIY. Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online. Praha: CZ.NIC, 2013. ISBN 978-80-904248-6-9.*

[11] *Social engineering techniques: 4 ways criminal outsiders get inside [online]. [citace 2019-11-1]. Dostupné z: https://www.csoonline.com/article/2125205/social-engineering-techniques--4-ways-criminal-outsiders-get-inside.html*

[12] *Top 10 Social Engineering Tactics [online]. [citace 2019-11-1]. Dostupné z: https://www.informit.com/articles/article.aspx?p=1350956&seqNum=8*

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

[14] *Zákon č. 40/2009 Sb. (Trestní zákoník) [online]. [citace 2020-2-5]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40*

[15] *Zákon č. 181/2014 Sb. (Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů) [online]. [citace 2020-2-5]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181*

[16] *Vishing and smishing: The rise of social engineering fraud [online]. [citace 2019-11-22]. Dostupné z: https://www.bbc.com/news/business-35201188*

[17] *VoIP Phishing and the Way it Works [online]. [citace 2020-2-22]. Dostupné z: https://www.lifewire.com/voip-phishing-3426534*

[18] *JAMES, Lance. Phishing bez záhad. Praha: Grada, 2007, 281 s. ISBN 978-80-247-1766-1.*

[19] *What is Social Engineering? Employees are your Weakest Link [online]. [citace 2019-11-20]. Dostupné z: https://stories.akosweb.com/what-is-social-engineering-employees-are-your-weakest-link-25fa049ddfce*

[20] *HADNAGY, Christopher a FINCHER, Michele. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails. Indianapolis, IN: Wiley, 2015. ISBN 978-1-118-95847-6.*

[21] *Tips for Detecting a Phishing Email [online]. [citace 2019-11-28]. Dostupné z: https://www.myalignedit.com/2019/09/tips-for-detecting-a-phishing-email/*

[22] *Pharming [online]. [citace 2020-3-25]. Dostupné z: https://us.norton.com/online-threats/glossary/p/pharming.html*

[23] *How Intruders gain access to Network using social engineering [online]. [citace 2019-11-25]. Dostupné z: https://www.researchgate.net/publication/280843782_How_Intruders_gain_access_to_Network_using_social_engineering*

[24] *PARSONS, June Jamrich a OJA, Dan, 2014.* New perspectives, Computer concepts, *Boston, MA : Course Technology, ISBN 978-1-285-09692-6.*

[25] *CZ.NIC - O doménách a dns [online]. [citace 2020-3-14]. Dostupné z: https://www.nic.cz/page/312/o-domenach-a-dns/*

[26] *Attacks over DNS [online]. [citace 2020-3-21]. Dostupné z: https://resources.infosecinstitute.com/attacks-over-dns/*

[27] *What is DNS cache poisoning? | DNS spoofing | CLOUDFLARE [online]. [citace 2020-4-11]. Dostupné z: https://www.cloudflare.com/learning/dns/dns-cache-poisoning/*

[28] *BROWN, Bruce. Ocala : Atlantic Publishing Group Inc. 2010. ISBN 978-1-601-38303-7.*

[29] *Social Engineering: Would You Take the Bait? [online]. [citace 2019-11-23]. Dostupné z: https://www.darasecurity.com/article.php?id=32*

[30] *Baiting, what is it? How to defend yourself from social engineering [online]. [citace 2020-4-18]. Dostupné z: https://blog.mailfence.com/what-is-baiting-in-social-engineering/*

[31] *CROSS, Michael a Robert SHIMONSKI. Social Media Security: Leveraging Social Networking While Mitigating Risk. Syngress, 2014. ISBN 1-59749-986-2.*

[32] *ALCORN, Wade, Christian FRICHOT a Michele ORRÙ. The browser hacker's handbook. Indianapolis: Wiley, 2014. ISBN 978-1-118-66209-0.*

[33] *What Is Smishing? [online]. [citace 2019-11-25]. Dostupné z: https://uk.norton.com/norton-blog/2016/06/what_is_smishing.html*

[34] *DUNHAM, Ken, Mobile malware attacks and defense. Burlington: Syngress, 2009. ISBN 978-1-59749-298-0.*

[35] *Co je to 2FA a proč vícefaktorovou autentizaci používat [cit. 2019-11-25]. Dostupné z: https://www.spajk.cz/co-je-to-2fa-a-proc-vicefaktorovou-autentizaci-pouzivat/*

[36] *The SMISHING threat [online]. [citace 2019-12-10]. Dostupné z: https://blog.checkpoint.com/2017/02/09/smishing-threat-unraveling-details-attack/*

[37] *How to Avoid Becoming the Victim of a SMiShing Scam [online]. [citace 2019-9-10]. Dostupné z: https://www.thebalance.com/smishing-scams-315808*

[38] *BOSWORTH, Seymour, Michel E. KABAY a Eric WHYNE. Computer security handbook. New Jersey: Wiley, 2014. ISBN 978-1-118-12706-3.*

[39] *5 Social Engineering Attacks to Watch Out For [online]. [citace 2019-12-1]. Dostupné z: https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/*

[40] *Successful Pretexting - Security Through Education [online]. [citace 2020-1-19]. Dostupné z: https://www.social-engineer.org/framework/influencing-others/pretexting/successful-pretexting/*

[41] *Phishing|Raiffeisenbank [online]. [citace 2020-4-30]. Dostupné z: https://www.rb.cz/bezpecne-bankovnictvi/phishing#lg=1&slide=20*

[42] *MFCR varuje před podvodnými e-mailovými zprávami [online]. [citace 2020-6-23]. Dostupné z: https://www.mfcr.cz/cs/aktualne/aktuality/2020/ministerstvo-financi-varuje-pred-podvodn-38408/*

[43] *Kromě phishingových e-mailů posílají útočníci také SMS | ČSOB [online]. [citace 2020-1-28]. Dostupné z: https://www.csob.cz/portal/-/b200113*

[44] *České uživatele Apple produktů ohrožuje nový phishing [online]. [citace 2020-1-28]. Dostupné z: https://jablickar.cz/ceske-uzivatele-apple-produktu-ohrozuje-novy-phishing/*

[45] *Česká pošta varuje před podvodnou soutěží o iPhone 11 [online]. [citace 2020-1-28]. Dostupné z: https://manipulatori.cz/ceska-posta-varuje-pred-podvodnou-soutezi-o-iphone-11/*

Seznam obrázků

Obrázek 1: Kevin Mitnick 7
Obrázek 2: OK 10
Obrázek 3: radost 12
Obrázek 4: smutek 13
Obrázek 5: překvapení 14
Obrázek 6: strach 14
Obrázek 7: Cyklus útoku sociálního inženýrství 17
Obrázek 8: Příklad podvodného e-mailu 27
Obrázek 9: Hrozba DNS cache poisoning 29
Obrázek 10: Příklad nastraženého CD 31
Obrázek 11: Smishing na klienty České pošty 33
Obrázek 12: Adresní řádek s protokolem 38
Obrázek 13: Podrobnosti SSL certifikátu 39
Obrázek 14: Podvodný e-mail ČSOB 41
Obrázek 15: Podoba podvodné webové stránky ČSOB 41
Obrázek 16: Podvodný e-mail Raiffeisenbank 42
Obrázek 17: Podvodný e-mail MFCR 43
Obrázek 18: Podvodná SMS zpráva ČSOB 44
Obrázek 19: Podvodná SMS zpráva APPLE 44
Obrázek 20: Podoba podvodné stránky APPLE 45
Obrázek 21: Fiktivní výhra 46
Obrázek 22: Pravá podoba webové stránky 48
Obrázek 23: Podvodná podoba webové stránky 48

Obrázek 24: Upozornění o možné hrozbě phishingového útoku....49
Obrázek 25: První varianta phishingového e-mailu....50
Obrázek 26: Druhá varianta phishingového e-mailu....50

Seznam grafů

Graf 1: Vyhodnocení odpovědí k otázce č. 1....58
Graf 2: Vyhodnocení odpovědí otázky č. 2....59
Graf 3: Vyhodnocení odpovědí otázky č. 3....60
Graf 4: Vyhodnocení odpovědí otázky č. 4....61
Graf 5: Vyhodnocení odpovědí otázky č. 5....62
Graf 6: Vyhodnocení odpovědí otázky č. 6....63
Graf 7: Vyhodnocení odpovědí otázky č, 7....64
Graf 8: Vyhodnocení odpovědí otázky č. 8....65
Graf 9: Vyhodnocení odpovědí otázky č. 9....66
Graf 10: Vyhodnocení odpovědí otázky č. 10....67
Graf 11: Vyhodnocení odpovědí otázky č. 11....68
Graf 12: Vyhodnocení odpovědí otázky č. 12....69
Graf 13: Vyhodnocení odpovědí otázky č. 13....69

Seznam tabulek

Tabulka 1: Přehled výsledků variant phishingového e-mailu....56