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. Ověřte pomocí analýzy stromem událostí.

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: **25. července 2022**
Termín odevzdání bakalářské práce: **19. srpna 2022**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

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

Ve Zlíně dne 25. července 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 návrh scénářů ukazuje na problematiku sociálního inženýrství v praxi.

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

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 draft scenarios point to the issue of social engineering in practice.

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

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 byl vytvořen návrh scénářů. Praktická část zahrnuje metodu vyjednávání a sociálního inženýrství. Byl sestaven plán odpovědí, podle kterých probíhá útok na oběť s cílem dostat citlivé informace. Byla zde použita metoda pretextingu. Samotný útok je veden po telefonu, nebo pomocí fyzického střetu s obětí. Celá praktická část práce byla vyhodnocena jako neověřená v praxi z důvodu nelegálnosti činnosti. Navržený scénář byl ověřen podle ETA analýzy.

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 další 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: „Koťátko“ může mít varianty „K0tatko“ a další. [5]

1.1.11 Záznam stisku kláves (Keylogger)

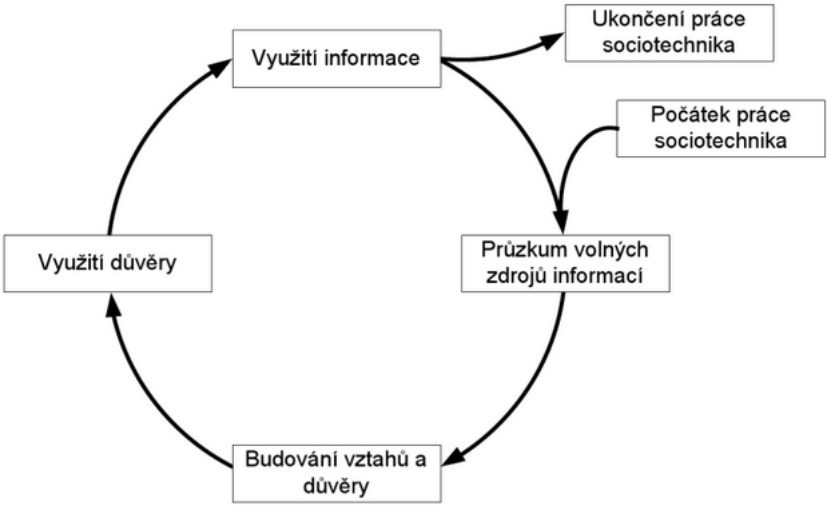
Záznam stisku kláves (Keylogger) je softwarové zařízení, které je nainstalováno do počítače, mobilu, tablet apod. Zaznamenává vše, co je stisknuto na klávesnici. Ať už se jedná o hesla, či přihlašovací údaje. Zaznamenaná data jsou odeslána útočníkovi, který je může použít k nelegální činnosti. [5]

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

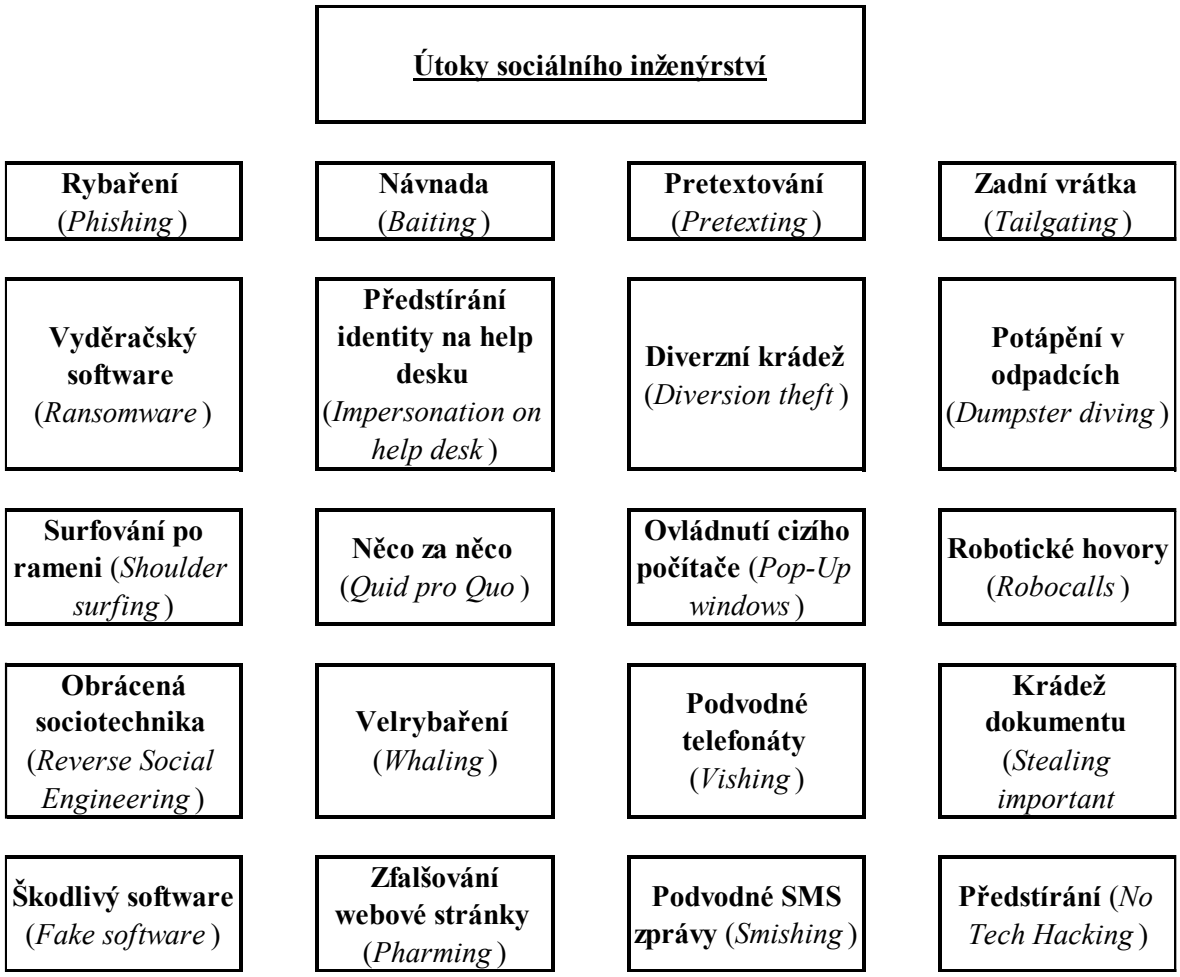
snaží přesvědčit oběť, že má stejný oblíbený koníček, vyrůstal ve stejném městě apod. Když budou mít oba lidé stejné, nebo velmi podobné zájmy a názory je pro útočníka snazší rozpovídat oběť, která si nemusí dávat pozor a vyzradí důležité informace. Při rozhovoru využívá útočník i napodobování chování,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

Tabulka 1 shrnuje jednotlivé oblasti sociotechnického útoku s použitými taktiky a způsoby obrany.

Tabulka 1: Oblasti sociologických útoků, taktika, obrana [8]

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

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]

Sociální inženýrství používá citlivé informace k získání přístupu, důvěry a dalších informací od lidí, aby od nich nakonec získali to, co chce útočník. [32]

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. 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]

Emoce jsou při vyjednávání vždy přítomné. Každý člověk se postupem času nechá vlastními emocemi ovlivnit i když může mít mnoho let zkušeností. Emoce při vyjednávání důležitým způsobem ovlivňují například tělo, myšlení, chování. Při vyjednávání je potřeba pochopit, a nenechat se ovlivnit vlastními emocemi. A také pochopení emocí druhé strany, s kterou člověk vyjednává, může pomoci splnit zájmy při vyjednávání vybudovat vztah s protějškem pro získání informací. [33]

3.1 Metody přesvědčování

Lidská důvěra ostatním lidem umožňuje útočníkům s námi lehce manipulovat a ovlivňovat. Opačný případ, kdy ovlivňování a přesvědčování lidí může vyvolat důvěru, je také pravda. Mezi principy přesvědčování patří: [34]

- vzájemnost,
- nedostatek,
- autorita,
- konzistence,
- záliba.

Vzájemnost – Vzájemnost může být způsobena darem, který dostaneme od jiné osoby (útočníka) za podmínkou vyvolat pocit povinnosti daný dar oplatit například vyzrazením informací o firmě ve které pracujeme. Této taktiky hojně využívají sociální inženýři, kteří se pokouší navázat spojení se svými oběťmi, že nejprve nabídnou informaci, nebo dar. [34]

Nedostatek – Metoda přesvědčování pomocí nedostatku (informací, nebo hmotných, či nehmotných předmětů) spočívá na lidské povaze. Když něco nemůžeme mít, chceme to o to víc. Tento psychologický trik funguje pořád a ani s příchodem internetu se to nezlepšilo. [34]

Autorita – Lidé mají tendenci následovat vedení důvěryhodných odborníků. Mnoho kybernetických zločinců chápe, že je důležité dát svým obětem jasně najevo, že jsou důvěryhodnými a informovanými autoritami pro své oběti, než se je pokusí ovlivnit. [34]

Konzistence – Lidé mají rádi konzistentnost s věcmi, které už někdy řekli, nebo udělali. Jakmile je oběť odhodlána ke spojení s útočníkem, který pomalu rozvíjí nátlak po malých kouscích, je pro oběť těžké se z tohoto spojení dostat. Oběť má pořád v hlavě myšlenku, že pomáhá útočníkovi, který má problém, a přitom dělá přesně to, o co ji útočník požádá. [34]

Záliba – Lidé mají tendenci více důvěřovat a spolupracovat s lidmi, kteří mají tyto tři základní faktory:

- Máme rádi lidi, kteří jsou nám podobní.
- Máme rádi lidi, kteří nám skládají komplimenty.
- Máme rádi lidi, kteří s námi spolupracují na společných cílech.

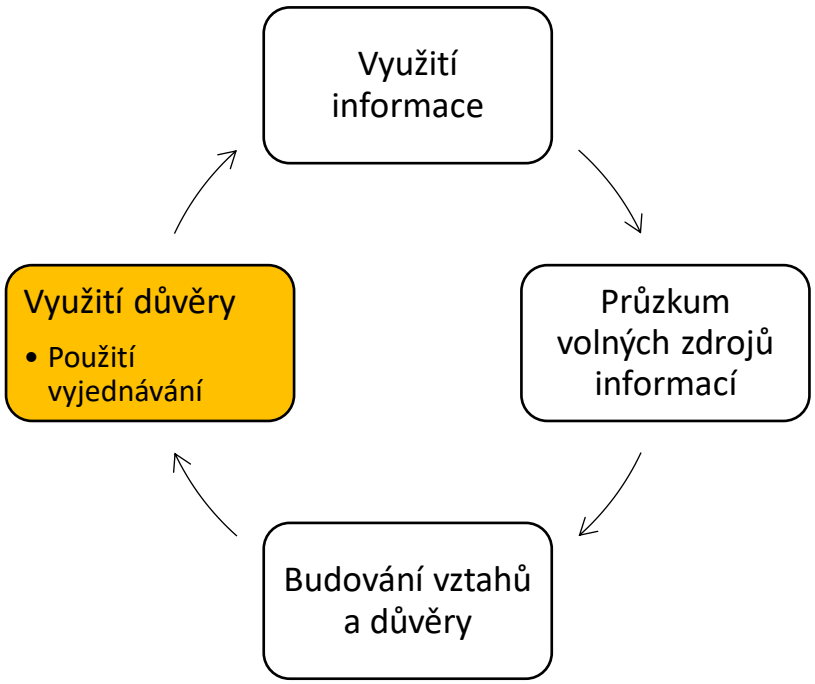
Jedná se o jednoduchý princip, který funguje dobře a má silné důsledky, které jsou kybernetičtí zločinci více než ochotni zneužít. [34]

3.2 Důležitost naslouchání

Na aktivním naslouchání spočívá vyjednávání, které je ve všem, co člověk dělá. V sociálním inženýrství se může jednat o udělání prvního dojmu na oběť, aby nepoznala Že postupem času z ní bude chtít útočník sebrat důležité informace. Při správné technice dochází u oběti k projevu empatie, která může vybudovat silnější důvěru mezi obětí a útočníkem. Tento postup umožní oběti cítit se bezpečně a vyjádřit své myšlenky a pocity. V tomto stavu už si oběť nedává pozor na to, co útočníkovi sděluje. [35]

3.3 Využití v praxi

V sociologickém útoku je vyjednávání vedeno jakožto dialog mezi dvěma, nebo více stranami. Útočník využívá vyjednávání až v předposlední fázi, chce s obětí navázat důvěrný vztah, který využije s úmyslem dosáhnout vzájemně prospěšného výsledku. Cílem je vyhnout se hádkám a sporům a dosáhnout nějaké formy kompromisu mezi stranami. [36]



Obrázek 3: Znázornění vyjednávání v cyklu sociologického útoku (Zdroj vlastní)

Obrázek (Obrázek 3) ukazuje v jaké fázi sociologického cyklu se využívá technika vyjednávání.

Důvěra je definována jako pocit sebejistoty vyplývající z ocenění vlastních schopností nebo kvalit. Aby bylo vyjednávání úspěšné, je potřeba zajistit silnou důvěru mezi útočníkem a obětí. Důvěru, mezi útočníkem a obětí, je velmi snadné ztratit pomocí špatně zvoleného

slova, nebo věty, se kterou oběť nebude souhlasit. Při dalším pokračování může dojít k obnově důvěry, ale oběť už bude vůči požadavkům útočníka ostražitější. [37]

Zvýšení sebedůvěry může být pomocí těchto bodů [37]:

- víra v sebe,
- praxe,
- záložní plán.

Víra v sebe – Jestli člověk pochybuje o svých schopnostech, znalostech, dovednostech a podobně je potřeba zabavit mozek, aby si člověk tyto informace nepřipouštěl a nejevil známky slabé sebedůvěry. Lidé vyřazující slabou sebedůvěru jsou pro okolí méně uvěřitelní a důvěra mezi útočníkem který si nevěří na útok a obětí bude téměř žádná. [37]

Praxe – Procvičování je potřeba v čemkoliv. Časté procvičování budování důvěry a sebedůvěry je nejlepší způsob, jak získat potřebné zkušenosti. Když člověk začne u malých prodejců zkoušet vyjednat lepší cenu, časem může vyjednávat ve světových firmách. Čím více bude člověk cvičit navazování důvěry, zvýší i jistotu ve všemožných situacích a bude pohodlněji vyjednávat. [37]

Záložní plán – vyjednávání, ať už v sociologickém útoku, nebo vyjednávání s dítětem, nemusí probíhat podle předem připraveného plánu. Jestli si útočník připraví více možností a alternativ, výrazně zvyšuje šanci na úspěch. [37]

II. PRAKTICKÁ ČÁST

4 NÁVRH SCÉNÁŘŮ

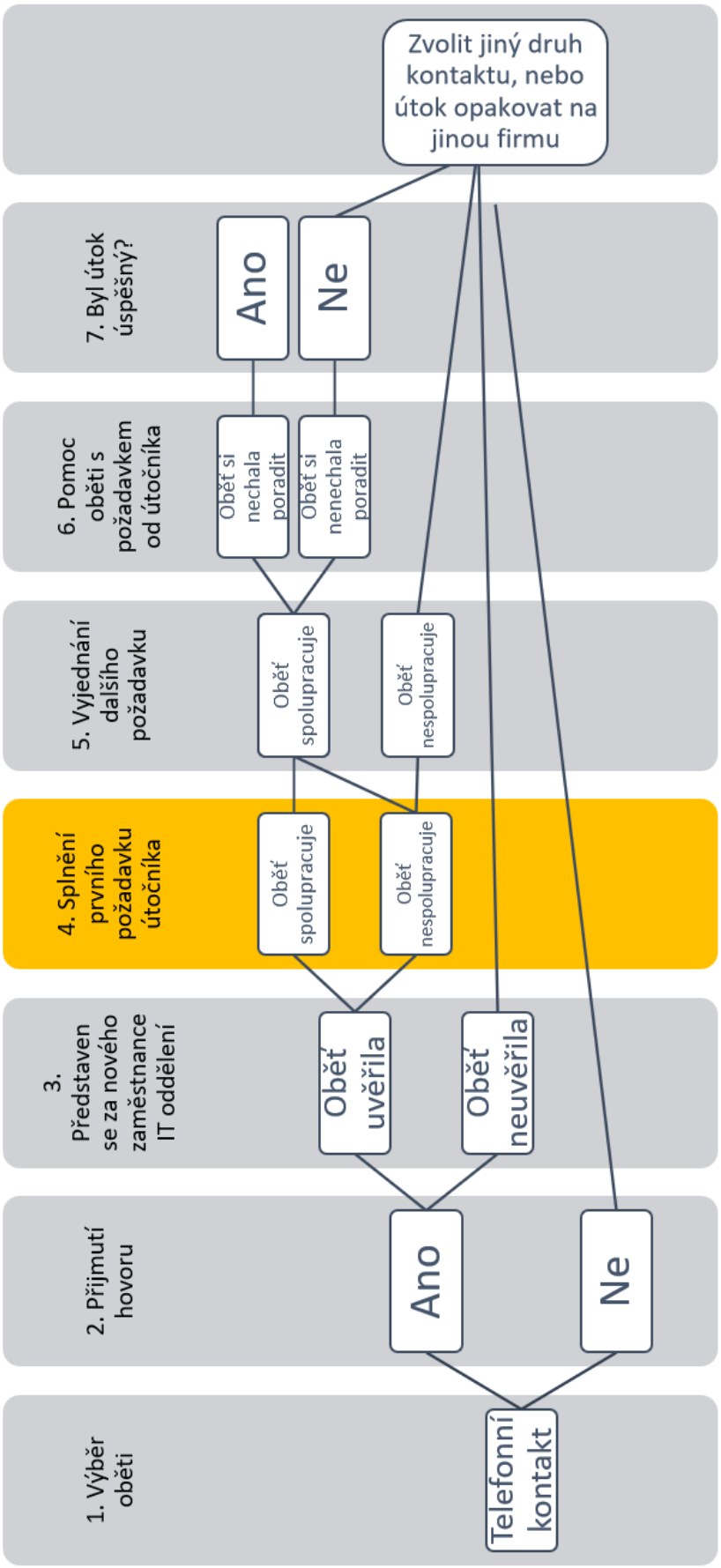
Navržené scénáře se skládají z techniky vyjednávání a techniky sociálního inženýrství. Je sestaven diagram řízeného rozhovoru. Ve scénářích je použita metoda pretextingu. Rozhovor využívá metody vyjednávání.

4.1 Scénář pomocí vzdáleného útoku na pracovníka firmy, útočník se představí jako IT pracovník

Jedná se o scénář útoku, který je veden po telefonu na pracovníka napadené firmy. Útočník se v této variantě představuje jako IT pracovník, který se pomocí připraveného scénáře na konkrétní problém se pokouší zmást oběť, aby mohl proniknout do firemního intranetu, nebo získat citlivé informace.

4.1.1 Navržený scénář 1

Jedná se útok vedeného pomocí mobilního telefonu. Scénář číslo 1, jak ukazuje (obrázek 4), je fiktivní zaměstnanec IT oddělení, který zavolá do firmy a pokouší se zaútočit na zaměstnance firmy. Útočník používá techniku vyjednávání, aby přiměl oběť splnit jeho požadavky a docílil tak úspěšného útoku. Cílem tohoto scénáře je získat kontrolu nad počítačem oběti, přistup do firemního intranetu, citlivé informace týkající se firmy, nainstalování škodlivého softwaru do počítače oběti a podobně. Obrázek (Obrázek 4) znázorňuje postup rozhovoru mezi útočníkem a obětí. Oranžové znázornění na (Obrázek 4) ukazuje, v jaké části rozhovoru je použita technika vyjednávání. Jedná se o vymyšlený scénář, který má jen jednu podobu. Realita může být jiná každý člověk reaguje jinak, a proto je velmi těžké podchytit všechny varianty.



Obrázek 4: Vymyšlený scénář 1

Obrázek (Obrázek 4) znázorňuje navržený scénář. Při zvolení negativní odpovědi by byl útok ukončen jako nezdařilý. Čtvrtý bod je znázorněn oranžovou barvu. Jedná se o barevné rozlišení, kdy se v útoku využívá technika vyjednávání.

4.1.2 Popis scénáře 1

Popis scénáře slouží k popsání jednotlivých bodů, jak ukazuje (Obrázek 4).

1. Útočník si vybere oběť a styl útoku, jestli bude útok fyzicky, nebo vzdáleně. V tomhle případě se jedná o vzdálený útok. Útočník zavolá do firmy.
2. Druhý bod rozhoduje, jestli útočníkovi někdo zvedne telefon.
3. Útočník se představí jako fiktivní zaměstnanec IT oddělení, který má nahlášený problém právě s počítačem oběti. V tomto scénáři se jedná o malware, který posílá data z počítače oběti někam mimo firmu. Má za úkol tento problém vyřešit. Útočník předstírá, že má za úkol tento problém vyřešit. Útočník se pokouší přesvědčit oběť, aby uvěřila falešnému příběhu.
4. Znázorněný čtvrtý bod ukazuje, kde se ve scénáři objevuje technika vyjednávání. Jedná se o **navázání důvěry** mezi útočníkem a obětí. Útočník položí oběti první požadavek. V případě že oběť odpoví negativně, celý útok nemusí být nutně ukončen. Díky vyjednávání je možné oběti přesvědčit, aby splnila druhý požadavek, který se pro oběť bude zdát jako jednodušší. Při spolupracování oběti hned od začátku je možné využívat její ochotu pro získání cenných informací.
5. Při spolupráci oběti od úplného začátku útoku, je pro útočníka snadné využít této pomoci co nejvíce pro svůj prospěch. Pokud ale oběť první požadavek odmítla, zde je možnost ji přemluvit, aby útočníkovi sdělila aspoň nějaké informace, které se na první pohled zdají nicneříkající.
6. Pomocí vyjednávání nabídne útočník oběti pomoc, jak dané informace získat, když mu je oběť následně poskytne. Všechno maskuji tím, že oběti opravuje počítač.
7. Sedmý bod scénáře je konec útoku, který může skončit pozitivně anebo negativně.

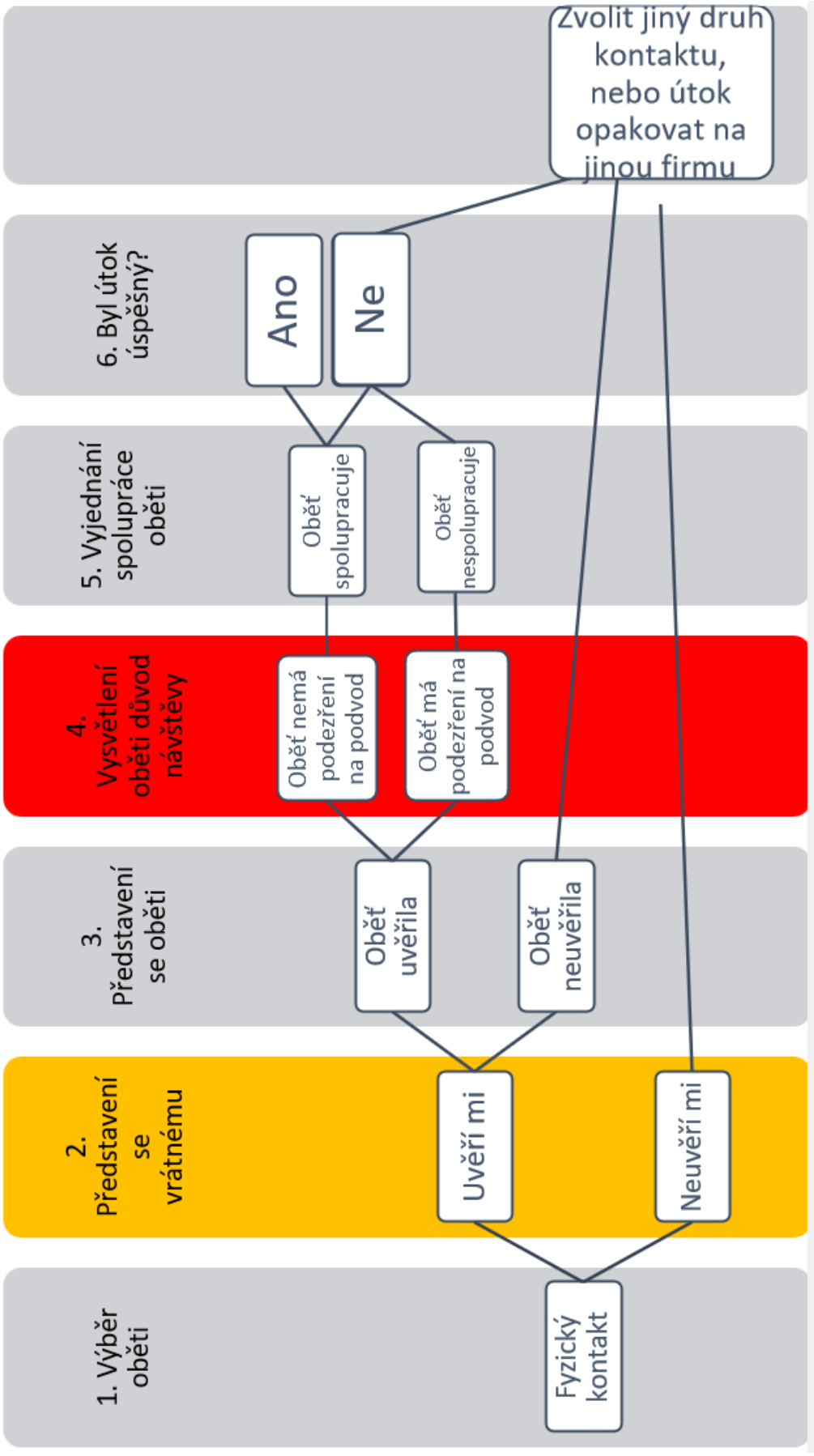
4.2 Scénář pomocí fyzického útoku na pracovníka firmy, útočník se představí jako IT pracovník

Jedná se o scénář fyzického útoku. Útočník se při útoku střetává fyzicky s napadeným pracovníkem napadené firmy. Útočník se v této variantě představuje jako IT pracovník, který

se pomocí připraveného scénáře na konkrétní problém se pokouší zmást oběť, aby mohl do počítače oběti nahrát škodlivý software, nebo získat citlivé informace.

4.2.1 Navržený scénář 2

Jedná se fyzický útok, kdy se útočník setká osobně s obětí. Scénář číslo 2 (Obrázek 5), je fiktivní zaměstnanec IT oddělení, který fyzicky přijde do firmy a pokouší se zaútočit na zaměstnance firmy. Útočník používá techniku vyjednávání, aby přiměl oběť splnit jeho požadavky a docílil tak úspěšného útoku. Cílem tohoto scénáře je získat kontrolu nad počítačem oběti, přistup do firemního intranetu, citlivé informace týkající se firmy, nainstalování škodlivého softwaru do počítače oběti a podobně. Použitý (Obrázek 5) znázorňuje postup rozhovoru mezi útočníkem, obětí a vrátným ve firmě. Oranžové zvýraznění, jak ukazuje (Obrázek 5) znázorňuje, v jaké části rozhovoru je použita technika vyjednávání s vrátným. Červené zvýraznění podle (Obrázek 5) znázorňuje v jaké části rozhovoru je použita technika vyjednávání mezi útočníkem a obětí. Jedná se o vymyšlený scénář, který má jen jednu podobu. Realita může být jiná každý člověk reaguje jinak, a proto je velmi těžké podchytit všechny varianty.



Obrázek 5: Vymyšlený scénář 2

Použitý (Obrázek 5) ukazuje diagram rozhovoru mezi útočníkem, vrátným a obětí. Barevné body jsou zvýrazněné, aby bylo na první pohled jasné, od kterého bodu v rozhovoru je použito vyjednávání, aby útočník dosáhl úspěšného útoku.

4.2.2 Popis scénáře 2

Popis scénáře slouží k popsání jednotlivých bodů, jak ukazuje (Obrázek 5).

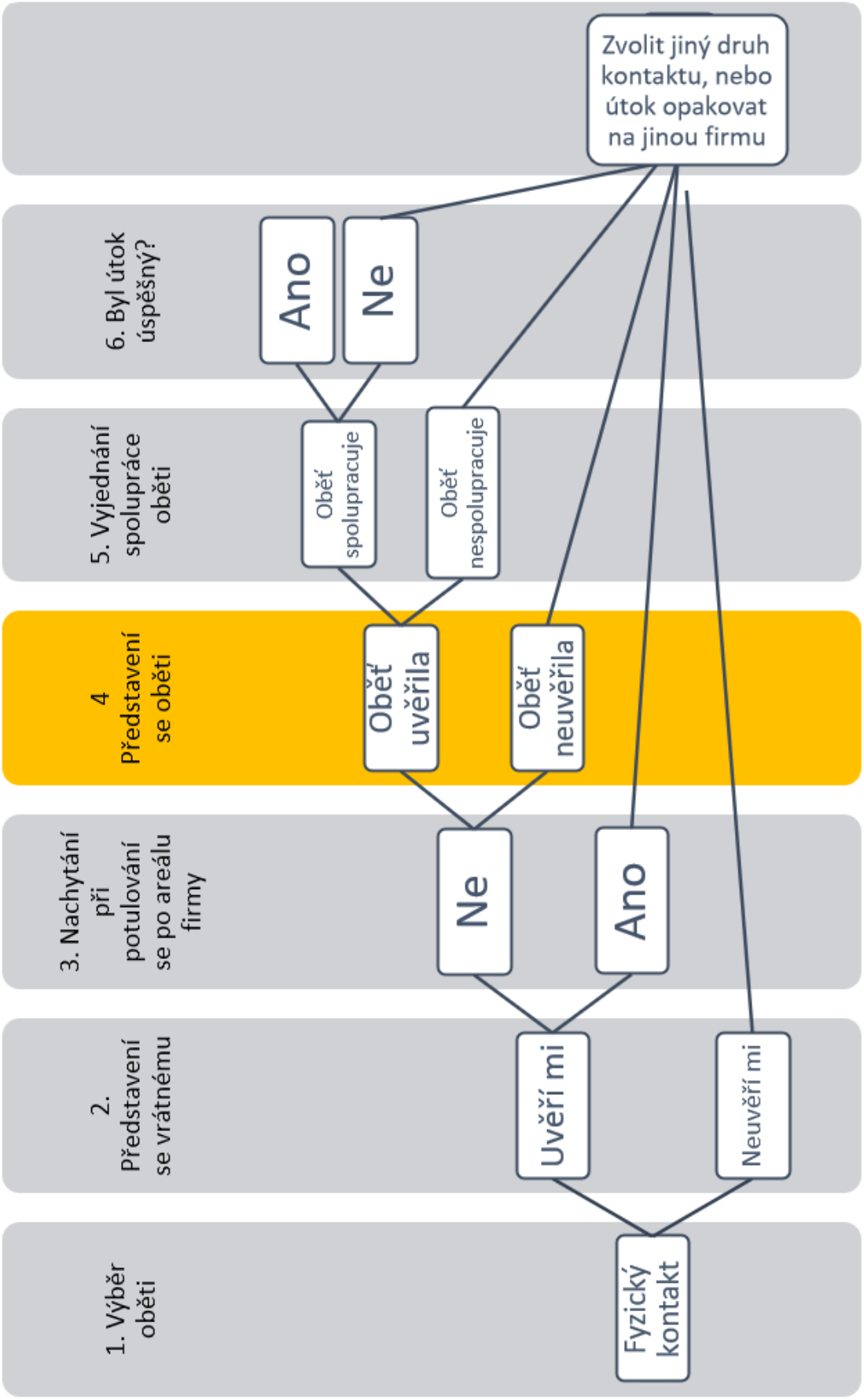
1. Útočník si vybere oběť a styl útoku, jestli bude útok fyzicky, nebo vzdáleně. V tomhle případě se jedná o fyzický útok. Útočník přijde do firmy.
2. Druhý bod ukazuje, že je mezi útočníkem a obětí použita technika vyjednávání, aby se útočník dostal dovnitř firemních prostor. Útočník má navržený scénář, že je pracovník IT oddělení a jde opravit počítač, který má v sobě údajně škodlivý software. Je zde použita technika vyjednávání cílená na **lidské emoce**.
3. Útočník se představí oběti jako fiktivní zaměstnanec IT oddělení, který má nahlášený problém právě s počítačem oběti. V tomto scénáři se jedná o škodlivý software (malware), který posílá data z počítače oběti někam mimo firmu.
4. Znázorněný čtvrtý bod ukazuje, kde se ve scénáři objevuje technika vyjednávání mezi útočníkem a obětí. Technika vyjednávání využívá **iluzi přátelství**. Útočník předstírá, že má za úkol vyřešit problém s napadeným počítačem. Útočník se pokouší přesvědčit oběť, aby uvěřila falešnému příběhu.
5. Když oběť uvěří falešnému příběhu, útočník vyjednává spolupráci s obětí, aby si usnadnil přistup k počítači a mohl do počítače nahrát škodlivý software (malware). Když oběť spolupracuje, pod záminkou, že usnadňuje práci odborníkovi, útočník má volný prostor působnosti a může s počítačem dělat co chce.
6. Šestý bod scénáře je konec útoku, který může skončit pozitivně anebo negativně.

4.3 Scénář pomocí fyzického útoku jakožto nový kolega

Jedná se o scénář fyzického útoku. Útočník se při útoku střetává fyzicky s napadeným pracovníkem napadené firmy. Útočník se v této variantě představuje jako nový kolega, který se pomocí připraveného scénáře snaží od napadených zaměstnanců dostat důležité informace o chodu firmy, citlivé informace, přístupy k omezeným datům, dostat se do prostor, kde je vstup zakázán a podobně.

4.3.1 Navržený scénář 3

Jedná se fyzický útok, kdy se útočník setká osobně s obětí. Scénář číslo 3 (Obrázek 6), je útočník představující se jako nový kolega, který fyzicky přijde do firmy a pokouší se od zaměstnanců firmy získat informace. Útočník používá techniku vyjednávání, aby přiměl oběť splnit jeho požadavky a docílil tak úspěšného útoku. Cílem tohoto scénáře je získat informace o zabezpečení firmy, provozním režimu, informace o hlídací službě a podobně. Použitý (Obrázek 6) znázorňuje postup rozhovoru mezi útočníkem, obětí a vrátným ve firmě. Oranžové zvýraznění, jak ukazuje (Obrázek 6) znázorňuje, v jaké části rozhovoru je použita technika vyjednávání s obětí. Jedná se o vymyšlený scénář, který má jen jednu podobu. Realita může být jiná každý člověk reaguje jinak, a proto je velmi těžké podchytit všechny varianty.



Obrázek 6: Vymyšlený scénář 3

Scénář (Obrázek 6) ukazuje diagram rozhovoru mezi útočníkem, vrátným a obětí (zaměstnancem firmy). Jedná se o vymyšlený scénář, jak by mohl vypadat útok útočníka na zaměstnance firmy, kdy se útočník představí jako nový kolega. Ve finále zjistil, jaké je zabezpečení firmy a jestli jsou bezpečnostní kamery neustále pod dozorem. Tento fakt by útočník mohl využit k předání informací o bezpečnostním posouzení firmy nějakému vandalovi, který následně firmu vykrade a způsobí tak finanční poškození dané firmě. oranžové zvýraznění (Obrázek 6) ukazuje, od jaké části rozhovoru je použito vyjednávání.

4.3.2 Popis scénáře 3

Popis scénáře slouží k popsání jednotlivých bodů, jak ukazuje (Obrázek 6).

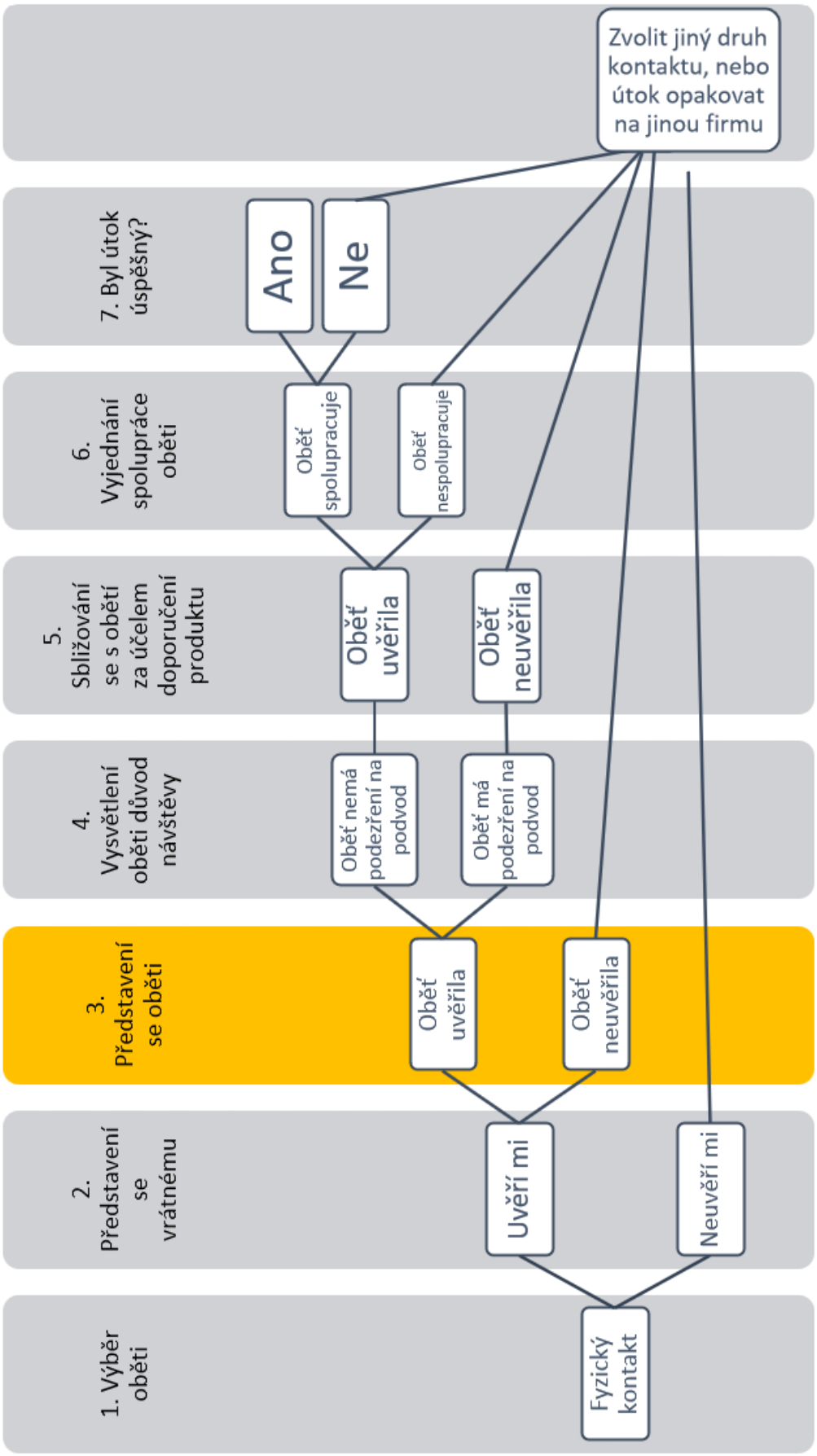
1. Útočník si vybere oběť a styl útoku, jestli bude útok fyzicky, nebo vzdáleně. V tomhle případě se jedná o fyzický útok. Útočník přijde do firmy.
2. Útočník přijde do firmy, kde jej odchytí vrátný. Představí se vrátnému a vysvětlí že zapomněl přístupovou kartu. Je zde použita technika sociálního útoku **„Quid pro Quo“ (Něco za něco)** Když vrátný pustí útočníka dovnitř, útočník slibuje že zítra si kartu určitě nezapomene. Vrátný si buď poznačí útočníkovo jméno a pustí ho dovnitř, nebo ho nepustí a útok končí.
3. Při nachytání útočníka při pohybu po areálu firmy by mohlo hrozit zavolání policie a celý útok by byl zmařen. Útočník se pohybuje po firmě a jejím areálu a zkoumá, jak všechno funguje, jaký je nastavený režim kontrol a podobně.
4. Představení se oběti a vysvětlení že jsem v práci nový a potřebuju poradit s informacemi, jak to ve firmě chodí. A kde, na jakých místech najdu různé kanceláře a podobně. Zároveň útočník používá metodu vyjednávání a její prvky, aby navázal s obětí přátelský vztah a dozvěděl se co nejvíce důležitých informací. Technika vyjednávání spoléhá na **lidské emoce** pomoci novému kolegovi a zároveň útočník **nabízí svou pomoc oběti**, když mu vysvětlí vhodné informace o dané firmě.
5. V pátém bodě útočník vyjednává spolupráci s obětí, aby mu řekl potřebné informace a nabízí mu své služby na oplátku. Při spolupráci oběti, je pro útočníka snadné využít této pomoci co nejvíce pro svůj prospěch.
6. Šestý bod scénáře je konec útoku, který může skončit pozitivně anebo negativně.

4.4 Scénář pomocí fyzického útoku jakožto obchodní partner

Jedná se o scénář fyzického útoku. Útočník se při útoku střetává fyzicky s napadeným pracovníkem napadené firmy. Útočník se v této variantě představuje jako obchodní partner, který se pomocí připraveného scénáře snaží od napadených zaměstnanců dostat důležité informace o chodu firmy, citlivé informace, přístupy k omezeným datům, dostat se do prostor, kde je vstup zakázán.

4.4.1 Navržený scénář 4

Jedná se fyzický útok, kdy se útočník setká osobně s obětí. Scénář číslo 4 (Obrázek 7), je útočník představující se jako obchodní partner, který fyzicky přijde do firmy a pokouší odpovědného pracovníka přimět spustit flash disk se škodlivým programem. Útočník používá techniku vyjednávání, aby přiměl oběť splnit jeho požadavky a docílil tak úspěšného útoku. Cílem tohoto scénáře je přimět oběť připojit flash disk, který obsahuje škodlivý software, k počítači a získat cenné informace Použitý (Obrázek 7) znázorňuje postup rozhovoru mezi útočníkem, obětí a vrátným ve firmě. Oranžové zvýraznění, jak ukazuje (Obrázek 7) znázorňuje, v jaké části rozhovoru je použita technika vyjednávání s obětí. Jedná se o vymyšlený scénář, který má jen jednu podobu. Realita může být jiná každý člověk reaguje jinak, a proto je velmi těžké podchytit všechny varianty.



Obrázek 7: Navržený scénář 4

4.4.2 Popis scénáře 4

Popis scénáře slouží k popsání jednotlivých bodů, jak ukazuje Obrázek 7.

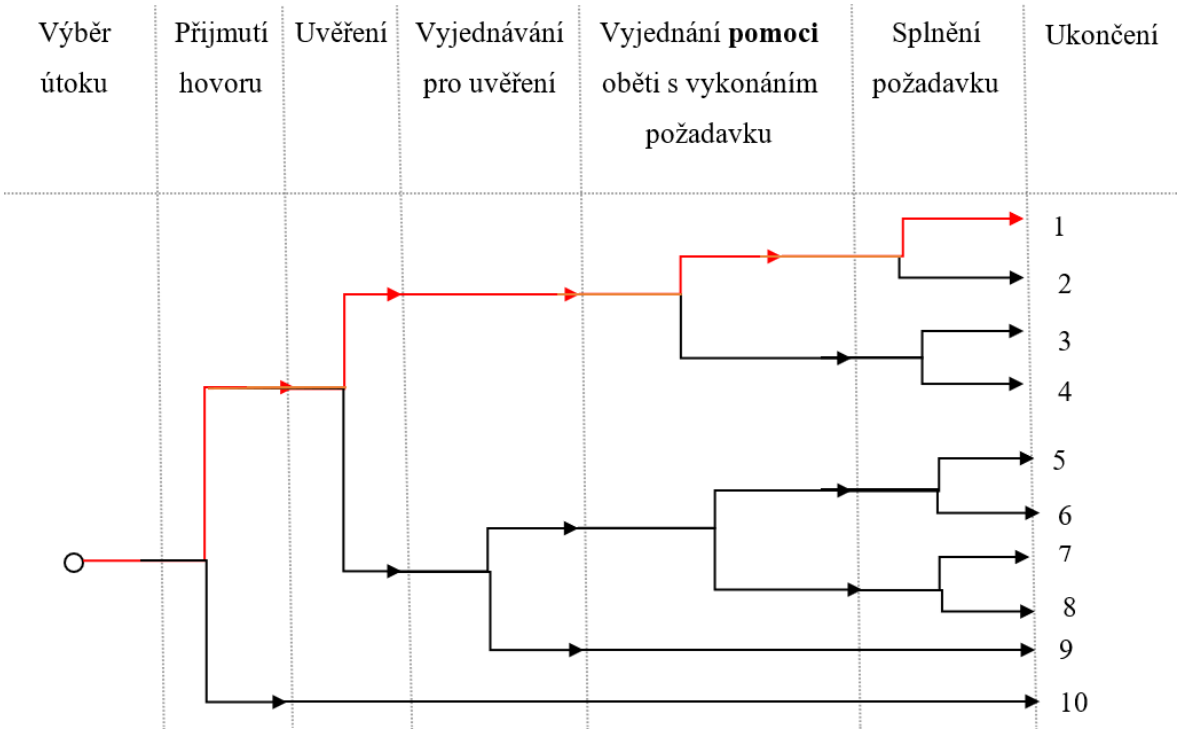
1. Útočník si vybere oběť a styl útoku, jestli bude útok fyzicky, nebo vzdáleně. V tomhle případě se jedná o fyzický útok. Útočník přijde do firmy.
2. Útočník přijde do firmy, kde jej odchytí vrátný. Představení se vrátnému a vysvětlí za jakým účelem přišel. Vrátný zavolá nadřízenému a pak buď útočníka pustí, nebo nepustí dovnitř.
3. Představení se oběti a vysvětlení za jakým účelem útočník přišel. Z jaké pocházím firmy, co nabízím a co pohledávám v jiné firmě. Při představení se oběti útočník využívá techniku vyjednávání, aby s obětí navázal důvěřivější pouto a zvýšil šanci na provedení útoku. Technika vyjednávání se zaměřuje na **důvěru v útočníka** a nabízí taky metody **„Quid pro Quo“** (něco za něco).
4. Nabídka oběti usnadnění a zlepšení přehlednosti bezpečnostních prvků pomocí softwarové aplikace. Nabídka vyzkoušení zdarma a volání kdykoliv, kdy bude mít oběť s aplikací problém. Útočník se takovým způsobem snaží navázat pouto mezi obětí a nabízí ji výhodnou aplikaci na zkušební dobu jednoho měsíce zdarma a po oběti zatím nechce nic. To se může zdát jako výhodná nabídka pro oběť a je velká šance, že bude útok úspěšný.
5. Sbližování se s obětí ve smyslu bavení se o stejném problému, který znají obě strany, jak útočník, tak i oběť. Oběť náhle dostane pocit, že se baví s přítelem, a útočník si takhle zvyšuje šanci na splněný útok.
6. Vyjednání spolupráce s obětí. Útočník nabízí zdánlivě výhodnou nabídku v podobě měsíčního vyzkoušení softwaru jejich firmy úplně zdarma. Dává tak oběti dar, který oběť bude chtít podvědomě vrátit. Když nebude mít čím, automaticky se pokusí tento čin oplatit vyzkoušením nového softwaru. Připojí infikovaný flash disk k počítači a útočník už bude mít vyhráno.
7. Sedmý bod scénáře je konec útoku, který může skončit pozitivně anebo negativně.

4.5 Vyhodnocení scénářů

Byl zvolen scénář, který bude vyhodnocen analýzou stromem událostí (Event tree analysis – dále jen ETA). Je sestavena tabula fází útoků (Tabulka 2) ve zvoleném scénáři. Na základě této tabulky a vybraného navrženého scénáře je navržena analýza ETA.

Tabulka 2: Tabulka fází útoku

Název fáze	**Charakteristika fáze**	**Jsou z firmy odcizené informace?**
Výběr útoku	Útočník si vybere způsob útoku. Fyzický, nebo vzdálený.	Ne
Přijmutí hovoru	Oběť zvedne telefon, nebo ve firmě nikdo nebude a telefon nezvedne	Ne
Uvěření	Oběť uvěří útočníkovi, který se představil jako IT zaměstnanec	Ne
Vyjednávání pro uvěření	Když oběť neuvěří útočníkovi, že se vydává za zaměstnance IT oddělení, je potřeba aby útočník s obětí vyjednával a pokusil se o zdařilý útok	Ano
Vyjednání pomoci oběti s vykonáním požadavku	Když oběť neví, jak má daný požadavek splnit. Útočník ji poradí a navede co má, jak udělat	Ano
Splnění požadavku	Když oběť spolupracuje, útočník chce docílit stavu, kdy oběť splní první požadavek, aby se mohl dostat k informacím	Ano
Ukončení	Útočník se rozloučí s obětí. Nic netušící oběť buď útok poznala a zamezila případným komplikacím, nebo útoku podlehla	Ne



Obrázek 8: ETA analýza navrženého scénáře 1

1. **Sociální útok byl úspěšný**. Útočník se do firmy dovolal. Oběť uvěřila útočníkovi jeho představení. Útočník pomohl obětí s plněním úkolů a oběť splnila požadavky, které útočník po oběti požadoval. Napadená firma **přichází o informace.**
2. *Sociální útok byl neúspěšný.* Útočník se do firmy dovolal. Oběť uvěřila útočníkovi jeho představení. Útočník pomohl obětí s plněním úkolů, ale oběť nesplnila požadavky, které útočník po oběti požadoval. Napadená firma *nepřichází o informace.*
3. **Sociální útok byl úspěšný**. Útočník se do firmy dovolal. Oběť uvěřila útočníkovi jeho představení. Oběť nechtěla pomoci od útočníka s plněním úkolů. Oběť splnila požadavky, které útočník po oběti požadoval. Napadená firma **přichází o informace**.
4. *Sociální útok byl neúspěšný*. Útočník se do firmy dovolal. Oběť uvěřila útočníkovi jeho představení. Oběť nechtěla pomoci od útočníka s plněním úkolů. Oběť nesplnila požadavky, které útočník po oběti požadoval. Napadená firma *nepřichází o informace.*
5. **Sociální útok byl úspěšný**. Útočník se do firmy dovolal. Oběť neuvěřila útočníkovi jeho představení. Útočník musel s obětí vyjednávat ohledně toho co má v úmyslu. Oběť uvěřila a chtěla pomoci od útočníka s plněním úkolů. Oběť splnila požadavky, které útočník po oběti požadoval. Napadená firma **přichází o informace**.
6. *Sociální útok byl úspěšný.* Útočník se do firmy dovolal. Oběť neuvěřila útočníkovi jeho představení. Útočník musel s obětí vyjednávat ohledně toho co má v úmyslu.

Oběť uvěřila a chtěla pomoci od útočníka s plněním úkolů. Oběť nesplnila požadavky, které útočník po oběti požadoval. Napadená firma *nepřichází o informace.*

7. **Sociální útok byl úspěšný**. Útočník se do firmy dovolal. Oběť neuvěřila útočníkovi jeho představení. Útočník musel s obětí vyjednávat ohledně toho co má v úmyslu. Oběť uvěřila, ale nechtěla pomoci od útočníka s plněním úkolů. Oběť splnila požadavky, které útočník po oběti požadoval. Napadená firma **přichází o informace**.
8. *Sociální útok byl úspěšný*. Útočník se do firmy dovolal. Oběť neuvěřila útočníkovi jeho představení. Útočník musel s obětí vyjednávat ohledně toho co má v úmyslu. Oběť uvěřila, ale nechtěla pomoci od útočníka s plněním úkolů. Oběť nesplnila požadavky, které útočník po oběti požadoval. Napadená firma *nepřichází o informace.*
9. *Sociální útok byl úspěšný*. Útočník se do firmy dovolal. Oběť neuvěřila útočníkovi jeho představení. Útočník musel s obětí vyjednávat ohledně toho co má v úmyslu. Oběť i nadále neuvěřila. Napadená firma *nepřichází o informace.*
10. *Sociální útok byl úspěšný*. Útočník se do firmy nedovolal. Napadená firma *nepřichází o informace.*

Byl vybrán navržený scénář 1 (Obrázek 4), který je analyzován pomocí analýzou ETA. V obrázku (Obrázek 8) je vybraný scénář červeně znázorněn. Cílem útoku bylo tyto scénáře dodržovat a řídit jimi rozhovor. Jsou vymyšlené varianty pro útok pomocí mobilního telefonu, i pomocí fyzického kontaktu s obětí. V rozhovorech je použito a znázorněno vyjednávání, které hraje v úspěšném útoku klíčovou roli.

Samotné scénáře nejsou v praxi bohužel ověřené. Sociální inženýrství a útoky na firmy, či instituce, podniky a podobně je na pokraji trestného činu. Z tohoto důvodu bylo vyhodnocení jako neověřený z důvodu legálnosti.

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 praktické části bakalářské práce byl vytvořen návrh scénářů. Praktická část zahrnuje metodu vyjednávání a sociálního inženýrství. Byl sestaven plán odpovědí, podle kterých probíhá útok na oběť s cílem dostat citlivé informace. Byla zde použita metoda pretextingu. Samotný útok je veden po telefonu, nebo pomocí fyzického střetu s obětí. Celá praktická část práce byla vyhodnocena jako neověřená v praxi z důvodu nelegálnosti činnosti. Navržený scénář byl ověřen podle ETA analýzy.

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.

[32] *NEGOTIATIONS NINJA* [online]. MWI, 2019 [cit. 2022-08-12]. Dostupné z: https://www.negotiations.ninja/blog/social-engineering-in-negotiation/

[33] SANPIETRO, Lara. Teach Your Students Negotiation Psychology. *PROGRAM ON NEGOTIATION HARVARD LAW SCHOOL* [online]. 2018, 19.3.2018 [cit. 2022-08-12]. Dostupné z: https://www.pon.harvard.edu/daily/teaching-negotiation-daily/teach-students-negotiation-psychology/

[34] KASSNER, Michael. 6 persuasion tactics used in social engineering attacks. *TechRepublic* [online]. 2020 [cit. 2022-07-22]. Dostupné z: https://www.techrepublic.com/article/6-persuasion-tactics-used-in-social-engineering-attacks/

[35] Active Listening: The Secret to Any Successful Negotiation. *SECURITY THROUGH EDUCATION* [online]. 2020 [cit. 2022-07-22]. Dostupné z: https://www.social-engineer.org/social-engineering/active-listening-the-secret-to-any-successful-negotiation/

[36] TEAM, CFI. Negotiation: What is Negotiation?. *CFI* [online]. CFI Education, 2020, 6.5.2020 [cit. 2022-08-12]. Dostupné z: https://corporatefinanceinstitute.com/resources/careers/soft-skills/negotiation/

[37] *Confidence in Negotiation- How Far Will It Get You?* [online]. Negotiations Training Institute, 2018 [cit. 2022-08-12]. Dostupné z: https://www.negotiationstraininginstitute.com/confidence-in-negotiation-how-far-will-it-get-you/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Apod. A podobně

Např. Například.

Aj. A jiné.

Tzv. Takzvaně

GDPR General Data Protection Regulation

SEZNAM OBRÁZKŮ

SEZNAM TABULEK