Technika vyjednávání jako součást sociálního inženýrství

Lukáš Borovský

Bakalářská práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2021/2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Lukáš Borovský**
Osobní číslo:	**A19449**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Prezenční**
Téma práce:	**Technika vyjednávání jako součást sociálního inženýrství**
Téma práce anglicky:	**Negotiation Technique as a Part of Social Engineering**

Zásady pro vypracování

1. Popište základní pojmy související se sociálním inženýrstvím a vyjednáváním.
2. Vysvětlete souvislost vyjednávání a sociálního inženýrství.
3. Stanovte nejčastější typy útoků v rámci sociálního inženýrství.
4. Navrhněte sociální experiment.
5. Vyhodnoťte výsledky experimentu.

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

Seznam doporučené literatury:

1. NAKONEČNÝ, Milan. Úvod do psychologie. Praha: Academia, 2003. ISBN 80-200-0993-0.
2. JIROVSKÝ, Václav. Kybernetická kriminalita. Grada, 2007. ISBN 978-80-2471-561-2.
3. ZAVRŠNIK, Aleš. Kyberkriminalita. Wolters Kluwer, 2017. ISBN 978-80-7552-759-2.
4. KOHOUTEK, Rudolf. Základy užité psychologie. Brno: CERM, 2002. ISBN 80-214-2203-3.
5. NAKONEČNÝ, Milan. Sociální psychologie. Praha: Academia, 1999, 287 s. ISBN 80-200-0690-7.

Vedoucí bakalářské práce: **Ing. Lukáš Králík, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **17. ledna 2022**
Termín odevzdání bakalářské práce: **31. května 2022**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 17. ledna 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně, dne

Borovský Lukáš v.r.
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá tématem technikou vyjednáváni jako součást sociálního inženýrství. V práci jsou vysvětleny základní pojmy, které se využívají v sociálním inženýrství a pojmy, které se používají ve vyjednávání. Součástí práce je vysvětlení útoků, které využívají sociotechnici. Je vyjasněna souvislost mezi vyjednáváním a sociálním inženýrstvím. Sestavený experiment ukazuje na problematiku sociálního inženýrství v praxi.

Klíčová slova: sociální inženýrství, útoky sociálního inženýrství, sociotechnik, vyjednávání, experiment

ABSTRACT

The bachelor thesis deals with the topic of negotiation technology as a part of social engineering. The thesis explains the basic concepts that are used in social engineering and the concepts that are used in negotiation. Part of the work is an explanation of the attacks used by sociotechnics. The link between negotiation and social engineering is clarified. The compiled experiment shows the issue of social engineering in practice.

Keywords: social engineering, social engineering attacks, sociotechnics, negotiation, experiment

Rád bych poděkoval panu Ing. Lukáši Králíkovi, Ph.D. za vedení bakalářské práce. Dále bych rád zmínil a poděkoval své rodině, kteří mě ve studiu podporovali a stáli za mnou za jakýchkoliv situací.

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

OBSAH

ÚVOD

Snaha získání informací od lidí, byla, je a bude. Sociální inženýrství pojednává o způsobech, jak tyto potřebné informace dostat. Jako první se využívaly techniky, při kterých byl kladen důraz na vystupování člověka v reálném světě. S příchodem výpočetní techniky se tyto nelegální činnosti přesunuly i do virtuálního světa. V dnešní době existuje ohromné množství různých sociálních technik, které mají společný cíl. Získat informace, které nám nenáleží. Už samotná informace o existenci sociálního inženýrství je základním stupněm obrany.

Obrana před sociálním inženýrstvím je velice kontroverzní téma. Lidé obvykle spoléhají pouze na stroje, které chrání jejich majetek, data, a vše co má pro konkrétního člověka danou hodnotu. Do technických prostředků je možné investovat miliony, ale jak se říká, vše je dobré jako nejslabší článek a tím je člověk.

Sociální inženýrství využívá v některých případech i vyjednávací techniky. Vyjednávání je součástí v jakémkoliv okamžiku lidského života. Může se jednat o vyjednávání mezi zaměstnancem a zaměstnavatele, rodičem a dítětem, nebo mezi dvěma kamarády. Vyjednávání se stalo každodenní součástí životů, že je někdy přijímáno automaticky a lidé si této situace ani nevšimnou. Zkušený sociotechnik působí profesionálním a přátelským chováním, tudíž potencionální oběť nemusí mít podezření, že se jedná o nelegální činnost. Ale u oběti převládá pocit, že si přátelsky povídá s náhodným člověkem. Této situace chce dosáhnout každý sociotechnik, aby cesta k získání informací nebyla podezřelá.

V praktické části bakalářské práce je vytvořen experiment za použití jedné z technik útoků sociálního inženýrství. Útok je prováděn po telefonu čili využívá techniku vhishing (oklamání obětí po telefonu) a techniku pretexting (předem připraveného scénáře). Provedený pokus znázorňuje počet úspěšných a neúspěšných pokusů, cíle útoku, a nakonec vyhodnocení celého experimentu.

I. TEORETICKÁ ČÁST

1 SOCIÁLNÍ INŽENÝRSTVÍ

Sociální inženýrství je pojem, který je v posledních letech více známý, snaží se podvodem získat od obětí jejich informace jako jsou hesla, osobní informace apod. Sociální inženýrství nejvíce využívá lidské chybovosti, jejich hlouposti a slabin našeho vnímání. Sociální inženýrství je s lidstvem spjato už od pradávna a každý den využívají útočníci tyto negativní vlastnosti lidstva pro svoje obohacení.

Se sociálním inženýrstvím a, vývojem informačních technologií, je úzce spjata kyberkriminalita. Kyberkriminalita označuje konání trestného činu pomocí informačních a komunikačních technologií. Uživatelé osobních počítačů, chytrých mobilů apod. jsou pod neustálým tlakem útočníků, kteří využívají sociálního inženýrství pro páchání trestné činnosti. [1]

Sociální inženýrství můžeme rozdělit na dvě skupiny. Podvody, které využívají hackeři, či crackeři. A druhá skupina, kam patří podvodníci a sociotechnici. V následujících odstavcích budou podrobně rozebrána tato témata. [1]

1.1 Základní pojmy sociálního inženýrství

Vysvětlení pojmů hacker, cracker, podvodník a sociotechnik:

- **Hacker** – člověk, který označován jako hacker je vysoce nadaný v oblasti informačních technologií (dále jen IT). Hacker zjišťuje nové metody průniků do systémů. Svým nestandardním chováním odhaluje případné chyby, které by mohli být zneužity. Hacker není označení pro člověka, který by těchto chyb zneužíval pro svůj osobní prospěch. Zpravidla se jedná o zjištění chyb, který si daný vývojář, nebo skupina vývojářů opraví. [1]
- **Cracker** – je zpravidla osoba, nebo skupina osob, která ke své činnosti využívá spíše programování různých škodlivých aplikací, nebo infikovaných souborů. Snaží se prostřednictvím naprogramovaných aplikací, nebo škodlivých souborů napadnout a ovládnout počítač, nebo jiné informační zařízení. Jedná se o nelegální aktivitu. [2]
- **Podvodník** – podvodník je běžný člověk, který se od obětí snaží získat jen peníze, které využije pro svůj prospěch. K získání peněz využívá různých podvodných způsobů. [3]
- **Sociotechnik** – se snaží vymámit z oběti informace, které zneužije ve svůj prospěch. Sociotechnik využívá ke své práci různých manipulačních technik, které jsou spjaty s lidskou hloupostí, důvěřivostí apod. [2]

Mezi základní pojmy sociálního inženýrství patří také:

- škodlivý software (malware),
- vyděračský software (ransomware),
- bot a botnet,
- příkazový a řídící server (command and control),
- zpravodajství z otevřených zdrojů (open source intelligence – OSINT),
- zadní vrátka (back door),
- užitečné zatížení (payload),
- Obrácená sociotechnika (reverse social engineering),
- Více faktorová autentizace (multi-factor authentication – MFA),
- thrashing,
- útok hrubou silou (Brute-Force Attack),
- záznam stisku kláves (Keylogger).

Základních pojmů je ohromné množství. V bakalářské práci je vybraná část těchto pojmů, které jsou vysvětleny v následujících podkapitolách.

1.1.1 Škodlivý software (malware)

Označení jako škodlivý software (malware) je obecný název pro jakýkoliv škodlivý program, který je škodlivý pro systém zařízení. Cílem škodlivého softwaru je snaha poškodit nebo deaktivovat počítač a jiné informační zařízení. Škodlivý software může převzít částečnou kontrolu nad provedenými operaci zařízení. [4]

1.1.2 Vyděračský software (ransomware)

Vyděračský software (ransomware) je škodlivý software, který se snaží z lidí, nebo organizací dostat peníze tím, že převezme kontrolu nad samotným počítačem, tabletem, mobilem apod. oběti. Ransomware zašifruje soubory a po oběti chce peníze, aby své soubory a dokumenty dostala zpět. Platba útočníkovi probíhá nejčastěji přes nevysledovatelného převodu prostřednictvím kryptoměny. I když se oběť rozhodne výkupné za své data zaplatit, není jisté, že útočník, nebo skupina útočníku dešifrovaná data vrátí zpět. Nejběžnějšími vektory útoku na ransomware jsou přílohy e-mailů a odkazy na weby pro sdílení souborů, jako je Dropbox nebo Disk Google. [5]

1.1.3 Bot a botnet

Pojem bot (nebo také robot) je část softwaru, která je tajně nainstalována do zařízení oběti. Může se jednat o počítač, tablet, mobilní telefon apod. [5]

Botnet je útok infikovaných zařízení (botů), které se používají k masivním útokům, jako jsou e-mailové útoky. Velké množství e-mailů z jednoho místa může být zablokováno. Masivní útoky mají za úkol zahltit routery a následuje kolaps postižené webové stránky. [5]

1.1.4 Příkazový řídící server (command and control)

Příkazový řídící server (command and control) je stroj ovládaný útočníkem. Útočník odesílá příkazy, které počítač infikovaný škodlivým softwarem provede. Po provedení příkazu se obrátí na příkazový řídící server, který vyšla dalš´í pokyn k provedení. Útočník sedí za klávesnicí a celý útok organizuje. [6]

1.1.5 Zpravodajství z otevřených zdrojů (open source intelligence – OSINT)

Zpravodajství z otevřených zdrojů (OSINT – open source intelligence) je označení pro jakékoli informace, které jsou veřejně dostupné. Tyto informace jsou běžně na internetu a může si je vyhledat každý. Jedná se například o informace typu e-mailová adresa, telefonní číslo, jméno osoby pracující třeba v personálním oddělení. Tyto informace může mít firma volně přístupné na webových stránkách. [6]

1.1.6 Zadní vrátka (back door)

Zadní vrátka můžou označovat část aplikaci, nebo jen její část, která umožňuje přístup bez použití přihlašovacích údajů, jako jsou například jméno, heslo. Zadní vrátka se používají k obcházení bezpečnostních kontrol. Zadní vrátka můžou být v některých případech záměrná od výrobce pro efektivnější odstraňování problémů. [5]

1.1.7 Užitečné zatížení (payload)

Užitečné zatížení jsou tajně nainstalované sady počítačových instrukcí do počítače oběti. Nainstalované instrukce dále pomáhají útočníkovi utajit přístup k počítačovému systému oběti. Když oběť klikne na odkaz pro instalaci programu, aktivuje se užitečné zatížení a provedou se všechny akce, které jsou naprogramované útočníkem. [6]

1.1.8 Více faktorová autentizace (multi-factor authentication – MFA)

Více faktorová autentizace je ověřování se dvěma, nebo více samotných forem identifikace. Více faktorová autentizace se může nacházet u přihlášení do e-mailové schránky, internetové bankovnictví apod. Pro přihlášení do konkrétních aplikací, které využívají více faktorové autentizace, je potřeba použít heslo a následně zadat sekundární kód, který je většinou poslaný pomocí sms zprávy Více faktorová autentizace pomáhá zabránit útočníkům odcizit uživatelské účty. Více faktorová autentizace se nazývá jako dvou faktorová autentizace (2FA). [5]

1.1.9 Thrashing

Thrashing je problém, který vzniká při používání virtuální paměti. K thrashingu dochází tehdy, když virtuální paměť počítače vyměňuje data za data na pevném disku velkou rychlostí. Jakmile se hlavní paměť zaplní je potřeba do virtuální paměti zaměnit další stránky. Trahsing může vést k úplnému zhroucení pevného disku počítače. [7]

1.1.10 Útok hrubou silou (Brute-Force Attack)

Útok hrubou silou znamená zkoušení mnoha variant možného hesla do prostoru, který je chráněn heslem. K prolomení používají útočníci rozsáhlé databáze nejčastějších hesel a jejich kombinací. Útoky hrubou silou stále fungují, jelikož mnoho uživatelů používá slabá hesla, které neaktualizují po celou dobu jejich používání. Útočníci mají v rozsáhlé databázi hesel všemožné varianty. Například heslo: „Kotatko“ může mít varianty „K0tatko“ a další. [5]

1.1.11 Záznam stisku kláves (Keylogger)

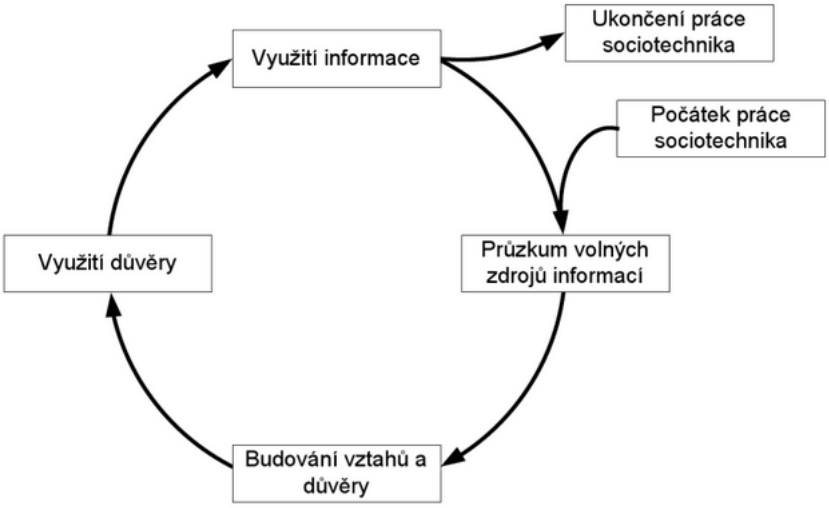
Záznam stisku kláves (Keylogger) je softwarové zařízení, které je nainstalováno do počítače, mobilu, tablet apod. Zaznamenává vše, co je stisknuto na klávesnici. Ať už se jedná o hesla, či přihlašovací údaje. Zaznamenaná data jsou odeslána útočníkovi, který je může použít k nelegální činnosti. [5]

1.2 Metody sociologického útoku

Základem sociotechnických metod, je získání informací útokem na nejslabší článek zabezpečení. Nejslabší článek je člověk. Útočník využívá slabých, nebo vůbec nepodchycených, míst v bezpečnostní politice firmy. Útočník se snaží manipulovat s obětí a za pomoci důkladně sofistikovaného plánu se snaží dosáhnou svého cíle. Při svých činnostech musí

útočník dobře reagovat na napadenou osobu. Jelikož je každý člověk originál, nemusí tak platit jeden perfektně předpřipravený scénář na všechny. Útočník je náhle v situaci, kdy musí improvizovat, aby dosáhl svého cíle, nevzbudil podezření a nebyl odhalen. [8]

Útočník si před útokem zjistí informace o firmě, kterou chce napadnout. Prozkoumá např. webové stránky firmy, různé reklamní inzeráty, jak ukazuje (Obrázek 1). Při získání dostatečného množství informací, začíná útočník budovat vztahy a získávat důvěru od obětí. Po získání důvěry útočník zneužívá svého útoku a dostává se do situace, kdy získal veškeré informace, které potřebuje. Jak ukazuje (Obrázek 1), útok může a nemusí skončit. Útočník má informace, které získal, ale svůj útok může začít zase v nové firmě a takhle celý postup opakovat. [8]



Obrázek 1: Sociotechnický cyklus [8]

V následujících podkapitolách budou probrány konkrétní metody sociologického útoku.

1.2.1 Přímí přístup

Metoda útoku pomocí přímého přístupu se může jevit jako absurdní, ale je potřeba pořád s touhle metodou počítat. Jedná se o vyžádání citlivých informací, např. hesel, od zaměstnanců firmy. Útočník se přímočaře otáže na tyto informace a nic netušící zaměstnanec vyzradí utajovaná data. [9]

1.2.2 Důležitý uživatel

Metoda důležitého uživatel spočívá v tom, že útočník útočí na „podřadné zaměstnance“ Podřadní zaměstnanci jsou lidé, kteří mají nad sebou vedoucí pracovníky, ať už se jedná o vedoucího směny, majitele firmy apod. Útočník předstírá vyšší postavení ve firmě než daná

oběť. Tímhle stylem útočník působí na psychiku zaměstnance, který bude chtít pomoci svému nadřízenému. Oběť se bude bát případných problémů, popřípadě ztráty zaměstnání. Právě tohoto strachu útočník využívá a ptá se oběti například na telefonní čísla, vzdálený přístup, různá hesla do systému, nebo serveru apod. [9]

1.2.3 Bezmocný uživatel

Při metodě bezmocného uživatele se útočník vydává za nového kolegu oběti. Útočník předstírá problémy s přihlášením do systému, sítě, nebo jakékoliv potíže s počítačem. Oběť, jakožto zaměstnanec, který už má ve firmě nějaké zkušenosti, se nad novým kolegou smiluje a nabídne mu využít svoje přihlašovací údaje na určitou dobu. [9]

Takovým stylem může útočník zaútočit i na administrátora, kterého přesvědčí o ztrátě přihlašovacích údajů. Administrátor útočníkovi vygeneruje nové. [9]

1.2.4 Pracovník technické podpory

Útočník se může dostat do prostor firmy, kde předstírá že je zaměstnanec informační, nebo technické podpory. Útok může probíhat přímo ve firmě, kdy útočník pracuje na počítači nic netušící oběti. Útočník předstírá pravidelnou kontrolu počítače, ale přitom si nastavuje vzdálený přístup pro pozdější použití. [9]

1.2.5 Obrácená sociotechnika

Metoda obrácené sociotechniky vytváří situaci, aby samotná oběť požádala útočníka o pomoc.

Žádný člověk není dokonalý, a proto i zkušení odborníci potřebují se svou prací poradit. Ve firmách to mohou být technici, správci sítí apod. Lidé, když nejsou schopni daný problém vyřešit sami, hledají radu na internetu. Na různých diskusních fórech se mnohdy nachází lidé, kteří stejný, nebo podobný problém řešili. Zde se nachází útočník. Útočník předstírá pomo své oběti a vytahuje potřebné informace, které jsou užitečné pro útočníka. [8]

Útočník může daný problém způsobit sám a až správci sítí budou konkrétní problém řešit, útočník bude připravený zaútočit. Tomuto postupu se říká reverzní sociální inženýrství a má tři fáze [8]:

- sabotáž – útočník zaviní chybu systému, kterou se snaží zaměstnanci vyřešit,
- inzerce – útočníky vyčkává na diskusních fórech, aby mohl pomoci případným obětím s vyřešením problému,

- asistence – útočník aktivně pomáhá oběti vyřešit konkrétní problém, ale získává i jinak nepřístupné informace.

1.2.6 Typy útoku

Typy útoků jsou rozděleny do dvou druhů [10]:

- fyzický kontakt s obětí
- útok pomocí internetu, nebo telefonu

Fyzický kontakt s obětí – útočník (vyjednavač) přijde za obětí, která nic netuší a snaží se dostat všechny potřebné informace, které potřebuje. Používá přitom metody spojené s vyjednáváním. Může ovlivnit situaci pomocí vystupování, charakteru, předem zjištěných informací apod. Oběť nemusí mít tušení, že jedná o citlivých informacích s útočníkem. Útočník může využívat styl získávání informací „něco za něco“ nabízí oběti například opravu počítače za citlivé informace.

Útok pomocí internetu, nebo telefonu – zde se jedná o útočné metody, při kterých útočník cílí na skupinu zejména starších lidí, kteří důvěřují podvodným e-mailům. Útok po telefonu může cílit na kohokoliv.

Dále lze sociální útoky rozdělit do tří kategorií, podle zaměření, které jsou [11]:

- technické,
- sociální,
- fyzické.

Útoky zařazené do technické kategorie se pohybují přes internet. Technická kategorie využívá sociálních sítí a webových stránek. Na těchto infikovaných webových stránkách, se shromažďují nelegální informace. Shromažďovat se mohou hesla, údaje o kreditních kartách apod. [11]

Sociální útoky už ke své činnosti potřebují lidskou interakci. Je zde cíleno na lidskou psychiku a emoce. Jedná se o nejnebezpečnější a nejúčinnější útoky. Příklady útoků využívající vztahu obětí na sociální vrstvě jsou například baiting (návnada), nebo spear phishing (rybaření oštěpem). [11]

Útočník provádí fyzické akce, aby se dostal k potřebným informacím. Jedná se například o prohledávání popelnic, nebo kontejnerů za účelem získání cenných dokumentů. [11]

1.3 Prostředky a cíle sociotechnického útoku

Cílem sociotechnického útoku je dostat se k osobním, nebo citlivým informacím osoby, nebo firmy. Útočník s těmito informacemi zachází de svého uvážení. Ve většině případů slouží získané informace k páchání nelegální činnosti, nebo k předání získaných informací třetí osobě za účelem vlastního obohacení.

Jako médium pro sociotechnický útok slouží kromě klasické pošty hlavně telefon a internet (e-mail, Facebook, Skype, Discord apod.). Zkušení sociotechnici mohou provádět i útoky "tváří v tvář". [9]

Jednoduchá přístupová hesla se dají uhádnou na základě chování člověka. Pokud útočník zná osobně potencionální oběť a ví jakým způsobem zadává svá hesla, je možné takové heslo prolomit hrubou silou. Čili neustálým zkoušením nových hesel. Časté hesla mohou být přezdívky, jména domácích mazlíčků, jména dětí, data a místa narození, název města apod. Pokud útočník nezná oběť osobně, aby mohl odhadnout použité heslo, využije například techniku phishing (rybaření), aby se k informacím dostal. [9]

Jako prostředek pro získání citlivých informací lze použít i různé vlastnosti lidské povahy člověka. Každý člověk je sám o sobě jedinečný, avšak lidské povahy se dají rozdělit do několika skupin. Útočník tak při získávání informací od oběti dokáže odhadnout, do jaké skupiny oběť patří. Po pečlivém prozkoumání zahájí útočník speciální útok pro konkrétní osobnostní vlastnost oběti. [12]

Vlastnosti lidské povahy jsou například [12]:

- autorita,
- sympatie,
- vzájemnost,
- společenský souhlas.

Autorita – zaměřuje se na vůli lidí podřídit se člověku jenž má moc. Například zaměstnanec a zaměstnavatel. Když se útočník bude vydávat za zaměstnavatele, nebo nadřízeného, může dostat od zaměstnance informace, ke kterým útočník nemá přístup. [12]

Sympatie – využívá lidské přirozené povahy pomoci lidem, kteří se nám zdají sympatičtí. Když se útočník představí oběti a jeho vystupování je slušné a přátelské, má útočník zvýšenou pravděpodobnost úspěchu. Při rozhovoru se útočník může dozvědět různé informace od oběti, jak je místo narození, oblíbený koníček, kde vyrůstal apod. Při konverzaci se útočník

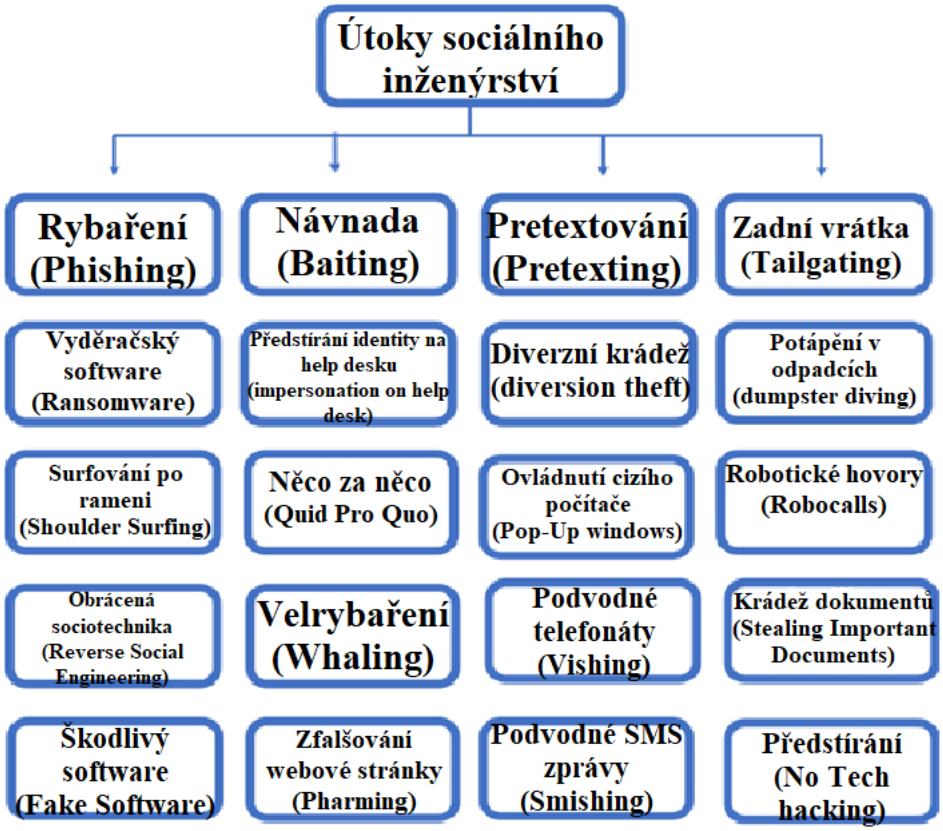
snaží přesvědčit oběť, že má stejný oblíbený koníček, vyrůstal ve stejném městě apod. Když budou mít oba lidé stejné, nebo velmi podobné zájmy a názory je pro útočníka snazší rozpovídat oběť, která si nemusí dávat pozor a vyzradí důležité informace. Při rozhovoru využívá útočník i napodobování chování, aby utvrdil v oběti pocit podobnosti. [12]

Vzájemnost – je využití pomoci, nebo darování daru oběti. Když útočník pomůže s vyřešením problému své oběti, nebo jen přinese přátelský dar, je v oběti probuzena touha daný čin oplatit. Touha oplatit daný dar, nebo službu se objevuje i po situaci, kdy oběť o žádný dar, nebo službu nežádala. [12]

Společenský souhlas – společenský souhlas využívá začlenění se do společnosti. Když s daným argumentem souhlasí většina, je snazší souhlasit taky než si udělat vlastní názor. [12]

1.4 Techniky sociálního útoku

Technik sociálního útoku je nepřeberné množství. Sociotechnici (útočníci) se pokoušejí každý den najít skulinu, kterou by mohli využít pro svůj prospěch a odcizit soukromá a citlivá data, nebo se dostat do prostor kde nemají co dělat. Na obrázku níže (obrázek 2) je vypsaných 20 vybraných útoků sociálního inženýrství.



Obrázek 2: Ukázka možných druhů sociologického útoku (Zdroj vlastní)

1.4.1 Phishing

Phishing (rybaření) je metoda sociálního útoku, při které útočník, nebo skupina útočníků využívá podvodné e-maily, telefon, nebo textové zprávy. Útočníci se vydávají za někoho jiného. Například oběť obdrží podvodný e-mail, jehož odesílatelem může být banka, kterou oběť využívá. Ovšem tento e-mail je falešný a rozkliknutím přiložených odkazů oběť přijde o důležité a cenné informace. [13]

Některé falešné e-maily jsou automaticky házeny do spam koše samotným e-mailem. Podvodný e-mail, který precizně vytvořen, se dá poznat pomocí automatického překladu do českého jazyka, což může výrazně ovlivnit důvěryhodnost e-mailu.

1.4.2 Pharming

Pharming (zfalšování webové stránky) je druh útoku, který využívá přesměrovávání uživatelů internetu. Běžný uživatel se snaží dostat na konkrétní webovou stránku, ale útočník, nebo skupina útočníků přesměruje oběť na falešnou stránku, která vypadá jako pravá. Vytvořené falešné stránky se snaží zachytit osobní identifikační údaje (PII – personally identifiable information) obětí, přihlašovací údaje apod. Útočníci se zaměřují na stránky, ze kterých mají největší potenciál dostat informace od oběti. Tyto stránky mohou být ve finančním sektoru, banky, platební platformy, elektronický obchod. Cílem útočníků je krádež identity. [14]

1.4.3 Baiting

Baiting (návnada) je jednoduchá metoda, která cílí na lidskou zvědavost. Útočník nastraží návnadu, což může být jakékoliv přenosné paměťové médium, a čeká až oběť spatří tuto návnadu. [15]

Příkladem baitingu může být flash disk s nahraným škodlivým softwarem, která je pohozená, nebo nechána na místě, kde si jí někdo všimne. Útočník spoléhá na lidskou zvědavost, která hraje v tomto druhu útoku klíčovou roli. Oběť jen připojí flash disk k počítači a útočník dosáhl svého cíle.

1.4.4 Pretexting

Pretexting (předpřipravený scénář) je metoda, která využívá předem vymyšleného scénáře, který vede k přesvědčení obětí, aby útočníkovi prozradily důležité informace. Útočníci využívající metodu pretextingu se snaží získat informace od společností tím, že se vydávají za

klienty. Útok je prováděn převážně po telefonu. Cíle útočníků jsou společnosti, které uchovávají klientská data. [16]

1.4.5 Vishing

Vishing (podvodné telefonáty), nebo také voice phishing (hlasové rybaření) je technika útoku, kde útočník využívá hovor přes mobilní telefon, aby získal důležité informace od oběti. Útočníci mohou k útoku využívat různé softwary pro úpravu hlasu, audionahrávky s dětským pláčem pro nátlak na emoční stránku oběti apod. [17]

1.4.6 Smishing

Útok pomocí telefonních zpráv (SMS). Tento druh útoku je prováděn automatickým generováním zpráv, které se odesílají náhodným uživatelům telefonního čísla. [18]

Zprávy mohou obsahovat pravopisné chyby, které jsou způsobeny automatickým překladem. Dále smishing mohou být klamné výherní zprávy typu: *„Vyhráli jste nový mobil, kliknutím na tento odkaz si o něj zažádáte“* a podobně. Cílová skupina jsou nejvíce senioři, nebo malé děti.

1.4.7 Whaling

Whaling (lov velryb, velrybaření) je útočná metoda sociálního inženýrství, při které se útočníci vydávají za někoho jiného. Útočník se může vydávat za vedoucího pracovníka ve firmě. Jedná se o cílený phishingový útok. Útočník pošle e-mail, který vypadá jak od vedoucího pracovníka firmy. Jenže tenhle email je infikovaný a oběť, která email otevře, pomůže útočníkovi získat cenná data, jako jsou bankovní účty, hesla, citlivé informace apod. [19]

1.4.8 Quid Pro Quo

Metoda Quid Pro Quo (neboli „něco za něco“) oplácí sdělení informace útočníkovi nějakou jinou informací, darem, či předmětem. Například útočník obvolává pracovníky firmy s dotazem, jestli nepotřebují pomoc s počítačem. Po poskytnutí pomoci si útočník vyžádá informace, které jsou pro něj důležité, nebo vzdálený přístup do počítače. [20]

1.4.9 Tailgating

Útočník následuje oběť, která mu pomůže projít do objektu. Pomoc ze strany oběti může být vědomá (tailgating), nebo nevědomá (piggybacking). [20]

1.4.10 No Tech Hacking

Druh sociálního útoku, který primárně nevyužívá informační a technické prostředky. Útočník například předstírá že je zaměstnanec firmy a při pohybu v budově získává informace. [21]

1.5 Nejčastější typy útoků

V bakalářské práci byl proveden průzkum mnoha zdrojů, ze kterých byl sestaven žebříček sedmi nejčastějších sociálních útoků.

1. phishing,
2. pretexting,
3. baiting,
4. whaling,
5. quid pro quo,
6. tailgating a piggybacking,
7. smishing a vishing.

1.6 Obrana proti sociálnímu inženýrství

Obrana proti sociálnímu inženýrství je vždy aktuální téma. Firmy vyplácí nemalé peníze na modernizace, automatizace a bezpečnost spojenou s nejmodernějšími prvky ochrany. Ať už se jedná o prvky mechanického zábranného systému, kamery, prvky poplachového zabezpečovacího a tísňového systému aj. Firmy, nebo spíše manažeři a lidé kteří rozhodují o školeních a modernizaci zabezpečovacích systémů často zapomínají na nejslabší článek, což je člověk. [22]

Obrázek 3 shrnuje jednotlivé oblasti sociotechnického útoku s použitými taktiky a způsoby obrany.

Oblast útoku	Sociotechnické taktiky	Obrana
Telefon (help desk)	Předstírání identity, přesvědčování	Zaměstnanci nesmí vydávat svá hesla a důvěrné informace
Vchod do budovy	Vniknutí v převleku	Průkazy, ostraha, trénink zaměstnanců
Kancelář	Nahlížení přes rameno	Hesla psát pouze s jistotou, že se nikdo nedívá
Kancelář	Procházení budovy a hledání odemknutých kanceláří	Každý host by měl být eskortován
Serverové místnosti	Pokus o logování, odstranění vybavení, nahrání trojského koně, který získává data	Serverové místnosti musí být pořád zamčené, měl by být veden inventář vybavení
Telefonní ústředna	Kradení linek a přesměrování	Kontrola meziměstských a mezikontinentálních hovorů
Odpadkové koše	Prohledávání odpadků	Odpadkové kontejnery v zabezpečené a monitorované oblasti, skartovat všechny důležité dokumenty, bezpečné mazaní magnetických medií
Intranet-Internet	Software na odchytávání hesel	Sledování programového vybavení počítačů
Kancelář	Zcizení dokumentů	Hierarchie důvěrnosti dokumentů a adekvátní zacházení s nimi

Obrázek 3: Oblasti sociologických útoků, taktika, obrana [8]

Mezi nejrizikovější skupinu lidí patří senioři a děti. Tyto dvě skupiny většinou nemají ponětí o sociálním inženýrství, a když jim na mobil přijde zpráva, že vyhráli nové auto v soutěži, pravděpodobně se pokusí zprávu otevřít. Tímto činem se mohou dostat na zavirované stránky. Stejná situace platí i pro řetězové e-maily. [22]

V praxi jsou ve firmách zaměstnaní dospělí lidé, kteří by měli mít o dané problematice potřebné informace, které jim pomůžou nenechat se nalákat. Je ale tahle informace opravdu pravdivá? Obrana proti sociálnímu inženýrství má ukázat možné způsoby, které mohou být aplikovány ve firmách. Jako možnou prevenci je možné zařídit pravidelné školení zaměstnanců. Změna hesla je další malý krok proti sociálnímu inženýrství. Je potřeba dbát na dostatečně silné heslo, které nebude použito pro všechny účty, pravidelná změna hesla a neodvoditelnost hesla z charakteru člověka.

V následujících podkapitolách bude probrána technikou ochranu před sociálním inženýrstvím a ochranu člověka před sociálním inženýrstvím.

1.6.1 Technická ochrana před sociálním inženýrstvím

Technická ochrana se dá pojmout z vícero úhlů, avšak výsledek zabezpečení by měl být stejný. Obrana proti tailgatingu je aplikování samo zavírajícího ramena na vstupní dveře, turnikety, příslušníci soukromé bezpečnostní složky apod. Vstupní dveře budou opatřeny fyziologickou kontrolou vstupu (otisk prstu). Dále je nutné zaměstnance poučit o vstoupení do objektu, to znamená, aby nedrželi dveře nikomu dalšímu, musí počkat u dveří, dokud se nezavřou, aby bylo zajištěno, že útočník nevnikne dovnitř. [23]

Ochrana proti baiting útoku spočívá v proškolení lidí. Když zaměstnanec najde podezřelý předmět, flash disk, paměťovou kartu, pevný disk, DVD, CD aj. neprodleně odevzdá nalezený předmět informačnímu oddělení. Dojde tak k zamezení nahrání škodlivého softwaru. [23]

Proti pretextingu, smishingu a vishingu je možné realizovat interní pevnou linku, na kterou nelze přesměrovat hovory odnikud než jen z dané firmy. [23]

Útok stylem něco za něco se musí odehrávat uvnitř firmy. Je potřeba proškolit zaměstnance, aby se s případným problémem obrátili na vedoucí oddělení, které zaměstnance přesměruje na oddělení pro jeho daný problém.

Ochranu proti farming útoku zajistí informačně technické oddělení (dále jen IT oddělení) firmy, kdy všem zaměstnancům zablokují přístup na jiné stránky, než které ke své práci potřebují. Je potřeba proškolit zaměstnance o problematice a zakázat nošení vlastních zařízení do práce. [23]

1.6.2 Ochrana člověka před sociálním inženýrstvím

Do ochrany člověka před sociálním inženýrstvím spadá phishing a no tech hacking. Možné zabezpečení proti phishingu může být proškolení zaměstnanců na podvodné emaily. Neotvírat emaily, které nemají žádnou spojitost s prací. Využívat firemní e-mail jen pro firemní účely, ne pro osobní. Tím se eliminuje riziko napadení. Před otevřením emailu, který se jeví jako podvodný je vždy lepší kontaktovat odesílatele. Když odesílatel žádný e-mail neposlal, jedná se o útok. [23]

Ochrana před no tech hackingem může být zrádná. Je potřeba dbát dostatečného soukromí při práci, aby potencionální útočník nemohl vysledovat použité heslo do systému. Při případném podezření na potencionálního útočníka, který si obhlíží okolí firmy, nebo dokonce

kanceláře, zavolat bezpečnostní službu. Proškolit zaměstnance o možném útoku bez technických prostředků. [24]

2 DEFINICE VYJEDNÁVÁNÍ

Vyjednávání je proces, při kterém se minimálně dvě strany snaží dosáhnout svých zvolených podmínek a přinutit druhou stranu s těmito podmínky souhlasit. Pojem vyjednávání je ve společnosti nejvíce spjat s terorismem. Kdy se teroristé a profesionální vyjednavači snaží dosáhnout svého a ve většině případů ohrožují nevinné civilisty. [25]

Vyjednávání se ovšem nachází všude. Ve firmách může zaměstnanec vyjednávat se šéfem ohledně zadané práce. V osobním životě rodiče vyjednávají s dětmi apod. Zkrátka, nemusí se vždy jednat o trestný čin ohrožující životy lidí.

2.1 Fáze vyjednávání

Celý proces vyjednávání se skládá z několika předem promyšlených fází. Fáze vyjednávání pomáhají určit směr, kterým bude celý proces směřovat. Podle předem připraveného plánu se člověk dokáže vyhnout nepříjemným situacím, které můžou vést ke špatnému výsledku vyjednávání. Fáze se dají popsat do pěti druhů. [26]

2.1.1 Příprava

Samotné vyjednávání začíná nejlépe ještě před samotným aktem. Je potřeba důkladně připravit plán, kterého je možné se držet. Zde je dobré si sepsat myšlenky, které mohou být v podobě otázek. Otázky mohou být například [27]:

- čeho chci dosáhnout?
- co jsem ochoten obětovat?
- jakou zvolím taktiku?
- čeho chce dosáhnout můj oponent?
- silné a slabé stránky oponenta?

Právě důkladným sepsáním otázek a pečlivou přípravou se šance na úspěch zvyšuje.

2.1.2 Volba strategie

V druhé fázi, tedy ve volbě strategie je potřeba rozhodnout jakou strategii zvolit. Volba strategie může být rozdělena do [27]:

- spolupráce,
- kompromis,
- konfrontace.

Spoluprací se rozumí, že vyjednavač má stejné plány jako oponent. Tudíž mají za úkol dosáhnout stejného výsledku a nejjednodušší způsob je spolupracovat. [27]

Kompromis vzniká v situacích, kdy je potřeba upustit od nějakého předem připraveného cíle, ale na oplátku je vyjednavači nabídnuto jiné řešení. [27]

Konfrontační řešení nastává tehdy, jestliže se jedna, nebo více stran snaží dosáhnout svého výsledku za každou cenu. [27]

2.1.3 Začátek vyjednávání

Začátek vyjednávání bývá o poslechnutí a pochopení druhé stany. Vyjednavač by se měl vcítit do situace oponenta, pochopit situaci a cíle, kterých chce druhá strana dosáhnout. Podle zjištěných informací se vyjednavač snaží zvolit nejoptimálnější variantu strategie. [27]

2.1.4 Průběh

Průběh vyjednávání se zpravidla liší podle dané situace. Odlišnosti budou při vyjednávání rodiče s dítětem ohledně večerky, nebo únosce obětí s profesionálním vyjednavačem.

V průběhu situace se vyjednavač snaží přinutit oponenta, pomocí sofistikovaných otázek, k přistoupení na podmínky, které určuje vyjednavač. Okolnosti a dané situace se rychle mění, proto je vhodné měnit styly strategií i v průběhu. [27]

2.1.5 Konec

Konec vyjednávání se dá rozdělit do 3 bodů:

- zdařilé vyjednávání,
- zdařilé vyjednávání s menšími změny,
- nezdařilé vyjednávání.

Zdařilé vyjednávání – vyjednavač byl úspěšný a podařilo se docílit všech cílů, které byly stanoveny.

Zdařilé vyjednávání s menšími změny – vyjednavač byl úspěšný, avšak nepodařilo se docílit všech stanovených cílů.

Nezdařilé vyjednávání – vyjednavač nebyl úspěšný. Nepodařilo se dosáhnout ani jednoho z vytyčených cílů.

Celé vyjednávání je řízeno podle dané situace. Připravený plán s postupem může vypadat sebelíp, ale v reálné situaci je potřeba pečlivě zvažovat každou změnu plánu. Někdy je lepší

vyjednávání řídit jiným stylem, než který je určen na papíře. Může to mít za následek rozsáhlé škody a v nejhorším případě i lidské životy. [27]

2.2 Základní pojmy vyjednávání

Podle složek Federálního úřadu pro vyšetřování (dále jen FBI) je vyjednávání rozděleno do pěti základních bodů, kterými se celý proces řídí. [28]

V bakalářské práci jsou základní pojmy vyjednávání shrnuty podle knížky „Nikdy nedělej kompromis: aneb vyjednávej tak, jako by ti šlo o život“ autor knihy je Christopher Voss. Pojmy vyjednávání jsou dlouhodobě vyvíjeny složky FBI, které se vyjednáváním s teroristy setkávají téměř každý den. Pojmy jsou tyto [28]:

- aktivní naslouchání,
- tón hlasu a intonace,
- zrcadlení,
- „černá labuť“,
- falešné domněnky,
- rozdíl mezi tím co dotyčný chce,
- rozdíl mezi tím co potřebuje (nezbytné minimum pro dosažení metody),
- taktická empatie,
- pojmenování (zopakování jeho úhlu pohledu),
- přehled obvinění.

2.2.1 Aktivní naslouchání

Aktivní naslouchání patří mezi nejzákladnější princip při vyjednávání. Jedná se o základní stavební kámen celé situace. Aktivní naslouchání je něco, co někteří lidé postrádají. Zejména s tímto naslouchání mají problém lidé s extrovertní povahou. Nejedná se jen o tiché sezení a dívání se na útočníka, když mluví. Taková situace naopak může celou událost ještě zhoršit. Útočník se musí cítit pochopen. Musí mít pocit, že mu vyjednavač rozumí. Aktivní naslouchání spočívá v opakování posledních slov. Jedná se o poslední slovo, až poslední tři slova. [28]

Například:

Osoba 1: „V práci dostávám málo peněz!“

Osoba 2: „Dostáváte málo peněz?“

Osoba 2 použila aktivní naslouchání osoby 1. Osoba 1 dostala pocit, že jí vyjednavač (v tomhle případě osoba 2) rozumí a může pokračovat rozhovor, který už nemá nekontrolovatelný průběh.

2.2.2 Tón hlasu a intonace

Tón hlasu a intonace při vyjednávání hraje podstatnou roli tón hlasu a intonace, která by se v průběhu akce neměla měnit. Z pravidla platí, když člověk slyší klidný hlas normálního, až lehce hlubokého tónu, funguje na lidský mozek klidněji. Když je útočník klidný, může přemýšlet racionálně a ne emočně. Emoční rozhodování je nepředvídatelné a může způsobit škodu. [28]

2.2.3 Zrcadlení

Při vyjednávání tváří v tvář je důležité dodržovat metodu zrcadlení.

Metoda zrcadlení napodobuje osobu takovým stylem, jako by se vnímal v zrcadle. Člověk, který využívá zrcadlení (vyjednavač) se snaží zrcadlit vše co zrcadlený subjekt dělá. Jedná se o hlas, pohyb těla, mimické výrazy apod. Techniku zrcadlení využívají jak zkušení vyjednavači při jednání s pachateli, ale i terapeuti, kteří se snaží od klienta dozvědět všechny podstatné informace. [29]

Zdroje zrcadlení jsou [29]:

- tělo,
- dech,
- slova,
- hlas.

Tělo – Zrcadlením těla se rozumí to, že zrcadlený subjekt (v našem případě oběť vyjednávání) vytváří pohyby těla, rukou, nohou, očí, mimických svalů apod. Vyjednavač opakuje tyto pohyby po oběti. Přiklad může být tento. Oběť zkříží ruce a opře se o židli, vyjednavač taktéž zkříží ruce a opře se o židli. [29]

Dech – Při zrcadlení dechu dochází k sladění rytmu a intenzity dýchání zrcadlené oběti. Při zrcadlení dechu si musí vyjednavač dát pozor, aby nevzbudil pozornost u zrcadlené osoby, jelikož by toto odhalení mohlo mít negativní vliv na průběh celé akce. [29]

Rozdělení dýchání lze takto [29]:

- hluboké, klidné dýchání,

- povrchní, rychlý dech,
- téměř neznatelný dech.

Slova – Zrcadlení slov je popsáno v bodu aktivního naslouchání. Zrcadlení řeči je úzce spjato s aktivním naslouchaním. [29]

Hlas – Zrcadlení hlasu je popsáno v bodu tón hlasu a intonace. [29]

2.2.4 Falešné domněnky

Falešné domněnky zahlcují nezkušené vyjednavače. Tím vyjednavač docílí špatnému odhadu situace a celé vyjednávání může skončit tragédií. [28]

2.2.5 „Černá labuť“

V knize: „Never Split the Difference: Negotiating As If Your Life Depended On“ (český překlad jako: „Nikdy nedělej kompromis: aneb vyjednávej jako by ti šlo o život“) od autora Christophera Vosse je černá labuť vysvětlena jako souhrn událostí, které předchází konečné situaci kdy je potřeba vyjednávat.

Například agresivní člověk jde přepadnout banku. Po cestě do banky zastřelí na ulici bezdůvodně tři občany. Právě tito zabití občani jsou tzv. „černé labutě“. Jde ze situace vyčíst, že agresivní člověk nemá zájem o vyjednávání, jen se chce zviditelnit před sebevraždou. [28]

2.2.6 Rozdíl mezi tím, co dotyčný chce a co potřebuje

Rozdíl mezi tím, co dotyčný chce a co potřebuje je jednoduchý. Každý člověk na planetě něco chce. Přiklad může být následovný. Normální běžný člověk by chtěl finanční nezávislost. Cíl tohoto člověka spočívá dostávat každý měsíc x set tisíc korun, aby nemusel nikdy pracovat. Tohle je případ toho, co dotyčný chce. Rozdíl tím, co potřebuje je například zvýšení platu v práci, nebo povýšení. [27]

2.2.7 Taktická empatie

Taktická empatie spočívá v rozeznání emocí v dané situaci a jejich pojmenování. [28]

2.2.8 Pojmenování

Pojmenování spočívá v přiřazení názvů jednotlivým problémům, které tíží člověka (útočníka). Práce vyjednavače je tyto problémy najít a správně pojmenovat. Cílem pojmenování je ukázání útočníkovi, že vyjednávač pozorně naslouchal jeho požadavkům a rozumí situaci,

která jej tíží. Například to může být: útočník vyřkne větu „Nedostává se mi mnoho pozornosti.“ Vyjednavač by si měl tuto informaci pojmenovat jakožto nedostatek pozornosti. Dále ve vyjednávacím cyklu bude snazší s touto informací pracovat. [28]

2.2.9 Přehled obvinění

Přehled obvinění si každý vyjednávač před vyjednáváním napíše na papír. Připravený přehled obvinění má mít za následek připravení se na nejhorší možné scénáře, které si druhá protistrana vymyslí. [28]

2.3 Cíl vyjednávání

V první řadě ještě, než vyjednávání vůbec začne, je potřeba určit cíl vyjednávání, aby bylo jasné, jakým směrem se bude případná situace vyvíjet. Sepsáním nejhoršího a nejlepšího cíle se člověk připraví na obě varianty a ve výsledku nepodlehne emocím. Když si člověk napíše jen nejlepší cíl, kterého chce dosáhnout a nedosáhne, lidské emoce v daný moment budou hrát významnou roly a daný člověk se muže stát na chvíli psychicky vyčerpaný ze selhání. [30]

Stanovením nejvyššího cíle, kterého chceme dosáhnout se vyjednavač připraví na situaci a nenastane situace, že by na nabídce prodělal. „Například prodávám televizi. Chci ji prodat za 3000 Kč, ale udělám si průzkum, zjistím že se stejná použitá televize prodává za 3500 Kč. Tak nastavím cenu na 3400 Kč a vím že jsem minimálně o 400 Kč v plusu.“ [28]

Při stanovení cíle je potřeba myslet rozumně. Není vhodné vymyslet nesmyslně šílenou cenu, za kterou by se konečný produkt nemusel prodat. Všechny plány a myšlenky, které si vyjednavač připravuje by měly být konzultovány s nezávislými lidmi. Odstraní se subjektivita.

3 SOUVISLOST VYJEDNÁVÁNÍ A SOCIÁLNÍHO INŽENÝRSTVÍ

Určitě vrozené sklony jsou do jisté míry podstatně ovlivnitelné vlivem kultury a prostředí ve kterém se daný jedinec nachází. Lidské sklony se dají ovlivnit i v průběhu života, například přeprogramováním lidského chování, příkazy a zákazy regulující lidské chování. [31]

Každý jedinec je vystaven vlivu okolí, které působí na lidské chování. Ať už člověk vyrůstá a starají se o něj rodiče, nebo je dospělý a stará se o sebe sám. Vždy nás svým způsobem ovlivňuje okolní vlivy. Můžou to být mravní zvyklosti, tradice, zákony, obyčeje, móda apod. Tyto faktory ovlivňují vystupování lidí, jejich postoje a chování. Očekává se, že se daný jedinec bude chovat a vystupovat, určitým způsobem, podle typu prostředí, které ho obklopuje. [31]

Člověk, který je od dětství vystavován vlivu okolí, které je za hranou zákona, lze očekávat že se bude projevovat určitými nelegálními činnostní. Vliv prostředí na jedince je velice důležitý. Hraje významnou roly v životě lidí. [31]

Sociotechnik ale nemusí vyrůstat v prostředí, ve kterém se okolní lidé pohybují v této nelegální činnosti. Člověk se může stát sociotechnikem z několika důvodů, buď má sám od sebe zájem o tuto činnost za účelem získávání citlivých informací a práci s nimi z nelegálního pohledu. Působil na něj negativní vliv prostředí, nebo je daný člověk otevřený zkoušení nových věcí a snaží se dosáhnout výsledků. [31]

Pokud se sociotechnik nechce zabývat pouze crackováním, nebo hackováním informačních zařízeních, je potřeba aby se naučil sociální stránku. „Práce“ sociotechnika zahrnuje mluvení s lidmi, jejich manipulace, vystupování, sebejistota a mnoho dalšího. [31]

3.1 Využití v praxi

Psychologie používána v praxi, tedy aplikovaná psychologie, je užita v mnoha společenských činností a jim odpovídajících institucí. Jak ukazuje obrázek (Obrázek 4) níže. Jsou to například [31]:

- Výchovně-vzdělávací,
- Zdravotnické instituce,
- Výrobní a obchodní instituce,
- Armáda,
- Sport,

- Umění a mnohé další.

Komunikace a interakce:	Oblasti praxe:
– komunikace	– organizace
– rétorika	– hospodářství
– trénink	– média
– moderování	– škola
– poradenství	– právo
– vyjednávání	– zdraví
– skupinová dynamika	– prostředí
– management konfliktu	– sport
– mediace	a další možnosti
– globalizace	
– inovace	
– management vědění	
a další možnosti	

Obrázek 4: Aplikovaná sociální psychologie [31]

Sociální psychologie a také vyjednávání má své místo v mnoha oborech. Může to být personální řízení čili oblast managementu, v politice, ve výrobních a jiných organizacích. [31]

II. PRAKTICKÁ ČÁST

4 EXPERIMENT

V bakalářské práci byl proveden experiment ohledně sociálního inženýrství. Jednalo se o formu vhishingu (sociální inženýrství po telefonu) a pretextingu (vymyšleného scénáře).

Cílem experimentu bylo vytáhnout citlivé, nebo jiné informace od lidí, společností, firem. Celý experiment postupoval za dozoru cílené oběti (člověk, který udělil souhlas). Kvůli ochraně GDPR nejsou v provedené práci zveřejněny jména obětí ani firem, lidí, společností, které byli napadeny.

Daný pokus byl rozdělen do 4 kategorií. Jsou to:

- rodiče,
- prarodiče,
- sourozenci,
- kamarádi.

Bylo tak učiněno z důvodů, že v každé situaci bude daný operátor, na kterého je vytvořen útok jednat jinak. Jinak bude komunikace probíhat, když zkoušený operátor bude vědět že útoční je vnuk starého pána, nebo když předstírá kamarádství s obětí.

Prováděný experiment znázorňuje, jaký byl celkový výsledek úspěšnosti útoku formou vhishingu. Za do provádění se v některých organizacích změnili operátoři, a tak jsou tyto změny zaznamenány i v provedené tabulce.

V použitých tabulkách jsou následující údaje:

- pořadové číslo,
- potencionální oběť,
- pohlaví oběti,
- věkový rozsah oběti,
- napadená firma / společnost,
- telefonní číslo,
- pohlaví operátora,
- grafický a číselný výsledek.

Ve všech 100 případech byla na konci rozhovoru ujasněná situace. Bylo řečeno že se jedná o experiment k bakalářské práci a zda dotyčný, nebo dotyčná obstáli. Při úspěšném pokusu útočníka bylo dále vysvětleno, jak v dané situaci reagovat a na co si dát příště pozor.

Experiment byl prováděn amatérem, který nemá vysoké zkušenosti s praktickou stránkou věci. Lépe připravený a zkušený profesionál by mohl dopadnout s výsledky mnohem lépe.

4.1 Oběti rodiče

V experimentu, jsou použity kontakty ve věkové kategorii 44–52 let. V tabulce (Tabulka 1) je znázorněno pět dobrovolníků, kteří souhlasili s provedením pokusu. Jak je patrné z tabulky 1, tato část experimentu dospěla k výsledku 24 nepovedených pokusů a 1 úspěšný pokus.

Úspěšný pokus spočíval v rezervaci lístků ve společnosti Cinema City. Oběť si rezervovala dva lístky na film, který se měl promítat. Útočník (člověk prováděcí experiment) se vydával za syna potencionální oběti. Útočník znal jméno potencionální oběti, a tak operátorovi bylo řečeno na jaké jméno by měly být lístky do kina objednány. Zrušením rezervace byl pokus považován za platný.

Tabulka 1: Tabulka obětí představující rodiče (Zdroj vlastní)

	Pořadové číslo	Potencionální oběť	Pohlaví	Věk (Rozsah)	Napadená Firma / společnost	Telefonní číslo	Pohlaví operátora	Grafický výsledek	Číselný výsledek jednotlivých sekcí	
									Ano	Ne
Rodiče	1	Matka	Žena	45 - 50	Komerční banka, a.s.	602 551 543	Žena	Ne	1	24
	2				O_2	543 235 770	Muž	Ne		
	3				Modrá pyramida	210 220 230	Žena	Ne		
	4				Všeobecná zdravotní pojišťovna ČR	952 222 222	Žena	Ne		
	5				T-Mobile Czech Republic a.s	800 73 73 73	Žena	Ne		
	6	Otec	Muž	47 - 52	Česká spořitelna, a.s.	956 777 497	Žena	Ne		
	7				Vodafone a.s.	800 777 777	Muž	Ne		
	8				Generali česká pojišťovna	241 114 114	Žena	Ne		
	9				MND Energie a.s.	800 400 500	Muž	Ne		
	10				Allianz pojišťovna, a. s.	241 170 000	Žena	Ne		
	11	Kamarád	Muž	47 - 51	Innogy, a.s.	800 113 355	Muž	Ne		
	12				Brněnské vodárny a kanalizace, a.s.	840 177 177	Muž	Ne		
	13				T-Mobile Czech Republic a.s	800 73 73 73	Žena	Ne		
	14				NetDeluxe	737 747 659	Muž	Ne		
	15				Vojenská zdravotní pojišťovna České republiky	222 929 199	Žena	Ne		
	16	Teta	Žena	43 - 47	ČEZ, a.s.	800 850 860	Žena	Ne		
	17				Kooperativa, a.s.	957 105 105	Žena	Ne		
	18				Netflix	800 050 701	Žena	Ne		
	19				O_2	543 235 770	Muž	Ne		
	20				Cinema City	255 742 021	Žena	Ano		
	21	Strejda	Muž	44 - 48	E.ON Energie a.s.	800 733 322	Žena	Ne		
	22				GasNet, s.r.o.	555 901 010	Muž	Ne		
	23				Modrá pyramida	210 220 230	Žena	Ne		
	24				Alexandria cestovní kancelář	270 007 007	Žena	Ne		
	25				Všeobecná zdravotní pojišťovna ČR	952 222 222	Žena	Ne		

4.2 Oběti prarodiče

Druhou formou experimentu bylo vydávání se za vnuka. Bylo cíleno na lidskou empatii, o kterou se útočník snažil. Cílem této části bylo zjistit, jestli člověk bude soucítit se situací že důchodci (prarodiče) jsou již starší lidé a ve většině případů nerozumí věcem, které se pojí s novodobou technologií a postupy při vyřizování dokumentů.

Ze zvolených firem / společností, které byly napadeny (viz Tabulka 2) se podařilo dosáhnout úspěchu jen u dvou útoků. Útoky byly zvoleny na lékárny, kde paní lékárnice měli pochopení s lidmi vyššího věku. Útočníkovi se podařilo obelstít pracovnice lékárny a byly by ochotné podat léky útočníkovi, aniž by s ním nemusel být přítomný senior.

Tabulka 2: Tabulka obětí představující prarodiče (Zdroj vlastní)

	Pořadové číslo	Potencionální oběť	Pohlaví	Věk (Rozsah)	Napadená Firma / společnost	Telefonní číslo	Pohlaví operátora	Grafický výsledek	Číselný výsledek jednotlivých sekcí	
									Ano	Ne
Prarodiče	26	Děda z matčiny strany	Muž	69 - 73	Všeobecná zdravotní pojišťovna ČR	952 222 222	Žena	Ne	2	23
	27				Dr.Max	516 770 100	Žena	Ano		
	28				Komerční banka, a.s.	602 551 543	Žena	Ne		
	29				T-Mobile Czech Republic a.s	800 73 73 73	Žena	Ne		
	30				Brněnské vodárny a kanalizace, a.s.	840 177 177	Muž	Ne		
	31	Babička z otcovy strany	Žena	68 - 72	BENU lékárna	212 812 812	Žena	Ano		
	32				E.ON Energie a.s.	800 733 322	Žena	Ne		
	33				Fio banka, a.s.	224 346 111	Žena	Ne		
	34				O_2	543 235 770	Muž	Ne		
	35				Allianz pojišťovna, a. s.	241 170 000	Žena	Ne		
	36	Kamarádův děda	Muž	68 - 72	T-Mobile Czech Republic a.s	800 737 373	Žena	Ne		
	37				MND Energie a.s.	800 400 500	Žena	Ne		
	38				Innogy, a.s.	800 113 355	Muž	Ne		
	39				UNIQA - úrazové pojištění	488 125 125	Žena	Ne		
	40				MONETA Money Bank, a.s.	224 441 111	Žena	Ne		
	41	Kamarádova babička	Žena	66 - 68	Všeobecná zdravotní pojišťovna ČR	952 222 222	Žena	Ne		
	42				Vodafone a.s.	800 777 777	Muž	Ne		
	43				Komerční banka, a.s.	800 521 521	Muž	Ne		
	44				Modrá pyramida	210 220 230	Žena	Ne		
	45				Innogy, a.s.	800 113 355	Muž	Ne		
	46	Dědova sestra z matčiny strany	Muž	63 - 67	O_2	543 235 770	Muž	Ne		
	47				Komerční banka, a.s.	800 521 521	Žena	Ne		
	48				Česká spořitelna, a.s.	956 777 497	Žena	Ne		
	49				BleskMobil	267 267 061	Žena	Ne		
	50				GasNet, s.r.o.	555 901 010	Muž	Ne		

4.3 Oběti sourozenci

V sekci, kdy se útočník vydával za sourozence obětí bylo dosaženo následujících výsledků. Jak ukazuje tabulka níže (Tabulka 3) neúspěšných pokusů bylo 24 a úspěšný pokus byl pouze 1.

Stejně jako u sekci „Rodiče“ je úspěšný pokus přiřazen společnosti Cinema City, kde se jednalo o zrušení rezervace, kterou udělala oběť (sestra). Útočník se vydával za sourozence dané oběti a rezervaci zrušil i když správně nemá na takovou akci oprávnění.

Tabulka 3: Tabulka obětí představující sourozence (Zdroj vlastní)

	Pořadové číslo	Potencionální oběť	Pohlaví	Věk (Rozsah)	Napadená Firma / společnost	Telefonní číslo	Pohlaví operátora	Grafický výsledek	Číselný výsledek jednotlivých sekcí	
									Ano	Ne
Sourozenci	51	Sestra	Žena	23 - 27	Všeobecná zdravotní pojišťovna ČR	952 222 222	Žena	Ne	1	24
	52				Air Bank a.s.	224 174 222	Žena	Ne		
	53				Allianz pojišťovna, a. s.	241 170 000	Žena	Ne		
	54				Cinema City	255 742 021	Muž	Ano		
	55				T-Mobile Czech Republic a.s	800 73 73 73	Žena	Ne		
	56	Bratranec	Muž	22 - 26	Netflix	800 050 701	Žena	Ne		
	57				Vojenská zdravotní pojišťovna České republiky	222 929 199	Muž	Ne		
	58				Fio banka, a.s.	224 346 111	Žena	Ne		
	59				Allianz pojišťovna, a. s.	241 170 000	Žena	Ne		
	60				Vodafone a.s.	800 777 777	Žena	Ne		
	61	Sestřenice	Žena	21 - 25	Vodafone a.s.	800 777 777	Muž	Ne		
	62				Netflix	800 050 701	Žena	Ne		
	63				Všeobecná zdravotní pojišťovna ČR	952 222 222	Žena	Ne		
	64				Fio banka, a.s.	224 346 111	Žena	Ne		
	65				Česká spořitelna, a.s.	956 777 497	Žena	Ne		
	66	Sestřenice 2	Žena	27 - 31	ČEZ, a.s.	800 850 860	Žena	Ne		
	67				Air Bank a.s.	224 174 222	Žena	Ne		
	68				Česká spořitelna, a.s.	956 777 497	Žena	Ne		
	69				UNIQA - úrazové pojištění	488 125 125	Žena	Ne		
	70				Všeobecná zdravotní pojišťovna ČR	952 222 222	Žena	Ne		
	71	Sestřenice 3	Žena	23 - 27	BleskMobil	267 267 061	Žena	Ne		
	72				MONETA Money Bank, a.s.	224 441 111	Žena	Ne		
	73				Česká spořitelna, a.s.	956 777 497	Žena	Ne		
	74				Netflix	800 050 701	Žena	Ne		
	75				Allianz pojišťovna, a. s.	241 170 000	Muž	Ne		

4.4 Oběti kamarádi

V poslední kategorii se útočník vydává za kamarády obětí. Z následující tabulky (Tabulka 4) je možné vyčíst počet úspěchů a neúspěchů.

V této kategorii je 23 neúspěšných útoků a 2 úspěšné útoky. Jedná se zase o útok na společnost Cinema City, konkrétně o zrušení rezervace.

Tabulka 4: Tabulka obětí představující kamarády (Zdroj vlastní)

	Pořadové číslo	Potencionální oběť	Pohlaví	Věk (Rozsah)	Napadená Firma / společnost	Telefonní číslo	Pohlaví operátora	Grafický výsledek	Číselný výsledek jednotlivých sekcí	
									Ano	Ne
Přátelé	76	Kamarád 1	Muž	23 - 27	Komerční banka, a.s.	800 521 521	Žena	Ne	2	23
	77				Nej TV a.s.	488 999 488	Žena	Ne		
	78				Generali česká pojišťovna	241 114 114	Žena	Ne		
	79				Alexandria cestovní kancelář	270 007 007	Žena	Ne		
	80				T-Mobile Czech Republic a.s	800 73 73 73	Žena	Ne		
	81	Kamarád 2	Muž	20 - 24	Cinema City	255 742 021	Žena	Ano		
	82				Grand Travel, s.r.o.	517 371 868	Muž	Ne		
	83				UNIQA - úrazové pojištění	488 125 125	Žena	Ne		
	84				MONETA Money Bank, a.s.	224 441 111	Žena	Ne		
	85				Vodafone a.s.	800 777 777	Muž	Ne		
	86	Kamarád 3	Muž	21 - 25	BleskMobil	267 267 061	Muž	Ne		
	87				Netflix	800 050 701	Žena	Ne		
	88				Allianz pojišťovna, a. s.	241 170 000	Muž	Ne		
	89				Raiffeisenbank	412 440 000	Žena	Ne		
	90				Vojenská zdravotní pojišťovna České republiky	222 929 199	Žena	Ne		
	91	Kamarádka 1	Žena	21 - 25	Vodafone a.s.	800 777 777	Žena	Ne		
	92				Cinema City	255 742 021	Žena	Ano		
	93				Fio banka, a.s.	224 346 111	Žena	Ne		
	94				Netflix	800 050 701	Muž	Ne		
	95				Generali česká pojišťovna	241 114 114	Žena	Ne		
	96	Kamarádka 2	Žena	20 - 24	Všeobecná zdravotní pojišťovna ČR	952 222 222	Žena	Ne		
	97				Netflix	800 050 701	Žena	Ne		
	98				Alexandria cestovní kancelář	270 007 007	Žena	Ne		
	99				Komerční banka, a.s.	800 521 521	Žena	Ne		
	100				BleskMobil	267 267 061	Muž	Ne		

5 VYHODNOCENÍ VÝSLEDKŮ EXPERIMENTU

V experimentu bylo provedeno 100 telefonátů, které byly rozděleny do 4 skupin. Každá skupina měla 5 dobrovolníků a po každým účastníkem bylo provedeno 5 telefonátů.

Ve skupinách „Rodiče“ a „Sourozenci“ bylo 24 neúspěšných útoků po telefonu a 1 úspěšný.

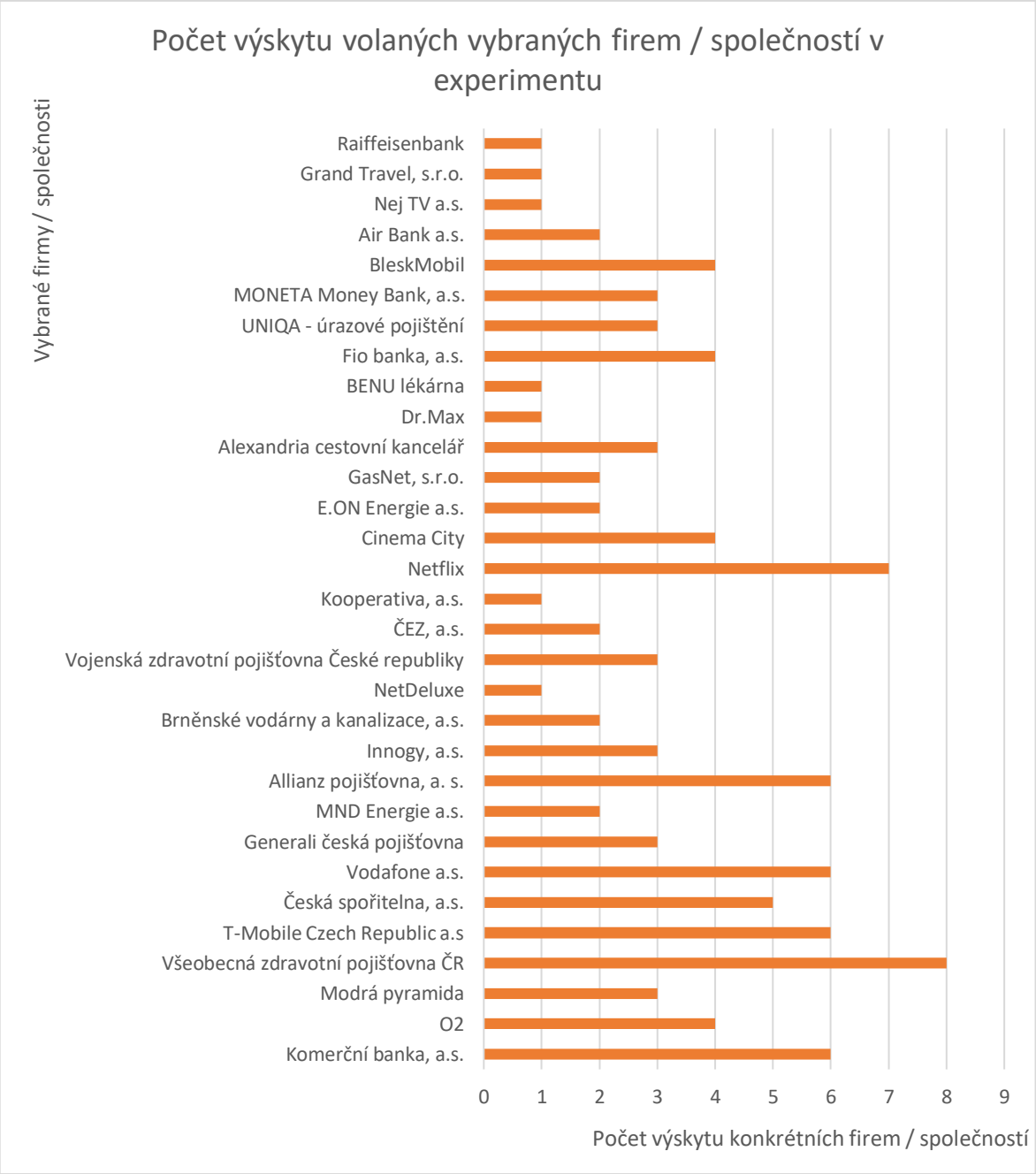
Ve skupinách „Prarodiče“ a „Kamarádi“ bylo 23 neúspěšných útoků po telefonu a 2 úspěšný.

Celková míra neúspěšnosti je 94 % a úspěšnosti 6 % jak ukazuje graf (Obrázek 5).

Obrázek 5: Graf celkové úspěšnosti experimentu (Zdroj vlastní)

V experimentu byly zvolené firmy a společnosti, které jsou znázorněny na grafu (Obrázek 6).

Celkem bylo zvoleno 31 firem a společností (viz Obrázek 6). Některé z těchto kontaktů byly použity vícekrát pod jinými dobrovolníky.



Obrázek 6: Počet výskytu volaných firem / společností (Zdroj vlastní)

5.1 Přínos experimentu

Přínosem experimentu byla myšlenka poukázat na lidský faktor ve firmách. Dbát dostatečného školení zaměstnanců na danou problematiku. Ukázat na problém sociálního inženýrství v jakékoli situaci. Zamyšlení se nad váhou rizika. Když takové výsledky zvládne naprostý amatér, čeho je schopný zkušený profesionál?

ZÁVĚR

Sociální inženýrství je stále aktuální téma. Patřičná část lidí si neuvědomuje, jaké riziko sebou tato činnost přináší. Jako první věc je definován rozdíl mezi útočníky, kteří využívají převážně informační a komunikační technologie pro svou legální i nelegální práci a mezi lidmi, kteří využívají techniky sociálního inženýrství.

Jak už bylo v bakalářské práci několikrát zmíněno, existuje nepřeberné množství sociotechnických útoků. Útočníci, kteří se snaží získat informace od jedince, nebo o celé společnosti využívají nelegálních praktik pro úspěch. Některé praktiky jsou více účinné, jiné jsou méně účinné. Ale pořád platí jedno. Nebezpečné jsou všechny.

Obrana proti sociálnímu inženýrství by měla být ve společnosti více diskutované téma. Lidé, kteří nejsou zvyklí často používat ke své práci informační a výpočetní techniku, jako je například osobní počítač, tablet, mobilní telefon, zanedbávají dostatečnou prevenci proti případným útokům. Nejznámější útok sociálního inženýrství, phishing (rybaření), je jeden z nejúspěšnějších a nejrozšířenějších útoků. I přes jeho povědomí se každým dnem najdou lidé, kteří jsou vystaveni jeho útoku a podlehnou.

Pro útočníky je snazší, z pohledu získání informací, zaútočit na člověka a pomocí svého vystupování na danou oběť zapůsobit a získat cenné informace než útok na techniku.

K sociálnímu inženýrství patří i schopnost vyjednávat. Bakalářská práce popisuje fáze vyjednávání, podle kterých se vyjednávací proces řídí. Umění vystupovat a mluvit s obětí je jedna věc, ale být schopný vyjednat „cenu“ za informace je věc druhá.

V bakalářské práci byl sestaven experiment, který využívá metod sociálního inženýrství. Jsou to metody vishing (podvodné telefonáty) a pretexting (předpřipravený scénář). Celý experiment je v souladu s GDPR (General Data Protection Regulation) o ochraně osobních údajů. Výsledky experimentu jsou zhodnoceny a je vyvozen závěr, který ukazuje na procentuální úspěšnost.

SEZNAM POUŽITÉ LITERATURY

[1] ZAVRŠNIK, Aleš. *Kyberkriminalita*. ČR: Wolters Kluwer, 2017. ISBN 978-80-7552-759-2.

[2] *Kdo je cracker* [online]. Praha: Aira GROUP, 2016 [cit. 2022-05-26]. Dostupné z: https://www.sprava-site.eu/cracker/

[3] *Kdo je to Podvodník?: Co znamená a jaký je význam slova Podvodník?* [online]. 2022 Superia.cz [cit. 2022-05-27]. Dostupné z: https://kdojeto.superia.cz/vlastnosti/podvodnik.php

[4] *All about malware* [online]. © 2022 All Rights Reserved [cit. 2022-05-29]. Dostupné z: https://www.malwarebytes.com/malware

[5] *A-Z Glossary of Information Security and Social Engineering Terms* [online]. Ireland: 2022 SecureClick | Privacy Policy [cit. 2022-05-29]. Dostupné z: https://www.itsecurityawareness.ie/a-z-glossary-of-information-security-and-social-engineering-terms

[6] *Social Engineering Terms Explained (with Examples!)* [online]. Copyright 2004 - 2022 Mitnick Security Consulting, 2021 [cit. 2022-05-29]. Dostupné z: https://www.mitnicksecurity.com/blog/social-engineering-terms-explained-with-examples

[7] *Thrashing* [online]. 2022 Techopedia [cit. 2022-05-29]. Dostupné z: https://www.techopedia.com/definition/4766/thrashing

[8] JIROVSKÝ, Václav. Sociální inženýrství. JIROVSKÝ, Václav. *Kybernetická kriminalita: Metody sociologického útoku*. Praha: Grada Publishing, 2007, s. 197. ISBN 978-80-247-1561-2.

[9] ŠIMEK, Richard. *Sociotechnika (sociální inženýrství)* [online]. Brno, 2003 [cit. 2022-05-14]. Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm. Kolokviální práce. Masarykova univerzita Brno, Faklulta informatiky.

[10] KOTKOVÁ, Dora. Sociální inženýrství: Speciální bezpečnostní technologie. 2016.

[11] SALAHDINE, Fatima a Naima KAABOUCH. *Social Engineering Attacks: A Survey* [online]. North Dakota, 2019 [cit. 2022-05-16]. Dostupné z: https://mdpi-res.com/d_attachment/futureinternet/futureinternet-11-

00089/article_deploy/futureinternet-11-00089.pdf?version=1554203904. Review. School of Electrical Engineering and Computer Science, University of North Dakota.

[12] HORNÍČEK, Jan. *SOCIÁLNÍ INŽENÝRSTVÍ: Sociotechnika a metody sociálního inženýrství* [online]. Zlín, 2009 [cit. 2022-05-14]. Dostupné z: https://digi-lib.k.utb.cz/bitstream/handle/10563/9113/horn%C3%AD%C4%8Dek_2009_bp.pdf?sequence=1&isAllowed=y. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce Ing. Jaroslava Gregušová.

[13] *What Is Phishing* [online]. KnowBe4 [cit. 2022-05-14]. Dostupné z: https://www.phishing.org/what-is-phishing

[14] *What Is Pharming and How to Protect Yourself* [online]. 2022 AO Kaspersky Lab. All Rights Reserved. [cit. 2022-05-14]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/pharming

[15] ČERMÁK, Miroslav. Baiting jak jej možná neznáte. *Clever and Smart* [online]. 2021, 26. 02. 2021 [cit. 2022-05-14]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/baiting-jak-jej-mozna-neznate/

[16] WILHELM, Thomas. Chapter 10 - Privilege Escalation. *Professional Penetration Testing*. Second edition. Printed in the United States of Americ: Copyright © 2013 Elsevier Inc. All rights reserved, 2013, s. 271-306. ISBN 978-1-59749-993-4.

[17] *What is Vishing?* [online]. © 2022. All rights reserved. [cit. 2022-05-15]. Dostupné z: https://www.proofpoint.com/us/threat-reference/vishing

[18] HODAČOVÁ, Veronika. Smishing. *Policie České republiky* [online]. © 2022 Policie ČR, 2021 [cit. 2022-05-15]. Dostupné z: https://www.policie.cz/clanek/preventivni-informace-smishing.aspx

[19] *What is a Whaling Attack?* [online]. 2022 AO Kaspersky Lab. All Rights Reserved [cit. 2022-05-26]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack

[20] HEJDA, Daniel. Techniky sociálního inženýrství: Security. *KPCS* [online]. Praha: 2016 - 2022 KPCS CZ | KPCS Consulting, 2020, 5.8.2020 [cit. 2022-05-27]. Dostupné z: https://www.kpcs.cz/cs/novinky/blog/techniky-socialniho-inzenyrstvi.html

[21] ŠELONG, Filip. Sociální inženýrství. *WikiKnihovna* [online]. KISK, ÚBK, ÚISK: Creative Commons, 2012 [cit. 2022-05-27]. Dostupné z: https://wiki.knihovna.cz/index.php?title=Soci%C3%A1ln%C3%AD_in%C5%BEen%C3%BDrstv%C3%AD

[22] JANDÁK, Jonáš. Sociální inženýrství a kyberprostor. *O₂* [online]. O2 Czech Republic a.s, 2021, 28.7.2021 [cit. 2022-05-27]. Dostupné z: https://blog.o2.cz/2021/07/28/socialni-inzenyrstvi-kyberprostor/

[23] KOVALČÍ, Marek. Metody sociálního inženýrství. *BDO Česká republika* [online]. BDO, USA ,LLP, 2021, 01.03.2021 [cit. 2022-05-27]. Dostupné z: https://www.bdo.cz/cs-cz/archiv/it-security/brezen-2021/metody-socialniho-inzenyrstvi

[24] ŠEVEČEK, Ondřej, Michael GRAFNETTER a Milan BORTEL. Jak na obranu proti Hackingu?. *GOPAS* [online]. Copyright © 2022 GOPAS, 2021, 11. května 2021 [cit. 2022-05-27]. Dostupné z: https://www.gopas.cz/jak-na-obranu-proti-hackingu-zeptali-jsme-se-nasich-odborniku

[25] *Jednání* [online]. Copyright By Economy-Pedia.com [cit. 2022-05-27]. Dostupné z: https://cs.economy-pedia.com/11031424-negotiation

[26] *VYJEDNÁVÁNÍ* [online]. [cit. 2022-05-27]. Dostupné z: https://vydavatelstvi-old.vscht.cz/knihy/uid_isbn-978-80-7080-657-9/vyjednavani.html

[27] *10 tipů, jak úspěšně vyjednávat: Konkrétní taktiky a příklady z praxe* [online]. Praha: myTimi, 2021 [cit. 2022-05-27]. Dostupné z: https://www.mytimi.cz/10-tipu-jak-uspesne-vyjednavat-konkretni-taktiky-a-priklady-z-praxe/

[28] VOSS, Christopher. *Never Split the Difference: Negotiating As If Your Life Depended On*. Jan Melvil publishing, 2016. ISBN 978-80-7555-002-6.

[29] *Technika zrcadlení* [online]. 2022 [cit. 2022-05-17]. Dostupné z: https://www.brainstools.cz/toolbox/koucink/technika-zrcadleni.htm

[30] *Strategie a taktika jednání* [online]. Praha: Copyright © 1997 - 2022 by Dashöfer Holding [cit. 2022-05-27]. Dostupné z: https://www.seniorzone.cz/33/definujte-si-zakladni-zasady-vyjednavani-uniqueidmRRWSbk196FNf8-jVUh4Ei2X4C2EHNhsECihpX3n1_vDQ6s4X3dldw/

[31] NAKONEČNÝ, Milan. *Sociální psychologie*. 2. Praha: Academia, 2009. ISBN 978-80-200-1679-9.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Apod. A podobně

Např. Například.

Aj. A jiné.

Tzv. Takzvaně

GDPR General Data Protection Regulation

SEZNAM OBRÁZKŮ

SEZNAM TABULEK