Sociální inženýrství jako metoda vytěžování osob

Bc. Adam Polášek

Diplomová práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Adam Polášek**
Osobní číslo:	**A16166**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Sociální inženýrství jako metoda vytěžování osob**
Téma anglicky:	**Social Engineering as a Method of Information Extraction**

Zásady pro vypracování:

1. **Seznamte se s problematikou sociálního inženýrství.**
2. **Uveďte nezbytnou terminologii a právní rámec.**
3. **Popište nejběžnější způsoby sociálního inženýrství.**
4. **Vypracujte systém testování zaměstnanců.**
5. **Tento systém testování zaměřte na průmysl komerční bezpečnosti.**
6. **Navrhněte školení zaměstnanců, které bude navazovat na předešlé testování.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **EKMAN, Paul. Odhalené emoce. Jan Melvil Publishing, 2015, 328 s. ISBN 9788087270813.**
2. **NAVARRO, Joe a Marvin KARLINS. Jak prokouknout druhé lidi: Příručka bývalého experta FBI. Grada, 2010, 224 s. ISBN 978-80-247-3350-0.**
3. **EKMAN, Paul. Emoce pod maskou. BIZBOOKS, 2015, 216 s. ISBN 9788026504221.**
4. **MITNICK, Kevin a William SIMON. Umění klamu. HELION, 2003, 348 s. ISBN 83-7361-210-6.**
5. **CIALDINI, B. Robert. Zbraně vlivu. Jan Melvil Publishing, 2012, 333 s. ISBN 978-80-87270-32-5.**
6. **HADNAGY, Christopher. Social engineering: The Art of Human Hacking. Indianapolis: Wiley Publishing, 2011, 408 s. ISBN 978-0-470-63953-5.**
7. **LONG, Johnny a Kevin MITNICK. No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. 1. Rockland: Syngress, 2008, 384 s. ISBN 978-1597492157.**

Vedoucí diplomové práce: **Ing. Dora Lapková**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. prosince 2017**

Termín odevzdání diplomové práce: **28. května 2018**

Ve Zlíně dne 8. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- 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 – diplomovou 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 diplomové 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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně, dne 18.5.2018

.....
podpis diplomanta

ABSTRAKT

Diplomová práce se zabývá problematikou sociálního inženýrství. Je zde uvedena nezbytná terminologie a právní rámec spojené se sociálním inženýrstvím. V teoretické části jsou popsány nejběžnější způsoby sociálního inženýrství. V praktické části diplomové práce je vypracován systém testování zaměstnanců, tento systém je zaměřen na průmysl komerční bezpečnosti. V závěrečné fázi praktické části je navrženo školení zaměstnanců, které má za cíl předejít vyzrazení senzitivních informací.

Klíčová slova: sociální inženýrství, social engineering card, systém testování zaměstnanců, školení zaměstnanců

ABSTRACT

This diploma thesis deals with the issue of social engineering. Necessary terminology and legal framework associated with social engineering are explained there. The theoretical part describes the most common methods of social engineering. A system of employee testing is developed in the practical part of the diploma thesis, this system is focused on the commercial security industry. In the final phase of the practical part, employee training is designed to prevent the disclosure of sensitive information.

Keywords: social engineering, social engineering card, employee testing system, employee training

Chtěl bych poděkovat mé vedoucí bakalářské práce **Ing. Doře Lapkové, Ph.D.** za její čas a trpělivost při konzultacích ohledně diplomové práce. Za její vstřícnost, ochotu a velkou spoustu cenných informací, které jsem zúročil při vypracovávání diplomové práce. Poděkování patří také **Ing. Lukáši Králíkovi**, který byl velice nápomocen při vypracovávání praktické části diplomové práce. Dále bych chtěl poděkovat své rodině a přátelům, kteří mi byli oporou. Také bych chtěl poděkovat vysoce postavenému manažerovi bezpečností firmy XY, který významným způsobem dopomohl k dokončení praktické části diplomové práce.

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

OBSAH

ÚVOD

Sociální inženýrství je v dnešní době široký pojem, který se zabývá hrozbami spojenými s vytěžováním senzitivních informací jak prostřednictvím internetu, tak prostřednictvím cílené konverzace. Hrozbou může být v dnešní době cokoli. Práce je zaměřená na sociální inženýrství v rámci průmyslu komerční bezpečnosti.

V práci je popsána terminologie, která je spojená se sociálním inženýrstvím. Zároveň také legislativa, která je s tímto tématem spojená. V práci jsou popsány nejběžnější způsoby sociálního inženýrství. Cílem diplomové práce je vytvoření systému testování zaměstnanců a zároveň také školení, které má za cíl předejít možnému vytěžování informací.

Teoretická část práce je zaměřena na vymezení pojmů týkajících se sociálního inženýrství. V první části je to historie a formy sociálního inženýrství. Další částí jsou sociotechniky, které jsou využívány v oblasti sociálního inženýrství. Následující část se zabývá neverbální komunikací, která je úzce spjata s tímto oborem. Neverbální komunikace může pomoct při praktikování cílené konverzace s osobou, od které chceme získat senzitivní informace.

V praktické části je vypracován systém testování zaměstnanců a jeho využití v praxi. Celý systém testování je rozdělen na dvě části. První část se zabývá využitím sociotechnik phishing a baiting v praxi. Byly navrhnuty dva EPC diagramy, které popisují postup průběhu testování. První diagram se zabývá sociotechnikou phishing, která je uskutečněna skrze elektronickou poštu. Druhý diagram se zabývá postupem při aplikování sociotechniky baiting pomocí USB flash disku. Bezpečnostní firma, se kterou bylo v průběhu práce spolupracováno, si nepřála být jmenována. Pro účely diplomové práce je tak využit fiktivní název – firma XY. Oba EPC diagramy byly představeny vysoce postavenému manažerovi bezpečnostní firmy XY. Návrhy se líbily, bohužel však nedošlo k jejich realizaci kvůli zdlouhavému procesu interního schvalování.

Druhá část praktické části diplomové práce se zabývá pojmem social engineering card. Je to systém testování zaměstnanců skrze cílený rozhovor za pomocí připravených kartiček, na kterých jsou umístěny otázky spadající do různých kategorií. Tento systém testování byl vyzkoušen v praxi.

Návaznou částí je poslední kapitola, ve které je navrženo opatření, které má zabránit možnému vytěžování informací, ke kterému může dojít během každodenního pracovního nasazení. Školení je rozděleno na více částí, kde má každá část jinou dobu trvání.

I. TEORETICKÁ ČÁST

1 SOCIÁLNÍ INŽENÝRSTVÍ

Sociální inženýrství je v této době chápáno jako souhrn prostředků a metod, díky kterým můžeme získat důvěrné informace nebo informace, které nám mohou být jakýmkoli způsobem prospěšné či užitečné. Základním předpokladem pro úspěšné využití sociálního inženýrství tkví v nevědomosti oběti tzn., ve chvíli, kdy je použita jedna z metod sociálního inženýrství, tak oběť netuší, že se snažíme získat potřebné informace a oběť nám tyto informace poskytne dobrovolně.

Jedna z nejvyužívanějších forem sociálního inženýrství je v dnešní době tzv. „bezkontaktní sociální inženýrství“. To znamená, že útočník nemá osobní kontakt s obětí. Jsou to techniky, které jsou nejrozšířenější přes internet, kde nejpoužívanější metodou je bezkonkurenčně phishing – je potřeba mít základní znalosti programování. Další formou využití může být tzv. „kontaktní forma sociálního inženýrství“, kde je potřeba využít osobního kontaktu s obětí, zástupcem této formy může být např. pretexing. Zde je potřeba mít základní povědomí o neverbální komunikaci a využít tak neverbální komunikaci ve svůj prospěch. [1]

Pachatelé využívají sociální inženýrství, protože je jednodušší obelstít samotného člověka, než obelstít např. software, který byl vytvořen s cílem chránit informace, které chceme získat (hesla, osobní údaje). Při úspěšném využití jedné z metod sociálního inženýrství nám totiž přístup k těmto informacím poskytne sám člověk, který s tímto softwarem pracuje. Nemusí to být ani člověk, který spravuje údaje, ke kterým se chceme dostat, ale cílem může být i obyčejný pracovník ochranky obchodu, který nám nevědomky může sdělit, jaká je trasa, kterou obchází, kdy má přestávku anebo kde se nachází kamery v objektu a které místo je tzv. „slepé“. [2]

V dnešní době je sociální inženýrství spojeno s kradením osobních údajů, jako jsou hesla nebo bankovní účty. Sociální inženýrství se dá však využít i k získání na první pohled zbytečných informací, které později v širším kontextu mohou posloužit např. k vyloupení objektu nebo k různým druhům krádeže.

Obecně je známo, že nejslabším článkem zabezpečení je lidský faktor. Pokud se zeptáme jakéhokoli člověka, který se pohybuje nebo pracuje v bezpečnostním průmyslu, kdo nebo co je nejslabším článkem komplexního zabezpečení např. objektu, tak odpoví, že je to člověk. [3]

1.1 Historie

Sociální inženýrství bývá v dnešní době spojováno spíše s hrozbami spjatými s internetem, a to například díky rozšířenosti metody phishing. Sociální inženýrství se však datuje do doby, kdy internet ještě neexistoval, a to do doby kolem roku 1918. Charles Ponzi (pravé křestní jméno Carlo), italský přistěhovalec, který se v roce 1918 přistěhoval do Ameriky. Přesvědčil své známé, aby mu půjčili peníze s vidinou vyššího výdělku (slíbil až zdvojnásobení vkladů). Peníze použil pro zaplacení starých dluhů, a tak to dělal pořád dokolečka. V roce 1920 se na podvod přišlo, od té doby se pojem Ponziho schéma běžně využívá.

Victor Lustig je český profesionální podvodník, který dělal podvody po celém světě. Nejvíce ho však proslavil podvod s Eiffelovou věží. V roce 1925, kdy se Francie zotavovala po první světové válce, se Lustig nacházel v Paříži. Přečetl si článek v novinách, že Eiffelova věz představuje velké náklady pro Paříž. Rozhodl se tedy, že Eiffelovu věž prodá. Zfalšoval vládní pozvánky a pozval největší obchodníky s kovovým odpadem, kteří v té době v Paříži fungovali. Představil se jako tehdejší ředitel Ministerstva pošty a telegrafů a vysvětlil jim, že je stavba pro Paříž moc nákladná a potřebují se ji zbavit. Vyzval obchodníky, aby mu do dalšího dne poslali peněžní nabídky, obchodníci tak učinili a Lustig vybral Andre Poisson, kterému věž nakonec prodal.

Dalším známým představitelem sociálního inženýrství je Frank Abagnale. Jeho příběh byl dokonce zfilmován pod názvem „Catch Me If You Can“ v českém překladu Chyť mě, když to dokážeš. Frank Abagnale se vydával jako pilot tehdejších aerolinek Pan Am, nechal si ušít stejnou uniformu, jakou používali piloti této společnosti. Nalétal tisíce kilometrů ještě jako teenager. Vydával se také za pilota, doktora nebo advokáta, mimo jiné dělal také podvody s šekovými směnkami. Později v průběhu své legální kariery stál u zrodu bezpečnostních prvků na šecích a bankovkách. [4]

Jedním z největších představitelů sociálního inženýrství je Kevin Mitnick, který započal dráhu podvodníka již ve dvanácti letech. Kevin Mitnick jako první v historii kombinoval obě formy sociálního inženýrství (výše zmíněné kontaktní a bezkontaktní sociální inženýrství). Jeho první úspěch byl, když ve dvanácti letech cestoval autobusem v Los Angeles do školy zadarmo. Dozvěděl se, kam se vyhazují staré raziče lístků, jednu si obstaral, spravil a tiskl si vlastní autobusové lístky. Když Mitnickovi bylo šestnáct, byl schopen obalamutit pracovníka softwarové firmy, aby mu přes telefon řekl přístupové heslo do jejich systému. Díky

tomu byl schopen zkopírovat software, který v té době společnost vyvíjela. S rychlým vývojem výpočetní techniky a možností se posunula i kreativita Kevina Mitnicka, který se byl později schopen, za pomocí sociálního inženýrství, nabourat do systémů společností jako Nokia, Motorola, Fujitsu Siemens apod. Mezi údajné činy patří nabourání se do systémů Pentagonu, FBI nebo paradoxně do firmy, která se specializuje na síťové operační systémy a jejich bezpečnost Novell. V roce 1995 byl Mitnick dopaden, v roce 2002 vydává svoji první knihu s názvem „Umění klamu“. V současné době se aktivně podílí na předcházení úspěšného užití sociálního inženýrství, ve všech jeho formách, v praxi. [4]

1.2 Terminologie

S pojmem sociální inženýrství souvisí také terminologie, která je s tímto oborem spjata. V následující podkapitole je uvedena základní terminologie, se kterou je možné se v práci setkat. Další pojmy jsou vysvětleny v následujících kapitolách.

1.2.1 Senzitivní (citlivé) informace

Informace jako taková je jednotné ucelené sdělení, které může být v písemné nebo ústní formě. Senzitivní informace je informace, která vyžaduje ochranu. Její neoprávněné použití nebo zveřejnění by mohlo způsobit škodu instituci nebo osobě, které se tato informace týká. Mezi senzitivní informace patří osobní údaje nebo ekonomické údaje. [5]

1.2.2 Cílený rozhovor

Cílený rozhovor je rozhovor, který má za cíl zjistit něco konkrétního, zjistit konkrétní informaci. Pro zvládnutí cíleného rozhovoru je potřeba určitá míra verbálních i neverbálních zkušeností a využití těchto zkušeností v praxi. Cíleným rozhovorem může být například pohovor.

1.2.3 Zájmová osoba

Zájmová osoba je osoba, která je předmětem zájmu. Může se jednat o osobu, která je podezřelá ze spáchání trestného činu anebo to může být osoba, jejíž postavení může disponovat informacemi, které jsou předmětem zájmu. Pro účely diplomové práce jsou zájmovými osobami pracovníci v průmyslu komerční bezpečnosti. [6]

1.2.4 Vytěžování osob

Vytěžování osob je jedna z metod detektivní činnosti. Cílem této disciplíny je získání informací. Důležitá je schopnost komunikace a přizpůsobení se k dané situaci. Žádná konverzace se nevyvíjí podle očekávání, proto je důležitá improvizace. Rozdíl oproti cílenému rozhovoru je v navázání kontaktu a ve správném vedení rozhovoru. Další rozdíl je v délce zjišťování informací o daném člověku. Je důležité sledovat neverbální komunikaci a přizpůsobit tomu rozhovor. Vytěžování osob může předcházet příprava formou vhodně sestavených otázek. V rámci této práce bylo vytěžování vyžito na pracovníky bezpečnostních služeb. [7]

1.3 Formy sociálního inženýrství v dnešní době

Sociální inženýrství může mít více podob. V jedné její podobě se se sociálním inženýrství můžeme setkat přes internet (bez fyzického kontaktu), kdy člověk využívá znalosti a zkušenosti spojené s vytěžováním informací, ke kterým nepotřebuje fyzický kontakt. Útočník může navázat komunikaci přes email nebo přes sociální sítě, které jsou v dnešní době nejrozšířenější formou komunikace a lidé si zde nedávají moc pozor na soukromé informace nebo na informace, které pomocí chatu sdělují svým známým. Dalším způsobem může být třeba, pro někoho zastaralá, emailová komunikace.

Druhou, často opomíjenou, formou sociálního inženýrství je tzv. kontaktní sociální inženýrství. Předpokladem pro úspěšné využití této formy je základní znalost lidského chování, vhodné použití a také využití neverbální komunikace. [8]

1.3.1 Emailová komunikace

Email byl a doposud je cílem mnoha útoků, jelikož email je asi nejjednodušší způsob, jak se dostat k zájmové osobě. Pokud je útočník dostatečně zručný a podaří se mu, využitím nějaké z technik sociálního inženýrství, dostat k heslu emailu oběti, tak se může jednoduše dostat i do účtů na sociálních sítích jako je Facebook, Twitter apod. Pachatel se nemusí k heslu dostat pouze s využitím technik sociálního inženýrství ale i využitím sofistikovaného softwaru – počítačového viru, který může zaznamenávat stisknutí klávesnice a odesílat je útočníkovi. Nebo může využít techniky tzv. „brutální síly“ (brutal force), kdy útočník vytvoří program, který opakovaně zadává hesla do přihlašovacího formuláře. Seznam hesel je dostupný na internetu, některé seznamy obsahují až půl miliardy hesel.

Pokud se tedy útočníkovi podaří proniknout do emailu, dostane se tak ke kontaktům oběti. Za předpokladu, že si oběť nevšimne vnějšího narušení bezpečnosti emailového účtu, dostává tak útočník možnost využít kontaktního seznamu oběti a rozeslat podvodné emaily s cílem získat důvěrné informace nebo dokonce hesla.

Zpráva, kterou útočník může odeslat kontaktům oběti, může mít několik podob. Ve zprávě může být obsažen odkaz, který oběť odkáže na fiktivní stránku, ze které se automaticky bez jeho vědomí stáhne do počítače škodlivý malware, který dá útočníkovi přístup do počítače. Zpráva může také obsahovat přílohy, které mohou být také infikované výše zmíněným malwarem. Předpokladem pro úspěšné využití je důvěřivost a zvědavost obětí, za normálních podmínek by člověk od cizího člověka žádnou přílohu nestáhl nebo by neklikl na žádný odkaz obsažený ve zprávě emailu. Pokud nám však tento email přijde od člověka z našeho seznamu, ani nepřemýšlíme nad tím, že by se za tím mohl skrývat nějaký podvod. [8]

1.3.2 Sociální sítě

Nejrozšířenější formou komunikace mezi lidmi jsou v dnešní době sociální sítě ať už je to Facebook, Twitter, Instagram... Je to nejjednodušší způsob, jak se spojit s přáteli, sdílet soukromé informace, sdílet fotky, a dokonce i polohu, na které se momentálně nacházíme. Všechny tyto vyjmenované věci sebou nesou rizika a mají jedno společné – dají se zneužít ve prospěch útočníka. Pokud má člověk špatně nastavený profil, může se tento profil stát viditelný i pro lidi, které nemá v seznamu přátel, tzn. kdokoli, kdo se podívá na tento účet, je schopen zjistit všechny informace, které majitel účtu vyplnil při registraci anebo například to, kde se právě nachází.

Tím, že jsou sociální sítě nejrozšířenějším a nejpoužívanějším prostředkem pro komunikaci, jsou taky nejčastějším cílem útočníků. Pokud se útočníkovi podaří dostat např. na Facebookový účet oběti, získává v podstatě stejnou moc, jako tomu bylo u nabourání se do výše zmíněného emailu. Útočník může kontaktovat lidi ze seznamu přátel oběti s odkazem na fiktivní stránku, kde se nachází malware nebo může ke zprávě přiložit infikovaný soubor.

Informace, které pachatel získá díky proniknutí např. na Facebookový účet oběti mohou být dále zneužity např. k vydírání. Díky tomu, že se na Facebooku ukládá historie zpráv, se může pachatel jednoduše zmocnit informací, které mohou mít pro oběť velkou hodnotu. Může to být klidně heslo, které oběť sdělila svému partnerovi nebo to mohou být kompromitující fotografie. Je znám případ v Americe, kdy oběť zaplatila pachateli v přepočtu padesát tisíc korun jenom proto, aby nezveřejňoval informace, ke kterým přišel v historii chatu. [8]

1.3.3 Neurolingvistické programování

Výše zmíněné formy byly zaměřeny spíše na umění vytěžování informací skrze internet. Neurolingvistické programování se zaměřuje na přizpůsobení se chování člověku, kterého chceme obelstít nebo ze kterého chceme dostat důležité informace. Díky neurolingvistickému programování je možné se dostat do podvědomí oběti a bez jeho vědomí získat informace, které nám mohou být užitečné.

Pro úspěšné využití této metody je třeba jisté míry sociálního vnímání, empatie a všímavosti. Neurolingvistické programování se totiž opírá o procesy, které jsou podvědomě vykonávány každým člověkem. Mohou to být zvyky, které jsme si osvojili v mládí, může to být styl vyjadřování. Neuroligvistické programování pracuje s odezvou chování člověka – jeho reakci na podněty z okolí, tedy na podněty, které oběti poskytujeme. Tyto vzorce se v neurolingvistice označují jako smyslové mapy (někdy neuromapy). Je to jakési upozornění na algoritmickou posloupnost našeho chování – vnímání – jazykové vyjadřování, které je ovlivněno vnějšími podněty. Jinými slovy, pro úspěšné využití této formy je potřeba si všímat, jakým způsobem člověk reaguje při konverzaci. Například, pokud není člověku příjemné, jakým směrem se konverzace ubírá, může mít tendence svírat pěst atd. [9]

Neurolingvistické programování má své využití zejména v psychoterapii, avšak díky popularitě a účinnosti této metody byla rozšířena do dalších odvětví. Vyučují se jí manažeři, tvůrci reklam, obchodníci, ale také policisté nebo vojáci, kde je tato metody velice důležitá. Na své si přišli i zruční sociální inženýři, kteří si metodu také osvojili a přizpůsobili k obrazu svému. Díky této metodě jsou totiž schopni rozeznat meze při komunikaci s obětí a přizpůsobit tomu celý průběh konverzace, dokážou také díky tělesné odezvě oběti určit, zda jsou blízko dosažení informace, kterou potřebují pro svůj prospěch.

Nedá se obecně říct, jak se proti této metodě bránit, je přirozenou vlastností člověka projevovat své emoce a podvědomé reakce na určité vjemy. Díky tomu je osvojení této techniky jednou z nejnebezpečnějších možností a nelze se proti tomu účinně bránit. Na druhou stranu je obtížné využít tuto metodu v plné její síle, jelikož podnětů, které je třeba sledovat je celá spousta a mnohé z nich trvají v řádech stovkách milisekund. Pro účely zkoumání této metody se používá kamera a následná analýza chování.

V první kapitole bylo vysvětleno, co to sociální inženýrství je. Byla popsána historie samotného vzniku sociálního inženýrství a dále byly představeny metody, prostřednictvím kterých je sociální inženýrství účinným nástrojem při vytěžování informací.

2 TECHNIKY SOCIÁLNÍHO INŽENÝRSTVÍ

Sociální inženýrství v praxi se opírá o chyby, které člověk dělá, aniž by si byl vědom toho, že je něco špatně. Těmto chybám se obecně říká kognitivní chyby v úsudku a jsou jakousi vstupní branou k informacím, které potřebujeme získat. Většina technik sociálního inženýrství se opírá právě o tyto chyby.

2.1 Pretexing

Pretexing je technika hojně využívána k získání informací prostřednictvím předem smyšleného scénáře. Cílem je, aby oběť tomuto scénáři uvěřila a dobrovolně sdělila potřebné informace. Nemusí to být jenom příběh, může to být role, do které se útočník vžije a snaží se, aby této roli oběť uvěřila.

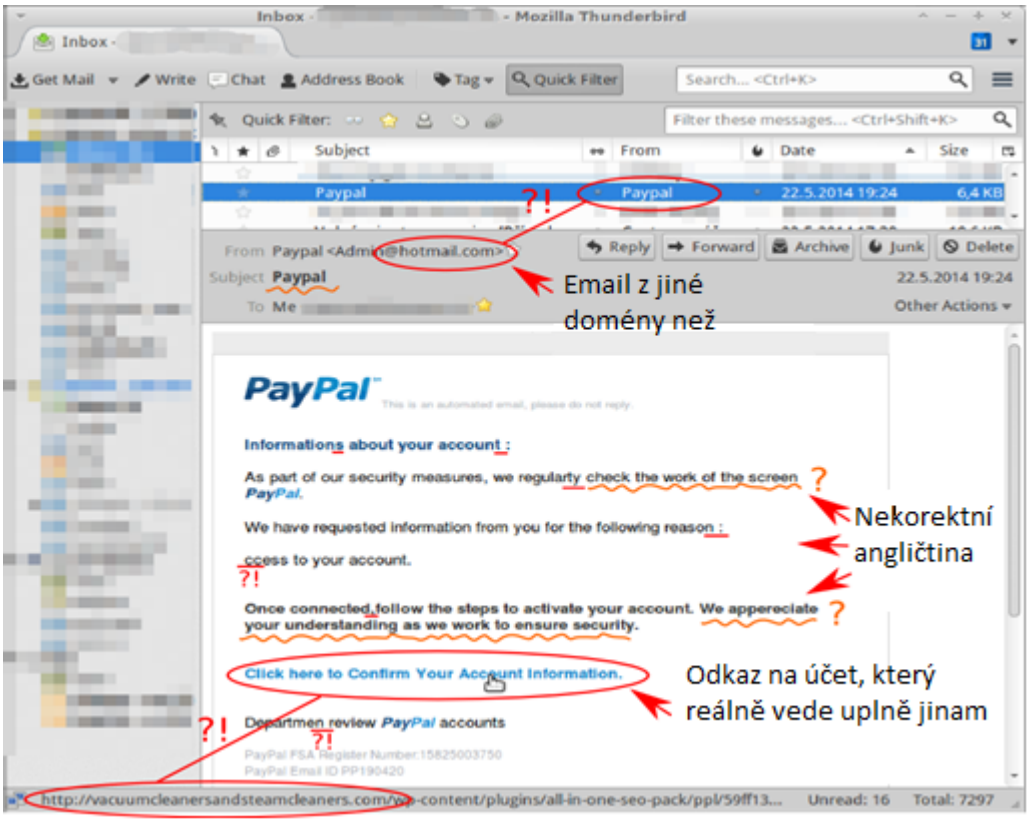
Zpravidla tato technika vyžaduje využití předem získaných informací, jako je např. jméno, datum narození, rodné číslo, telefonní číslo atd. Tyto informace útočník při komunikaci s obětí využije, aby zvýšil svoji důvěryhodnost a tím zvýšil šanci na úspěšnost této techniky. Důležité je si také předem připravit odpovědi na otázky, které mohou být při rozhovoru položeny.

Jak již bylo zmíněno, technika je nejvíce využívána k předstírání, že je útočník někým jiným. Hojně se tato metoda využívá v kruzích soukromé detektivní činnosti, kdy si tak soukromý detektiv může jednoduše například ověřit informace o poloze, nebo získat potřebné informace k získání polohy člověka, kterého například hledá. Soukromým detektivům tato technika pomáhá také při tzv. detektivním zpravodajství, které vede k naplňování nestátního zpravodajství. Další oblastí, kde se pretexing nejčastěji využívá je investigativní novinařina a vůbec novinařina celkově. [10]

Mimo osobní setkání bývá nejčastějším prostředkem pro komunikaci pachatele s obětí u pretexingu telefon. V dnešní době je stále velkým problémem to, že většina věcí se dá vyřídit pomocí telefonu. Většina velkých firem a společností, včetně bank a státních institucí se snaží vyjít lidem vstříc a umožnují tak uzavírání smluv, změnu údajů nebo dokonce dotaz na zůstatek na účtu pomocí telefonu. Banky, operátoři nebo státní instituce stále využívají jednoduše dostupné informace, jako jsou rodné číslo nebo jméno matky za svobodna jako ověření identity volajícího.

2.2 Phishing

Phishing je hojně využívaná metoda pro získání informací, jakou jsou hesla a přístupové údaje prostřednictvím webového rozhraní. Jde o podvodnou stránku, která se vydává jako stránka oficiální, ale informace, které vložíme do formuláře na této smyšlené stránce, putují k útočníkovi. Může to být například stránka s přihlášením do internetového bankovnictví, kde za normálních okolností vložíme číslo bankovního účtu, poté heslo a čekáme na přepojení do internetového bankovnictví. Fiktivní stránka nás sice může přesměrovat do internetového bankovnictví, ale přihlašovací údaje putují k pachateli, který se poté může přihlásit do internetového bankovnictví sám a zneužít tak své přítomnosti na tomto účtu ve svůj prospěch. [11]



Obr. 1. Příklad podvodného emailu. Upraveno z [12]

K těmto fiktivním webovým stránkám se většinou oběť dostane skrze emailovou schránku, na emailovou schránku oběti může dojít podvodný email, který se tváří jako email od banky. Email může obsahovat různé scénáře, nejčastějším scénářem je žádost o změnu hesla z důvodů toho, že uživatel používá pro přihlášení slabé heslo a může se tak stát terčem útoku. Nebo se tyto emaily mohou tvářit jako rutinní kontrola osobních údajů, u které je potřeba přihlášení do webového portálu. [13]

Phishing je nebezpečný v tom, že mnoho lidí si nedává pozor, na co na internetu klikají. Existují různé školení a kurzy, které se zaměřují na tyto podvodné aktivity a objasňují lidem, jak se zachovat v situaci, kdy se stanou obětí techniky sociálního inženýrství zvané phishing. Zároveň taky učí lidi, jak těmto situacím předejít, je potřeba si kontrolovat, zda odkaz je opravdu odkazem, který nás přesměruje na požadovanou stránku – lze tak jednoduše učinit najetím ukazatele myší na odkaz, který se ukáže dole v prohlížeči (viz Obr. 1).

2.3 Baiting

Další z řady použitelných technik sociálního inženýrství je technika baiting. Baiting je odvozený z anglického slova „bait“, které v češtině znamená návnada. Tato technika využívá přenosná datová média jako návnadu.

Principem této metody je ponechání infikovaného přenosného datového média tak, aby oběť toto médium našla a použila. Jako návnada se v dnešní době využívají flash disky, CD nebo DVD. Pro zvýšení úspěšnosti této techniky se může na přenosné médium napsat např. „Výplaty 2018“ nebo „Výpis z trestního rejstříku“, záleží, pro koho bude návnada cílena. [14]

Datové médium může být infikováno softwarem, který se při připojení datového média nahraje do počítače oběti a umožní nám tak vzdálený přístup k osobním údajům. Pokud se tento počítač nachází například v interní síti firmy, může se útočník snadno dostat do dalších počítačů, které se nachází v této síti. Důležité je, aby oběť toto nastražené médium zaujalo. [15]

Obr. 2. Příklad nastraženého CD

2.4 Vishing

Vishing se někdy také označuje jako phishing přes telefon. Je to tedy technika, která je nejvíce rozšířená přes telefonní hovory. V dnešní době lze také volat přes počítač. Prostřednictvím této techniky lze získat důvěrné informace nebo informace, které jsou pro nás důležité. Základem je, aby osoba na druhé straně důvěřovala volajícímu a na základě této důvěry tak dala útočníkovi to, co potřebuje. [16]

V dnešní době se tato technika moc nevyužívá, ačkoli stále se dá pomocí vishingu zjistit hodně informací. Může sloužit soukromým detektivům nebo třeba investigativním novinářům.

2.5 Quid Pro Quo

Quid Pro Quo znamená v češtině „něco za něco“. Tato technika spočívá v nabídnutí oběti službu, výměnou za nějakou službu nebo dárek. V praxi to funguje tak, že útočník například obvolává zaměstnance firmy a snaží se najít člověka, který zrovna potřebuje IT pomoc. Útočník, který se může vydávat za IT specialistu nabídne pomoc, která vyžaduje vzdálený přístup do počítače oběti.

Quid Pro Quo může nastat ve chvíli, kdy se útočníkovi podaří přemluvit oběť tím, že nabídne například službu výměnou za nějakou informaci. Může to být služba opravy počítače. V momentě, kdy oběť povolí přístup útočníkovi do svého počítače s vidinou opravy problému, umožní tak útočníkovi stáhnout potřebné informace z počítače oběti. K přístupu do počítače se většinou využívá software, který je obsažen přímo v operačním systému (vzdálená plocha) nebo externí program, který funguje na stejném principu (TeamViewer).

Ačkoli se Quid Pro Quo prezentuje jako technika sociálního inženýrství, která se provádí prostřednictvím internetu, lze tuto metodu využít i v rámci fyzického kontaktu útočníka s obětí nebo oběťmi. Byly hlášeny případy, kdy do firmy přišli lidé, kteří se vydávali za bezpečnostní specialisty a vyhlásili ve firmě takovou soutěž. Soutěž spočívala v tom, kdo dokáže vymyslet nejsilnější heslo. Většina lidí, kteří se této soutěže zúčastnili, na papírek mimo jiné, vymyšlené, hesla napsali i heslo svoje. Napsali ho s vidinou, že jim bezpečnostní specialisté řeknou, zda je toto heslo silné nebo ne. Údajní bezpečnostní pracovníci rozdali zúčastněným, kteří napsali nejsilnější heslo, bloček s tužkou a vyhlásili vítěze. [17]

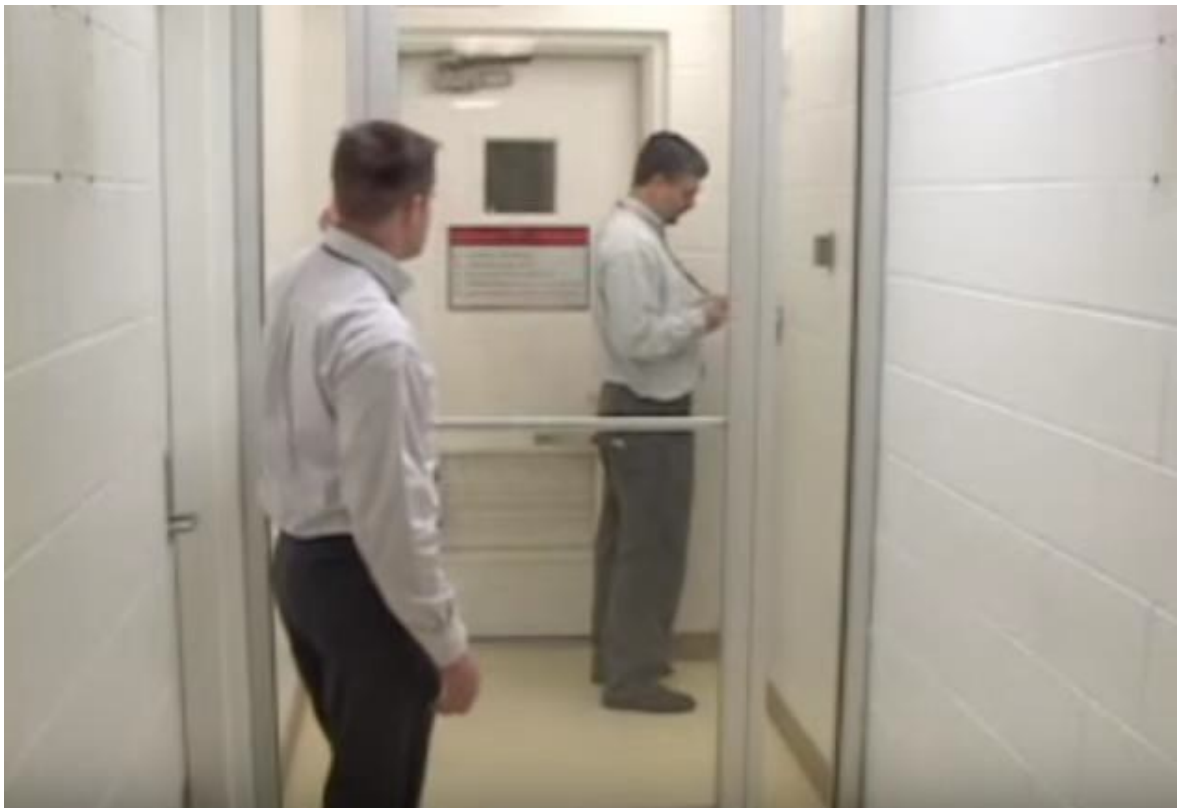
2.6 Tailgating a piggybacking

Dalším z technik sociálního inženýrství, které využívají zejména fyzického kontaktu je tailgating, kterému se taky někdy říká piggybacking. Tato technika využívá důvěřivosti a neopatrnosti lidí. Hlavní rozdíl mezi tailgatingem a piggybackingem je ten, že u tailgating následujeme člověka, který má přístupovou kartu, do místnosti nebo objektu v jeho těsném závěsu. Otevře dveře pomocí své ID karty a člověk, který se tam chce dostat a tuto ID kartu nemá, se drží těsně za tímto člověkem a projde. Piggybacking funguje podobně, ale útočník může předstírat, že kartu ztratil nebo ji nechal doma a vyžaduje si tak přístup do objektu po zaměstnanci, který stojí například venku. Tzn. tailgating je nevědomé vpuštění člověka do objektu a na druhou stranu piggybacking je nevědomé vpuštění člověka do objektu.

Obr. 3. Obrana proti tailgatingu ve společnosti Apple [18]

Jedním z dalších scénářů (příklad piggybackingu), který se často využívá může být, že útočník, který se chce dostat do objektu, kde je potřeba ke vstupu ID karta má plné ruce. Požádá člověka, který ID kartu vlastní, aby mu otevřel dveře ze zřejmého důvodu. Ve většině případů se tak stane a útočník se dostane do objektu, aniž by bylo někomu podezřelé, že nevlastní ID kartu opravňující vstupu do objektu. V mnoha případech se také může stát, že člověk, který si otevře pomocí přístupové karty, podrží dveře člověku, který jde za ním. Člověk, který podrží dveře si neuvědomuje, že může pouštět člověka, který tuto kartu nemá, ale udělá to, protože si myslí, že dělá dobrý skutek.

Proti tailgatingu a piggybakingu se dá jednoduše bránit pomocí tzv. dvojitého přístupu. Vstup do chráněné místnosti nebo objektu je chráněn dalším vstupem, kde se nachází přístupové identifikační zařízení. Přístupový systém je nastaven tak, že pro přiložení své ID karty je podmínkou být sám v této malé místnosti. Pokud jsou splněny všechny podmínky, přístupový systém dovolí přiložení ID karty a po následné identifikaci umožní přístup do chráněného objektu nebo místnosti. [19]



Obr. 4. Zabránění tailgatingu [20]

V této kapitole byly popsány nejvyužívanější techniky sociálního inženýrství. Jak můžeme vidět sociální inženýrství není fenomén, který se využívá pouze přes internet. Sociální inženýrství lze využít i jako metodu pro vytěžování informací pomocí fyzického kontaktu útočníka s obětí. Tyto techniky jsou obecně popsány, avšak neslouží jako návod. Pro úspěšné použití těchto technik je třeba improvizace přímo na místě, kde je tato technika použita.

3 NEVERBÁLNÍ KOMUNIKACE

Neverbální komunikace je základem pro navázání kontaktu. K technikám, které se v sociálním inženýrství používají v rámci fyzického kontaktu je zapotřebí znalost neverbální komunikace. Neverbální komunikace je klíčová k pochopení toho, jak člověk reaguje. Díky neverbální komunikaci můžeme také „číst“ reakce člověka a uzpůsobit tomu náš postoj, vyjadřování nebo držení těla.

Při komunikaci s lidmi je neverbální komunikace základním a důležitým faktorem. Díky neverbální komunikaci můžeme zjistit, zda je člověk otevřený konverzaci nebo jestli se konverzace vyvíjí správným směrem a zda to člověku není nepříjemné. Lze tak konverzaci usměrnit a vést správným směrem. Sociální inženýrství je tak úzce spjato s neverbální komunikací, kombinací dobře použité techniky a správně použitých neverbálních znaků můžeme zvýšit šanci na úspěch dané techniky.

Pro potřeby sociálního inženýrství je také potřeba rozeznat, zda nám člověk říká pravdu, či nikoli. Díky neverbálním projevům člověka můžeme zjistit, zda to, co člověk řekne, koresponduje s tím, jak se chová. Člověk může znát základní principy neverbální komunikace a správně identifikovat různé faktory neverbální komunikace, ale při rozhovoru, kdy se toho snaží využít, musí hodně přemýšlet i nad tím, co říká. Improvizace je při tomto procesu také velmi důležitá.

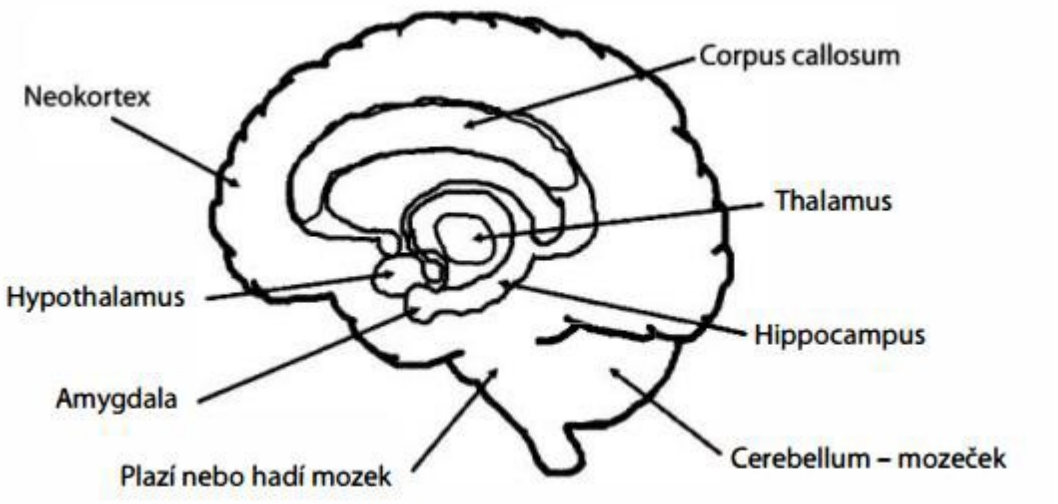
Neverbální komunikace je například klíčovým prvkem při odhalování lidí, kteří mají skryté úmysly. Může toho být využito například na letištích nebo veřejných shromážděních, kde jsou pracovníci, odborníci přes neverbální komunikaci, kteří sledují chování lidí a snaží se předejít možným hrozbám a nežádoucím situacím, jako je úmysl někoho zabít, či jinak poškodit. [21]

Základními faktory neverbální komunikace jsou gesta, mimika nebo třeba posturika, díky kterým můžeme například odvodit emoční stav daného člověka. Naše chování je doprovázeno právě těmito neverbálními projevy. Jsou to důležité znaky, kterými se dá proniknout do mysli dané osoby tím, že se do ní vcítíme. Pomáhají nám také pochopit, jak se člověk právě cítí nebo odhadnout, co se chystá udělat. Těchto faktorů a znaků neverbální komunikace je spousta. Pro účel této diplomové práce budou rozebrány a popsány základní znaky a faktory, které nám mohou pomoci ovládnout situaci v technikách, nezbytných pro dokončení praktické částí diplomové práce.

3.1 Proč neverbální komunikace funguje?

Náš mozek ovlivňuje veškeré procesy, které se dějí navenek našeho těla. Výše zmíněné faktory a znaky neverbální komunikace sídlí v našem limbickém systému, který při konfrontaci s vnějšími vlivy okolí může za to, jak se tváříme, jak se cítíme nebo jak se projevujeme. Limbický systém je jakési emoční centrum, které vysílá signály dál do našeho těla. Limbický systém také ovládá naše chování nebo dlouhodobou paměť.

Díky vlastnostem limbickému systému je v dnešní době neverbální komunikaci přikládána vysoká váha. Limbický systém je totiž část mozku, kterou nemůžeme nijak ovládat, nemůžeme ho ani nijak řídit. Znaky a faktory, které pramení v limbickém systému jsou tedy upřímné a dají se kategorizovat či přesně popsat. Proto je neverbální komunikace v mnoha ohledech nápomocná i při výslechu policii, kdy se snaží zjistit, zda pachatel mluví pravdu nebo ne. Bohužel však v České republice není analýza chování, založená na neverbální komunikaci, přípustným důkazem u soudu, jako tomu je například v Americe. [22]



Obr. 5. Limbický systém [23]

„*Další důležitou součástí našeho mozku je neokortex, což doslova znamená nová mozková kůra. Této části mozku se také říká "lidský", "myslící" nebo "intelektuální" mozek, protože má na starosti vyšší poznávací činnost a paměť. Právě tato část mozku nás odlišuje od ostatních savců kvůli velkému množství jeho hmoty (kůry) používané k myšlení. Pro jeho schopnost počítat, analyzovat, interpretovat a chápat na úrovni, která je jedinečná pro lidský druh, je to náš kritický a tvůrčí mozek. Je to ale také část mozku, která je nejméně poctivá, a proto je to také náš "prolhaný mozek". Vzhledem k tomu, že je schopen komplexního uvažování, je*

tento mozek – na rozdíl od svého limbického protějšku – ze všech tří hlavních součástí mozku nejméně spolehlivý. Je to mozek, který umí podvádět a který podvádí často.“ [23]

Příklad identifikace neverbálních faktorů a znaků uvedl ve své knize bývalý agent FBI Joe Navarro. Událost se stala v roce 1999 v Americe. Při namátkové kontrole na dálnici zastavila policie auto. Policista, který komunikoval s řidičem, si všiml, že řidič vykazuje nadměrné známky nervozity. Podle policisty se řidič hodně potil a třásly se mu ruce při podávání řidičského průkazu. Policista si původně myslel, že řidič je pod vlivem drog a požádal tedy řidiče, aby vystoupil z vozidla. Jakmile řidič vystoupil z vozidla, dal se na útěk. Po chvíli byl dopaden a při kontrole vozidla bylo nalezeno detonační zařízení spolu s třemi kilogramy výbušniny. [23]

Jak již bylo zmíněno výše, limbický mozek se nedá nijak oklamat. Nadměrné působení vnější vlivů – strach z odhalení, se projevily nadměrným pocením, třesem rukou a celkově velkou nervozitou řidiče. Díky pohotové reakci policisty, kterému tato situace přišla podezřelá, se podařilo odhalit potencionálního bombového útočníka. Tento případ byl jeden z prvních, u kterých byl prokázán přínos neverbální komunikace v rámci odhalení nebezpečného člověka.

3.2 Projevy neverbální komunikace

Působení vnějších vlivů na náš limbický systém může mít mnoho následků, které se mohou fyzicky projevit na našem těle. Tyto faktory a znaky se dají přečíst. Můžeme těmto fyzickým odezvám přiřadit skupinu a můžeme předpokládat, jaké mají tyto fyzické odezvy význam. Existují různé druhy neverbální komunikace, které jsou rozděleny podle částí těla nebo jejich funkcí:

- Kinezika nebo také gestika (pohyby těla, rukou)
- Haptika (dotyk)
- Mimika (pohyby obličeje)
- Oční kontakt
- Posturika (postoj celého těla)
- Proxemika (vzdálenost komunikujících)
- Chronemika (pracování s časem při neverbální komunikaci) [24]

Pro účel diplomové práce budou vysvětleny pouze některé z výše uvedených projevů neverbální komunikace.

3.2.1 Kinezika

Kinezika se v běžném žargonu moc nepoužívá, používá se spíše název „řeč těla“. Kinezika znamená to, jak se pohybujeme, jaký máme postoj nebo jakým způsobem reagujeme na určité vjemy. Mohou to být gesta, které jsou doprovázeny při rozhovoru nebo gesta jako reakce na určité události. Nejen v rámci kineziky je třeba si dávat pozor na kulturní předpoklady dané osoby, protože v rámci kulturních zvyklostí se mohou gesta lišit podle toho, z jaké části světa člověk pochází. [25]

Problematikou kineziky se zabývají i Friesen a Ekman, kteří rozdělili znaky a ukazatele kineziky na pět částí, které mohou napomoct při tzv. „čtení řeči těla“.

3.2.1.1 Znaky

Neverbální znaky jsou chápány jako signály, které mohou obecně hodně vypovědět o dané situaci. Typickým příkladem neverbálního znaku je palec nahoru, který běžně znamená souhlas. Důležitý je ovšem kontext, ve kterém se tento znak může objevit. Jak již bylo zmíněno, běžně je tento symbol chápán jako souhlas, ale v jiném kontextu může být chápán jako pouhé číslo jedna.

Obr. 6. Symbol OK [26]

Dalším typickým znakem, který se všeobecně využívá může být znak OK. Tento znak je typický zejména pro země jižní Evropy. Stejně jako v přechozím příkladu je třeba si dávat pozor na kontext, ve kterém se tento symbol může objevit. Stejně jako OK může tento znak vyjadřovat nulu.

3.2.1.2 Ilustrátory

Ilustrátory jsou pohyby, které jsou doprovázeny při běžné verbální komunikaci. Ilustrátory mohou odrážet náš názor na danou věc nebo náš názorový postoj. Při běžné verbální komunikaci slouží jako doprovod pohybům těla. Ilustrátory můžeme také zdůrazňovat intenzitu našeho názoru.

Typickým příkladem zdůraznění intenzity našeho názoru mohou být ruce v pěst. Pokud si při verbální komunikaci všimneme použití rukou v pěst, může toto gesto znamenat, že si člověk stojí za svým názorem. Nebo tento člověk může být mírně podrážděn, jelikož typickým znakem pro ruce v pěst je připravenost k boji nebo tendenci člověka se bránit.

Obr. 7. Zdůraznění intenzity pomocí rukou v pěst [27]

Typickým příkladem hojného využívám ilustrátorů jsou země jižní Evropy (Italové), kteří jsou známí tím, že při verbální komunikaci využívají gesta pro zpřesnění nebo zvýšení intenzity svých názorů. Nebo například pokud na někoho v Indii máváme rukou, neznamená to „Ahoj“ nebo „Pojď sem“, ale znamená to přesný opak „Jdi pryč“.

3.2.1.3 Projevy emocí

Emoce jsou doprovázeny každou neverbální i verbální komunikací. Emoce nebo to, jak se člověk cítí, lze poznat z výrazu obličeje nebo postoje těla. To, jak se člověk cítí, můžeme poznat i z verbální komunikace podle hlasu.

Jako příklad si můžeme uvézt člověka, který má stažené obočí, mírně našpulenou pusu a koutky pusy jsou směrem k zemi. Člověk, který vykazuje tyto známky, může být smutný

nebo může být v depresi. Opakem je člověk, který má naopak roztažené obočí, koutky pusy jsou směrem nahoru a obočí nahoru. Tento člověk je ve většině případů šťastný, má dobrou náladu apod.

Emocemi a to, jakým způsobem je identifikovat a přečíst, se věnuje Paul Ekman ve své knize Odhalené emoce. Emocemi a jejich stručnou charakteristikou se budu věnovat v další podkapitole.

Obr. 8. Smutek [28]

3.2.1.4 Regulátory

Regulátory jsou podle Ekmana chápány jako pomocné znaky při verbálním projevu. Mohou napomoci kontrolovat situaci nebo intuitivně naznačit, co tím vlastně řečník myslí. Regulátory mohou fungovat i jako podpůrné signály, kterými můžeme koordinovat nebo monitorovat řeč druhého. Typickým příkladem je přikývnutí na řečníka při jeho mluveném projevu, můžeme mu tím naznačit, že souhlasíme nebo to, aby ve svém mluveném projevu pokračoval dál.

3.2.1.5 Adaptory

Adaptory jsou hodně specifické úkony, které v mnoha případech člověk ani nepostřehne. Adaptory jsou těžké zachytit a je potřeba vysoké obezřetnosti a všímavosti. Adaptory nám mohou dávat najevo to, co si o druhém člověku myslíme. Typickým příkladem mohou být ženy, které chtějí zapůsobit na muže – hrají si s vlasy. Typickým příkladem může být také nervozita, která může být doprovázena klepáním nohou, mačkání propisky apod. Adaptory se ve většině případech opakují, frekvenci určuje momentální emoční rozpoložení.

Adaptory mohou být také chápány jako jakési uspokojení potřeb, může to být škrábání, který se zbavíme svědění, odhrnutí vlasů, které nám brání ve výhledu nebo to může být narovnání brýlí, které nám padají.

Obr. 9. Adaptér – Stud, provinilost [29]

Za adaptér můžeme také považovat obrázek výše, kde jsou ruce přiloženy k hlavě. Toto gesto ve většině případů znamená stud nebo provinilost. Pokud při komunikaci člověk, se kterým mluvíme, udělá toto gesto, můžeme předpokládat, že je zklamaný, stydí se nebo ho to mrzí. Všechno, co si můžeme spojit se studem nebo provinilostí.

3.2.2 Haptika

Haptika je chápána jako komunikace dotekem. V praxi se komunikace dotekem využívá často. Dotek může během konverzace být intimní, ale může také mít za cíl vyvolat pocit nadvlády nebo kontroly nad člověkem, se kterým komunikujeme. Hodně záleží na kontextu a situaci, ve které je komunikace dotekem použita. Dotykem se můžeme snažit člověka přesvědčit, aby nám věřil.

Komunikace dotekem je hojně využívána v průmyslu komerční bezpečnosti strážnými, kteří takhle mohou vést člověka, který se ocitl na místě, kde nemá co dělat. Jednoduše mu dá ruku na rameno a nasměruje ho z objektu nebo místnosti ven. [30]

3.3 Emoce

S emocemi jsou spojovány pocity, mohou to být zkušenosti, které jsou spojovány s radostí, panikou, láskou nebo také nenávistí, zlostí a smutkem. Emoce jsou reakce na vnější vlivy a nemají dlouhé trvání. Emoce bývají často spojovány s náladou. Emoce mohou mít vliv na naši náladu, nálada je ale spíše dlouhodobý stav. Emoce a nálada mohou mít společné znaky, které se projevují často stejnými způsoby.

Emoce samy o sobě jsou složité a mohou mít fyzické i psychické příčiny. Dají se však jednoduše identifikovat a následně využít pro náš prospěch. U projevů neverbální komunikace, jako je kinezika, jsou emoce rozdílné podle kultury. Vyjadřování emocí však nepočítá s žádnou kulturní odlišností, protože emoce všichni vyjadřujeme stejně – stejnými znaky. [30]

Ekman spolu se svým společníkem Friesenem pracovali na vědeckém výzkumu, který měl vyvrátit odlišnost emocí na základě kulturní odlišnosti. Ekman s Friesenem navštívili kmeny, které sídli ve státě Papua Nová Guinea a zjistili, že ačkoli jsou tyto kmeny mimo civilizaci a nemají tam mediální ani fyzický kontakt s ostatními lidmi, tak vykazují stejné známky emocí, jako ostatní lidé. Výsledky tohoto výzkumu vedly k členění emocí do šesti základních skupin:

- Hněv
- Radost
- Znechucení
- Překvapení
- Strach
- Smutek

3.3.1 Hněv

Hněv je jedna z emocí, která je na první pohled nepřehlédnutelná. Stejně jako je na první pohled nepřehlédnutelná, tak tuto emoci můžeme jen těžko skrýt. Hněv může být způsoben mnoha vnějšími vlivy. Může to být pocit nespravedlnosti, zášti nebo člověka může k hněvu vést pocit nebezpečí.

Pokud je člověk rozzuřený nebo naštvaný, je větší pravděpodobnost, že se bude chovat agresivně. Je třeba si tak dávat pozor na další jednání z naší strany, které by tak mohlo rozzuřeného člověka vyprovokovat. [30]

Hněv může mít hodně podob, u každého člověka tak může vypadat úplně jinak. Všichni lidé však vykazují společné znaky, které se dají shrnout. Výrazy a znaky, které člověk vykazuje ve hněvu, se nedají zakrýt. Hněv je stupňující se emoce. Základní znaky hněvu se dají rozdělit do těchto tří kategorii:

- Obočí, které jsou stáhnuté a směřují dolů
- Přimhouření očních víček – vypadá to jako by člověk zaostřoval
- Zúžení rtů

Obr. 10. Emoce – Hněv [31]

3.3.2 Radost

Radost bývá spjata s radostnými a příjemnými událostmi. Radost je pozitivní a nejpřirozenější emoce. Stejně jako tomu bylo u hněvu, radost také může mít stupňující ráz. Pro radost je typický úsměv, je ale třeba si dávat pozor, aby se úsměvem nemaskovala jiná emoce. Nejčastěji se emoce maskují právě radostí, stejně jako tomu je u stavu spokojenosti, radost nevyžaduje zapojení tolika svalů ve tváři, jako tomu bylo u hněvu. U radosti je potřeba rozeznat opravdový úsměv od falešného úsměvu. Celkově pro radost jsou typické roztáhlé nosní dírky, vypoulené oči a mírně zdvihnuté obočí.

Obr. 11. Emoce – Radost [31]

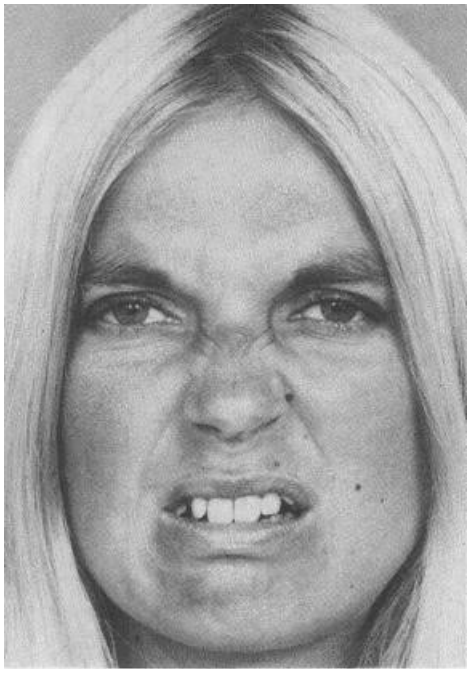
3.3.3 Znechucení

Znechucení může mít více podob, může být dokonce mířené proti nějaké osobě nebo názorům určité osoby. Jedním z častých projevů bývá projev znechucení při jídle, které nám nechutná. Stejně jako ostatní výše zmíněné emoce i znechucení má svou stupňující intenzitu. Intenzita znechucení může vést i k následné agresi člověka. Proto není dobré nechat člověka vystavěného znechucení dlouhou dobu.

Mírné znechucení a silné znechucení se může zásadně lišit. Liší se v počtu použitých svalů na obličeji, které při silném znechucení vytváří úplně jiné znaky než tvář při mírném znechucení.

Znechucení můžeme zařadit mezi mírné emoční projevy, ačkoli znechucení může eskalovat až ke vzteku či hněvu. Jak již bylo zmíněno, znechucení se projevuje podobně při mírném i silné formě. Dá se obecně říct, že znechucení poznáme podle:

- Zdviženého horního rtu, dolní ret může být také zdvižený nebo povystrčený
- Na nose se mohou objevit vrásky
- Nos je mírně sevřený
- Víčka jsou tlačena nahoru
- Obočí může být snížené



Obr. 12. Emoce – Znechucení [31]

3.3.4 Překvapení

Překvapení má rychlý nástup, nevydrží dlouho, a pak rychle odezní. Je to nejupřímnější emoce, kterou dokáže člověk vytvořit. Díky tomu, že nastupuje rychle a rychle také odeznívá, dá se tato emoce jen těžko obelstít. Nelze tak snadno tuto emoci předstírat. Předstírané překvapení bývá většinou dlouho, člověk se snaží držet ve tváři výraz překvapení příliš dlouho a tím se stává nepřirozenou.

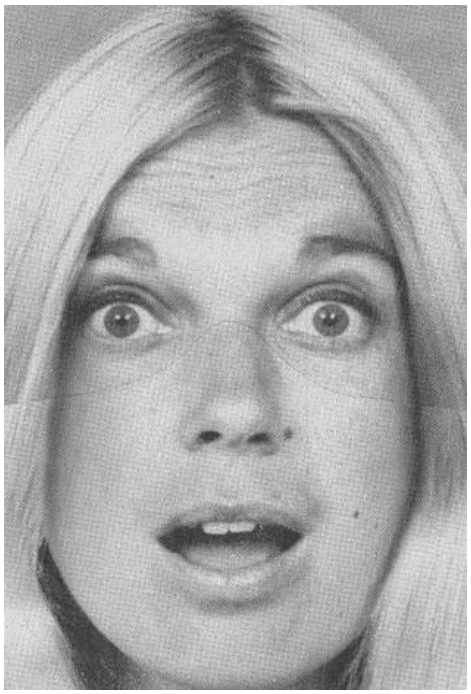
Pocit překvapení nám může vyvolat jakákoli zpráva nebo vjem z okolí. Může nás překvapit počasí nebo dárek či nečekaná návštěva. Pocit překvapení se však dá využít i pro ověření toho, zda člověk ví určitou zprávu či nikoli. Například pokud si chceme ověřit, že člověk ví o nějaké zprávě nebo události, můžeme ho na to zeptat a pozorovat reakci. Ve většině případů, pokud je člověk překvapený, tak o události nebo zprávě nevěděl. [31]

Tato metoda je hojně využívána například policií při výslechu, kdy je pachatel konfrontován s informacemi a následně pozorován kvůli jeho reakci. Tato metoda není u soudu brána jako důkaz, ale může policii pomoct při výslechu určit, zda vedou výslech správným směrem či nikoli.

Stejně, jako je tomu u všech předchozích emocí, i tato emoce je stupňující. U překvapení nepoužíváme tolik svalů ve tváři, jako tomu bylo u silného znechucení, ale i tak se dá překvapení snadno identifikovat.

Mírné překvapení, které je nejčastější, bývá doprovázeno pouze zdviženým čelem a zdviženým obočím. Mírné a silnější překvapení má své typické rysy, které se dají shrnout:

- Obočí může být mírně zdvižené [31]
- Zdvižené a stáhnuté čelo [31]
- Zdvižené a stáhnuté obočí [31]
- Čelist je tlačena směrem dolů [31]
- Vypouklé oči [31]
- Může být doprovázeno vrásky na čele [31]



Obr. 13. Emoce – Překvapení [31]

3.3.5 Strach

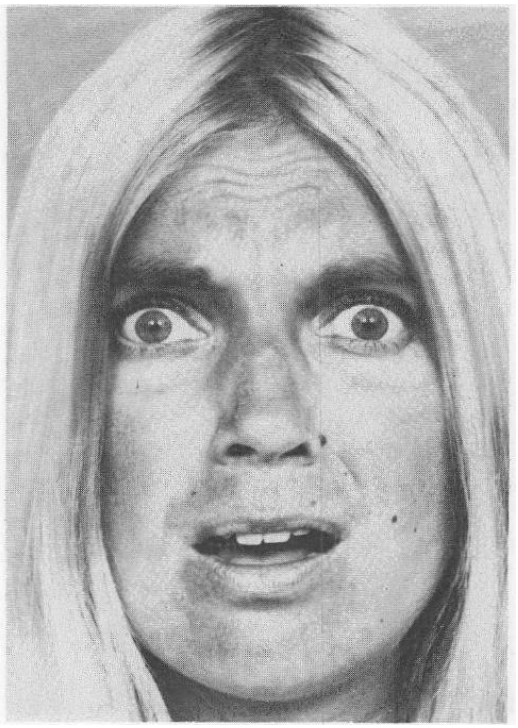
Strach je jednou z nejúčinnějších forem emocí. Strach ve své nejsilnější formě může být doprovázen hněvem. V této chvíli může být člověk agresivní a pro okolí nebezpečný. Strach bývá často doprovázen vysokým tlakem, nervozitou a třesem.

Strach bývá nejčastější důvod pro odhalení nekalé činnosti. Byl hlášen případ, kdy letištní ochranka odhalila člověka, který pašoval drogy. Tento člověk vykazoval známky strachu tím, že byl nervózní, chodil sem a tam, potil se. Toto chování vzbudilo u letištní ochranky podezření, letištní ochranka v rámci standartního protokolu tohoto člověka konfrontovala

s otázkami typu „Dobrý den, jak se jmenujete, kam letíte?“. Tento člověk však konfrontaci letištní ochranky nezvládl a ke všemu se přiznal. [31]

Jak již bylo zmíněno, strach bývá doprovázen agresí a hněvem. V jeho mírné podobě však můžeme předpokládat následující znaky:

- Obočí bývá zvednuté a stažené k sobě
- Oči jsou otevřené a víčka bývají napnutá
- Silný strach je doprovázen často rozšířenými zornicemi
- Pusa bývá otevřená a rty jsou napjaté
- Nos je mírně sevřený
- Na čele se vytvoří vrásky



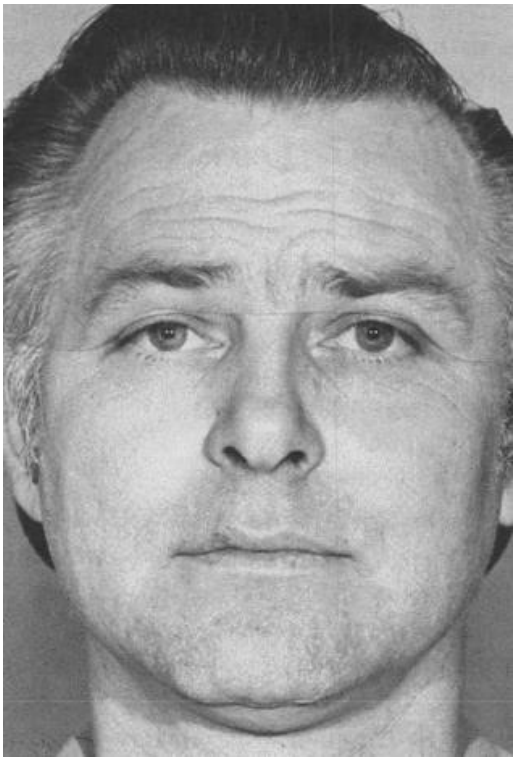
Obr. 14. Emoce – Strach [31]

3.3.6 Smutek

Smutek může mít příčinu v utrpení, které si člověk prožil. Smutek může být chápán jako forma úzkosti a bývá doprovázen pláčem. Smutek bývá také v hodně případech doprovázen vztekem nebo strachem.

Smutek se dá jednoduše rozpoznat celkově skleslou tváří. Smutek může také ovlivnit naši chůzi a verbální vyjadřování. Lidé, kteří jsou smutní, chodí většinou shrbení a mluví potichu.

Intenzita smutku se může stupňovat. Smutek v mírné podobě bývá zcela odlišný od smutku v jeho silné formě. V mírné formě může mít člověk neutrální výraz ve tváři – koutky pusy nejsou ani dole ani nahoře. Obočí bývá svěšené a nosní dírky roztažené. Mírná podoba smutku využívá nejméně svalů ve tváři, a proto je nejhůře identifikovatelná. Na rozdíl od silného projevu smutku, který může být doprovázen vztekem nebo hlasitým pláčem.



Obr. 15. Emoce – Smutek [31]

Ve třetí kapitole byla shrnuta neverbální komunikace a její praktické využití. Neverbální komunikace je využívána každodenně všemi lidmi. Neverbální komunikaci využívají lidé ve všech situacích. Valná většina lidí podvědomě tuší, co tyto faktory a znaky znamenají, ale málokdo se tím nezabývá. Bylo řečeno, proč neverbální komunikace funguje a že náš limbický systém se nedá lehce oklamat ani ovlivnit. S neverbální komunikací jsou spjaty její projevy. Projevy neverbální komunikace jsou řazeny do kategorií a pracuje se s pojmy, jako jsou ilustrátory nebo adaptory. Důležitou částí při rozpoznávání neverbální komunikace jsou emoce a jejich charakteristika. Emoce hrají klíčovou roli při pochopení vnitřních pocitů člověka a zároveň korektní identifikací momentálního rozpoložení člověka můžeme vést verbální komunikaci příslušným směrem.

4 LEGISLATIVA

V rámci této kapitoly budou popsány jednotlivé zákony, které se okrajově dotýkají zvoleného tématu. Problém je, že žádný zákon přímo nevymezuje sociální inženýrství jako takové. Proto je těchto zákonů více.

Pro účel této práce jsou vybrány pouze ty, se kterými přišel autor při vypracovávání praktické části do styku. Tedy zákony týkající se sociálního inženýrství v rámci fyzické formy sociálního inženýrství a formy, která se provádí vzdáleně – skrze internet.

4.1 Trestní zákoník

K trestné činnosti **zákona č. 40/2009 Sb. Zákon trestní zákoník**, se vztahuje mnoho zákonů, nařízení a legislativ. V následující podkapitole budou popsány zákony, které souvisí s problematikou tématu diplomové práce. [32]

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

„Uvést někoho v omyl či využít něčího omylu lze i provedením zásahu do počítačových informací nebo dat, zásahu do programového vybavení počítače nebo provedením jiné operace na počítači, zásahu do elektronického nebo jiného technického zařízení, včetně zásahu do předmětů sloužících k ovládání takového zařízení, anebo využitím takové operace či takového zásahu provedeného jiným.“ [32]

Při využití systému testování zaměstnanců, se může tazatel dostat do bodu, kdy ho bezpečnostní pracovník pustí do monitorovací místnosti, kde mohou být i počítače senzitivními údaji. Pokud by se tak stalo a tazatel by využil situace a snažil se z počítačů dostat nějaké informace, je tato činnost trestná.

§ 181 Poškození cizích práv

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

a) uvede někoho v omyl, nebo

b) využije něčího omylu,

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.“ [29]

V rámci diplomové práce by bylo jednodušší vydávat se za pracovníka bezpečnostní služby a tím dosáhnout požadovaných informací. V rámci praktické části diplomové práce nebyly

pracovníkům bezpečnostních služeb podávány žádné podněty, které by byly v rozporu se zákonem. Vytěžování informací probíhalo pouze na základě rozhovoru a dobrovolného sdělení informací ze strany dotázaného pracovníka.

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

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

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

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

d. neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,

bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci.“ [32]

Pokud by se jednalo o sociotechniku, která bývá využívána v rámci penetračního testování zaměstnanců firmy, jednalo by se o sociotechniky, jako jsou phishing nebo baiting. Pokud by se tyto metody měly využít legální cestou, musela by se s dotyčnou firmou uzavřít smlouva o vykonání penetračního testování. Pokud smlouva s dotyčnou firmou nebyla uzavřena, stává se z toho trestný čin.

V rámci phishingu jsou rozesílány emaily, jejichž obsahem je mimo jiné odkaz na fiktivní stránku, kde jsou zaměstnanci vyzváni např. ke změně hesla, což je doprovázeno vložením starého hesla. Tímhle způsobem se tak útočník může dostat k senzitivním údajům. Celý tento proces je taktéž v rozporu s trestním zákoníkem

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

(1) „Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze,

vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a. *zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo*
b. *počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,*

bude potrestán odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti.“ [32]

V tomto případě se může jednat o payload. Payload jsou data, která jsou pro nás užitečná. Jsou to data, která jsou přenášena. V rámci baitingu je na flashdisk nahrán skript, který při zapojení do cizího počítače umožní vzdálený přístup k tomuto počítači nebo databázi, což je v rozporu s trestním zákoníkem, konkrétně paragrafem výše zmíněným.

Skript, který je nahrán na médiu může také odposlouchávat komunikaci v interní síti. Odposlechnutou komunikaci může taktéž odesílat na server mimo interní síť firmy. V odposlechnuté konverzaci se mohou nacházet senzitivní informace. Tento čin je taktéž trestný.

4.2 Občanský zákoník

Jedním z dalších aspektů z právního prostředí, který budu zmiňovat v této práci je **zákon č. 89/2012 Sb. občanský zákoník.** Konkrétně se to bude týkat následujících paragrafů [33]:

§ 86

„Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.“ [33]

V praktické části diplomové práce, kde je prostřednictvím social engineering card využíváno rozhovoru s bezpečnostním pracovníkem, by bylo jednodušší, pro účel zaznamenání rozhovoru, využít nahrávacího média a tento rozhovor si nahrát.

Jelikož v rámci tohoto rozhovoru se můžeme setkat s člověkem, který bude velmi pozitivně reagovat na naše podněty a tím se spustí rozhovor, který může trvat i několik minut. Informace, které jsou obsaženy v tak dlouhém rozhovoru, mohou být těžké k zapamatování, avšak použití jakéhokoli nahrávacího média je trestný čin, protože se dá předpokládat, že souhlas k tomu nedostaneme.

4.3 Zákon o kybernetické bezpečnosti

Poslední z řady zákonů je **Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)**. Tématem zvolené diplomové práce se zabývá zejména tento paragraf [34]:

§ 7 Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

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

(2) Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.“ [34]

Co se týče kybernetické bezpečnosti, díky použití výše zmíněných sociotechnik, jako je např. baiting, může dojít k narušení databází, které jsou spravovány interními zaměstnanci ICT oddělení. Díky skriptu, který se nachází na flash disku, může být narušená databáze a může tak zapříčinit pád systému nebo narušení integrity dat.

V této kapitole byly shrnuty zákony, které se týkají sociálního inženýrství a na které je potřeba si dávat pozor při využívání social engineering card v praxi.

II. PRAKTICKÁ ČÁST

5 TESTOVÁNÍ ZAMĚSTNANCŮ

Cílem této kapitoly je ukázat postup, kterým je možné získat senzitivní informace od zájmových osob. Tyto postupy byly konzultovány s vysoce postaveným manažerem bezpečnostní firmy XY. Bezpečnostní firma si nepřála být jmenována. Pro účely diplomové práce bude využit fiktivní název – firma XY. Díky konzultaci s tímto člověkem byly vytvořeny manuály, které mohou dopomoci k získání senzitivních informací. Cílem je vypracovat postupy, kterými si firma může ověřovat své vlastní zaměstnance. V další kapitole bude rozebráno školení, které má za cíl připravit zaměstnance tyto techniky rozpoznat a bránit se jim.

5.1 Rozdělení

V rámci této kapitoly jsou postupy rozděleny na dvě části. První část je technicky zaměřená. Jedná se o phishingový email a sociotechniku baiting. Výstupem těchto technik je grafické znázornění pomocí Event-process-chain (EPC) diagramů. Tyto diagramy znázorňují postupy a procesy, díky nimž by mohly být tyto techniky realizovány. Návrhy byly předloženy firmě XY, která souhlasila s jejich realizací. Nicméně jejich implementace proběhne až v dalším plánovaném testování. Důvodem je nutnost schválení testu takového rozsahu užším vedením firmy. Tento bod se na program jejich zasedání bohužel dostane až po odevzdání diplomové práce.

Druhá část je zaměřená na vytěžovaní zájmových osob prostřednictvím cílené konverzace, tato část je rozebrána v další kapitole. Tato kapitola se zabývá popsáním technického testování zaměstnanců. Výstupem druhé části jsou kartičky (social engineering cards), které slouží nejen jako manuál pro úspěšně vytěžování osob, ale také jako účinná obrana proti tomuto vytěžování. Součástí těchto karet jsou otázky, které jsou mířeny na získání senzitivních (citlivých) informací. Kartičky jsou přizpůsobeny tak, aby byly z části využitelné přímo v terénu.

5.2 Technicky zaměřené testování

Technicky zaměřené testování se skládá ze dvou částí, výstupem z obou částí jsou EPC diagramy, které mají za cíl přiblížit, jakým způsobem by mohly být dané techniky využity v praxi. Jak již bylo zmíněno výše, oba diagramy se líbily, bohužel interní schvalování v bezpečnostní firmě XY trvá dlouho, proto nebyly tyto techniky zrealizovány.

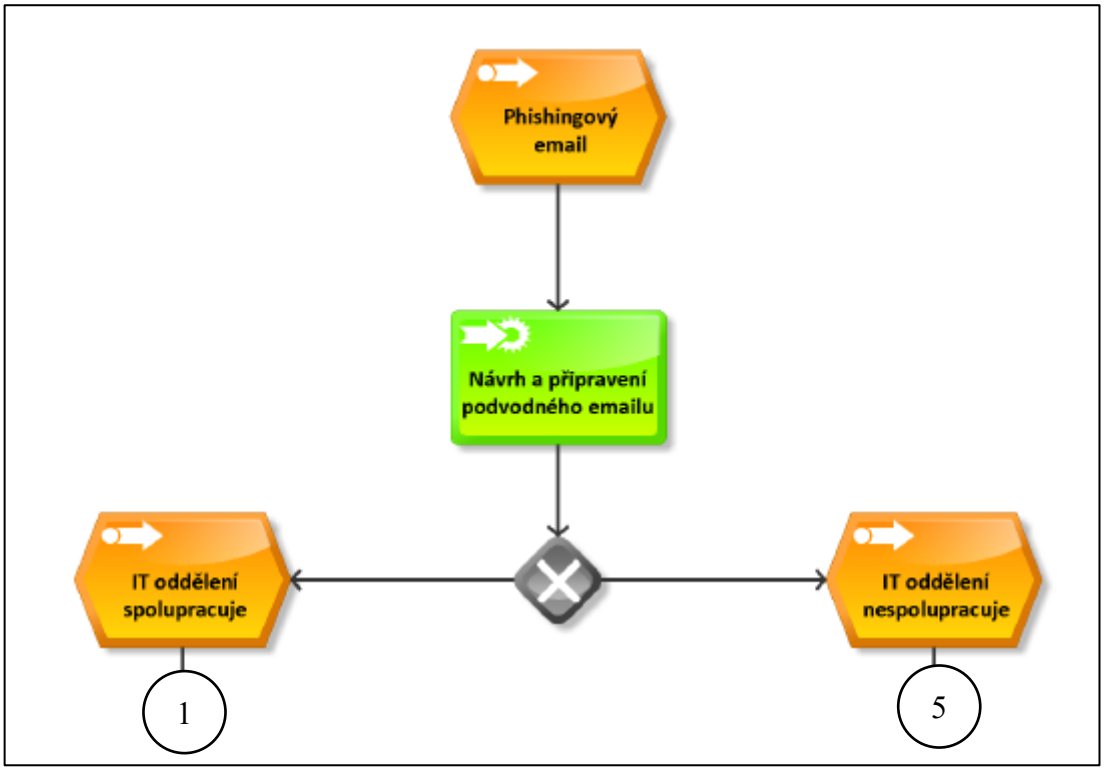
5.2.1 Phishingový email

První technikou je phishingový email. Jedná se o podvodný email, který má za cíl oklamat člověka, kterému tento mail posíláme. Cílem je zejména získání přístupových údajů a hesel.

5.2.1.1 Možný scénář

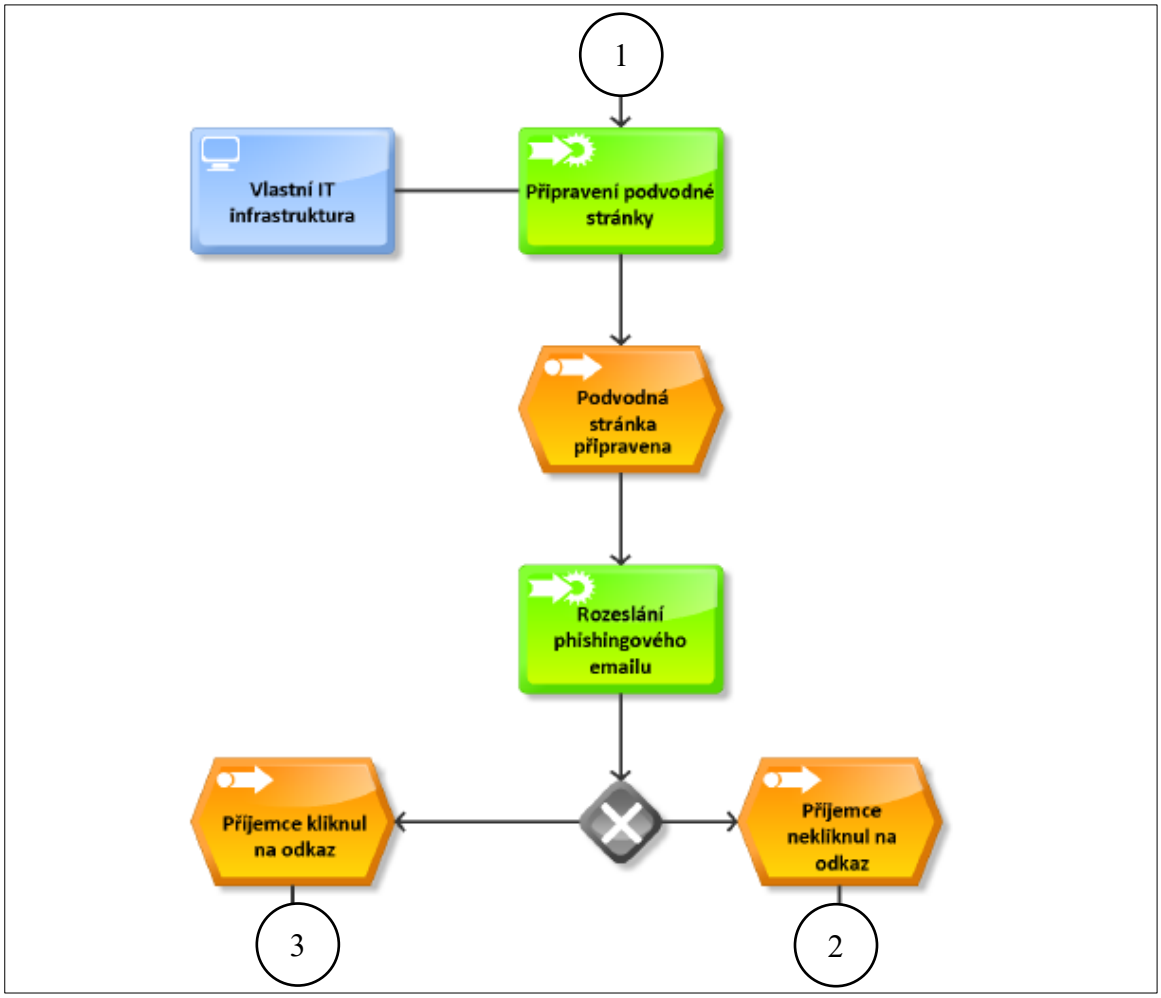
Mimo technické věci, které jsou potřeba k uskutečnění tohoto testu, je zapotřebí vytvořit důvěryhodný email. Pokud se jedná o email, který přijde do interní emailové schránky firemní sítě, může být v tomto emailu odkaz na formulář, který žádá o změnu stávajícího hesla z důvodu zvýšení bezpečnosti. Samozřejmě v rámci změny hesla je také důležité vyplnit přihlašovací údaje. V tento moment by pachatel disponoval jak heslem, tak přihlašovacím jménem.

Pokud se jedná o email, která je mimo interní síť firmy tzn. pro širší veřejnost, email nesmí obsahovat žádné formuláře ani jiné kolonky pro vyplnění, jelikož by se jednalo o trestný čin. Již samotné zaslání emailu může být považováno za šíření poplašné zprávy, což je taky trestné. Lze pouze umístit na stránku počitadlo, které bude počítat přístupy na stránku. Na stránce může být zobrazeno například „Stal jste se obětí phishingový emailu, dávejte si pozor, na co klikáte“.



Obr. 16. EPC diagram phishingový email – hlavní větvení

EPC diagram se skládá ze základních částí, kterými jsou aktivita (zelený obdélník) a událost (oranžový hexagon). Prvním krokem je aktivita vedoucí k navrhnutí phishingového emailu. Následně mohou nastat dvě události, buď bude IT oddělení firmy s tímto návrhem souhlasit – tedy bude spolupracovat (1), nebo IT oddělení s tímto návrhem souhlasit nebude – tedy nebude spolupracovat (5).

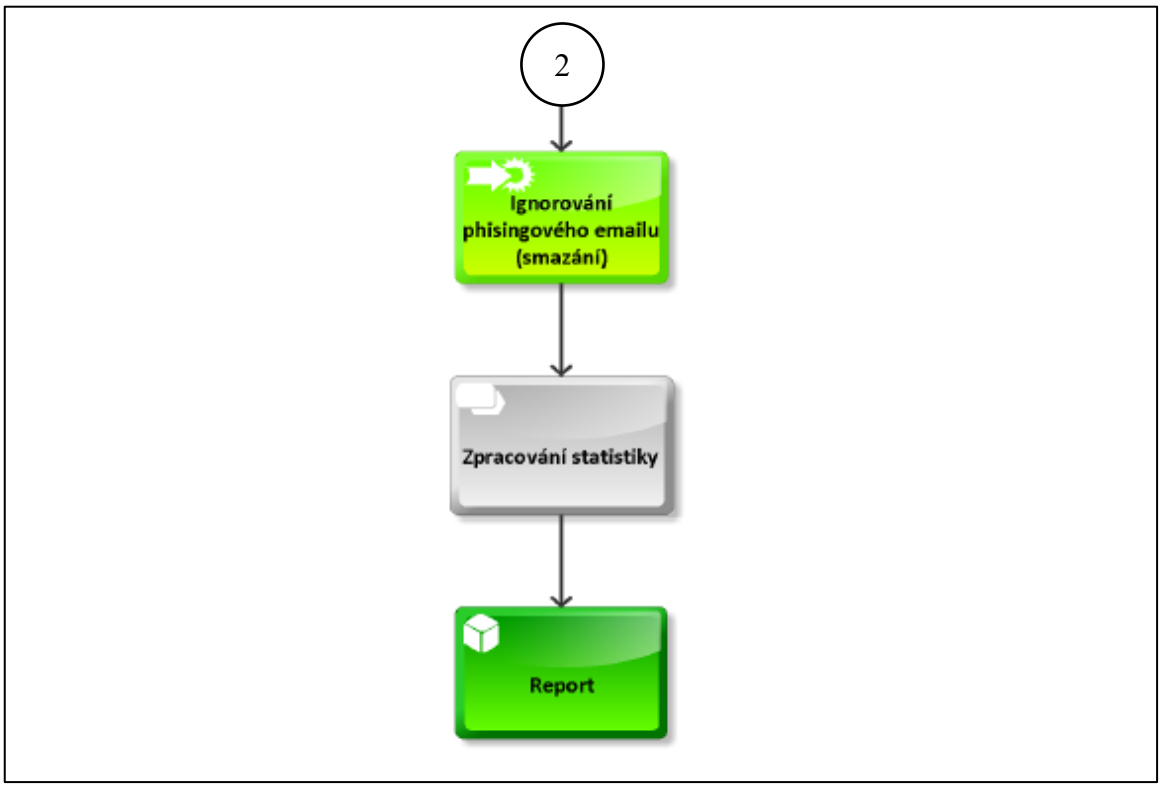


Obr. 17. EPC diagram phishingový email – IT spolupracuje

Následuje část, která zabývá scénářem, kdy IT oddělení spolupracuje (1). V dalším kroku je připravena podvodná stránka, která je provozována přímo na IT infrastruktuře dané firmy tzn., že si firma přizpůsobí zdrojový kód tak, aby nevznikl v průběhu testování žádný problém. Dalším krokem je připravení podvodné stránky. Podvodná stránka nesmí vypadat úplně stejně jako jsou stránky firemního webu, jelikož by to pak popíralo celý význam testování. Zde bude formulář pro vyplnění osobních údajů, jako jsou přihlašovací údaje do interní sítě firmy. Stránka se může tvářit jako interní zpráva, která žádá o vyplnění formuláře

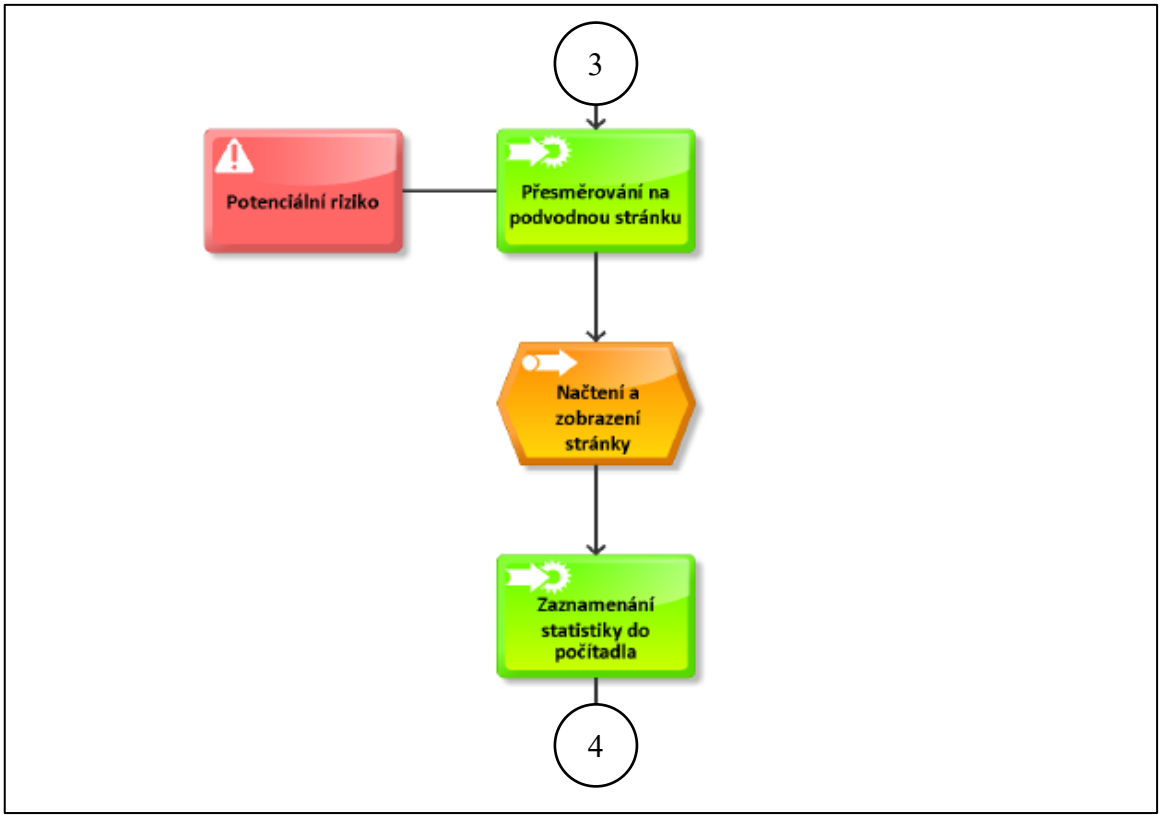
za účelem zdokonalení hesla, bude však nést malé známky nedokonalosti, aby mohl vniknout prostor pro podezření ze strany zaměstnanců.

Po vytvoření této stránky dojde k rozeslání emailů. Po příchodu emailu uživateli záleží, zda uživatel klikne na odkaz, který se nachází v emailu (3), nebo na tento odkaz neklikne (2).



Obr. 18. EPC diagram phishingový email – příjemce neklikl na odkaz

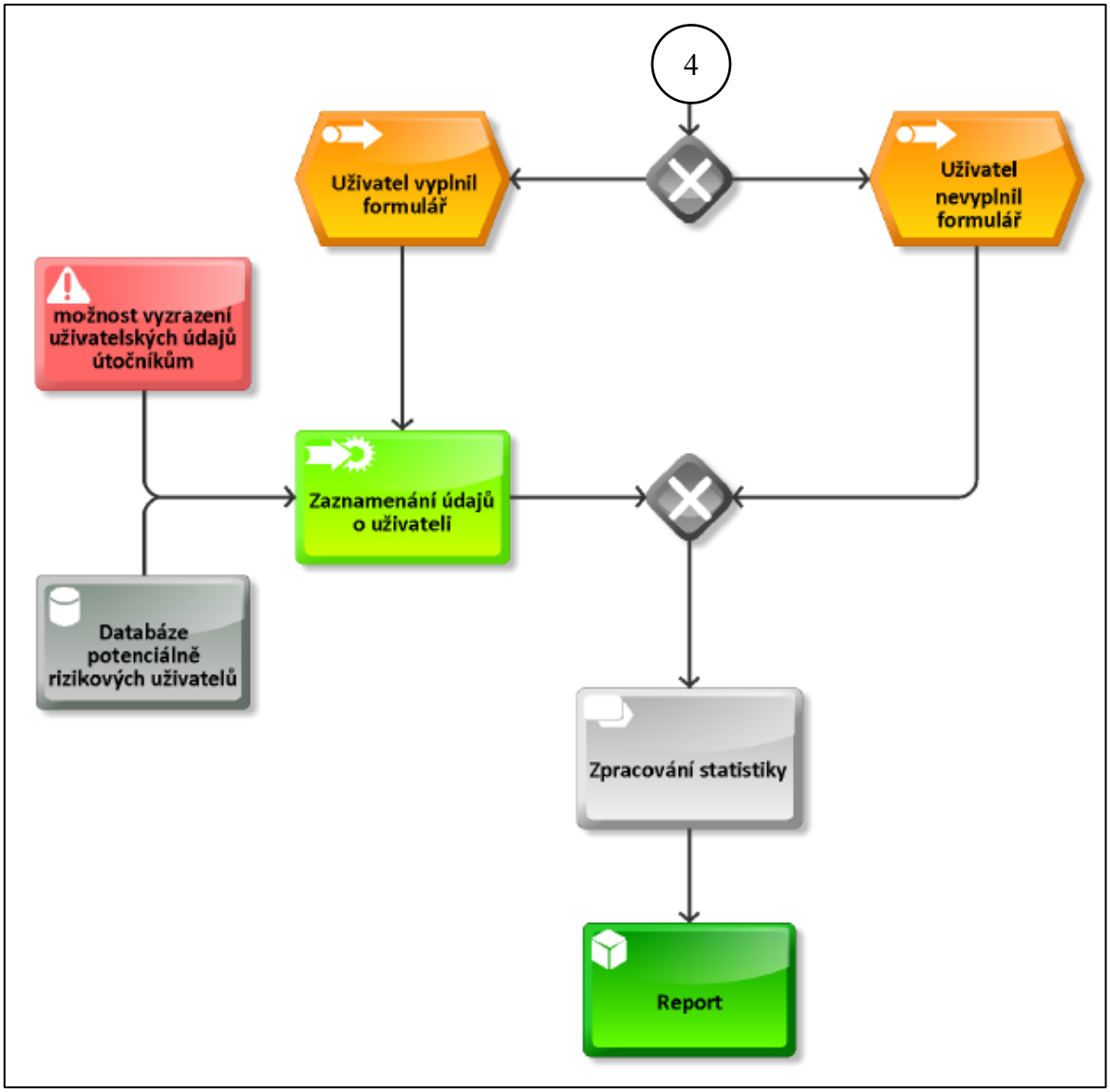
Další část se zabývá scénářem, kdy příjemce na odkaz v emailu neklikl (2). Může to být způsobené tím, že mu email vůbec nepřišel – spadl do spamu. V lepším případě si tento email přečte a ignoruje ho. Závěrem bude proces zpracování statistiky (v diagramu označeno jako šedý obdélník – sub-proces), jejímž výstupem bude report (produkt – označený tmavě zeleným obdélníkem).



Obr. 19. EPC diagram phishingový email – příjemce klikl na odkaz

Další část se zabývá scénářem, kdy příjemce na odkaz v e-mailu klikl. Po kliknutí na odkaz je uživatel přesměrován na připravenou podvodnou stránku. V jiném případě se tato stránka načte a přístup na tuto stránku se zaznamená do statistiky.

V rámci toho, že IT oddělení spolupracuje, je celý tento proces legální, protože se odehrává v interní síti firmy se souhlasem a podpisem obou stran – tedy člověka, který vykonává test a zástupcem firmy.

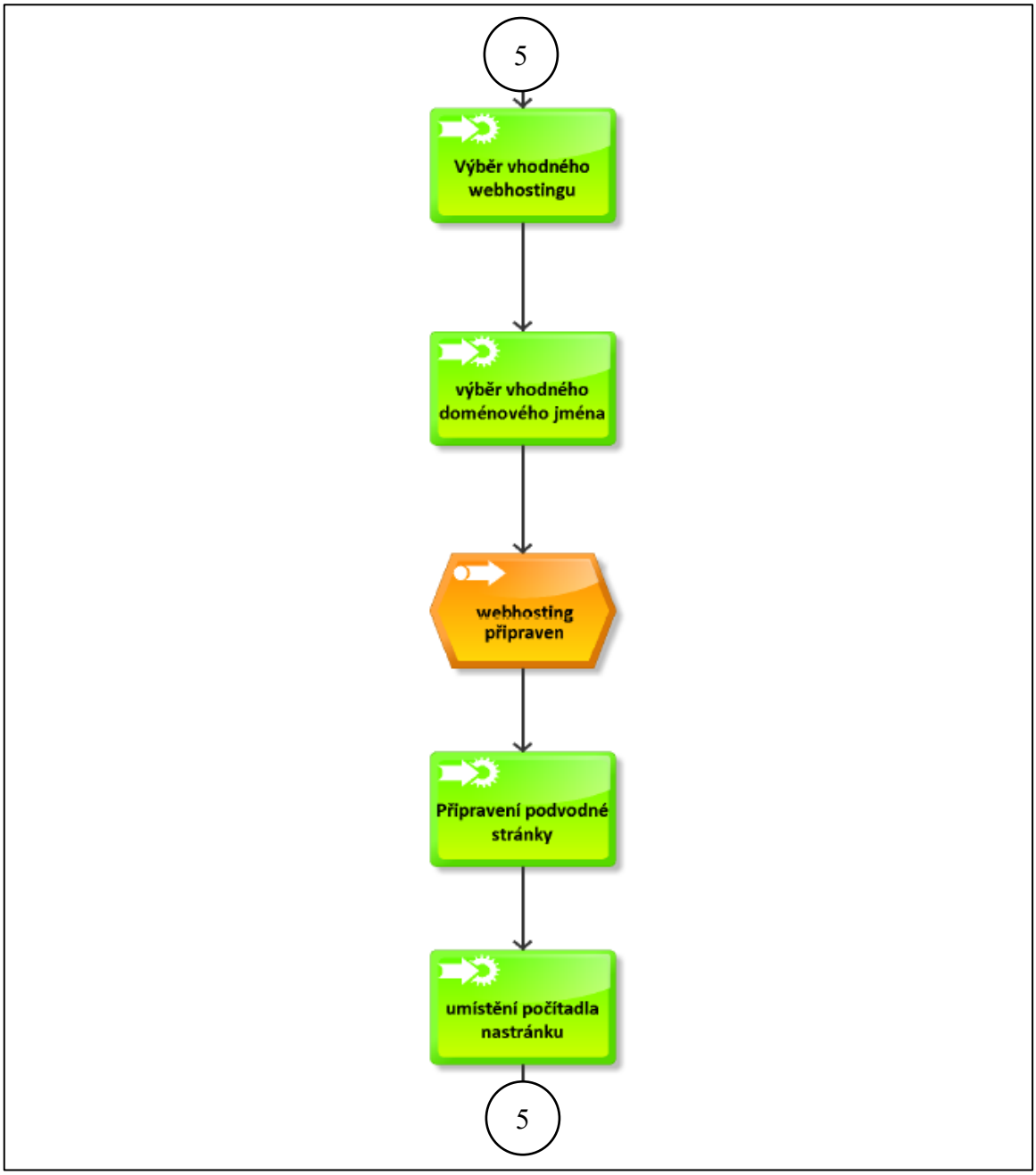


Obr. 20. *EPC diagram phishingový email – finální fáze větve, kdy oddělení spolupracuje*

V poslední části, která se týká větve, kdy IT oddělení spolupracuje, se dostáváme k bodu, kdy uživatel buď vyplní zobrazený formulář, nebo tento formulář nevyplní. Pokud tento formulář nevyplní, zapíše se do statistiky, že stránka byla zobrazena, ale nebyla vyplněna.

Pokud však uživatel tento formulář vyplní, zaznamenají se identifikační údaje o uživateli – za předpokladu, že každý uživatel má jedinečné přihlašovací údaje. V tomto bodě se mohou informace o uživateli uložit do databáze rizikových uživatelů. Zároveň je tento bod nejkritičtějším bodem celého EPC diagramu – je zde možnost, že uživatel, který vyplnit formulář, je potenciálně schopen vyzradit senzitivní informace jako jsou přihlašovací údaje.

Následující část se vrací zpět na základní větvení – tedy k části, kde IT oddělení nespolupracuje.



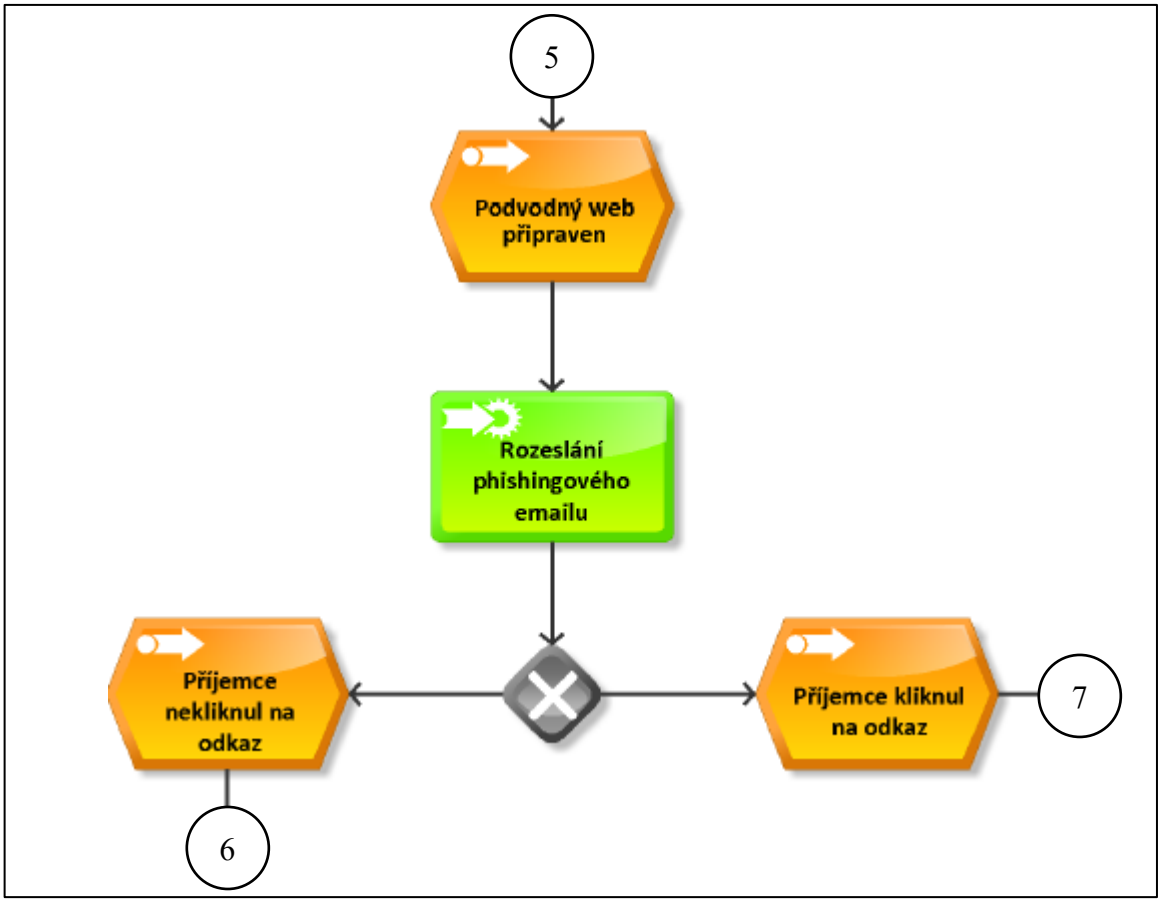
Obr. 21. EPC diagram phishingový email – IT oddělení nespolupracuje

V případě, že IT oddělení nespolupracuje, je důležité, aby byla doména důvěryhodná. Je tedy potřeba zvolit vhodný webhosting a zároveň vybrat vhodný název internetové domény.

V momentě, kdy je webhosting připraven, připraví se podvodná stránka. V tomto případě se podvodná stránka připraví za účelem ponaučení uživatele, který na tuto stránku klikne. Po-

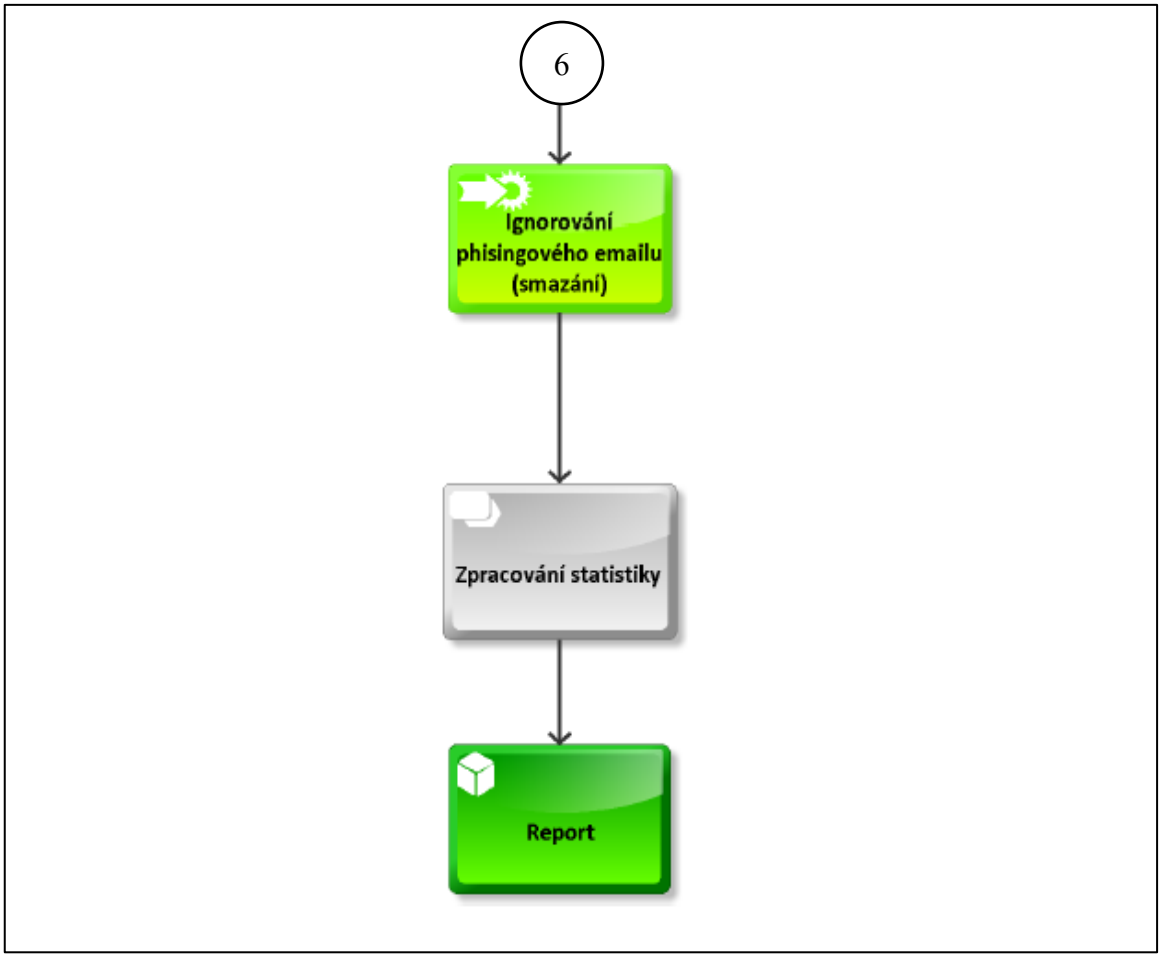
kud by na stránce byl podobný formulář, jako tomu bylo u větve, kdy IT oddělení spolupracuje, byl by to trestný čin. Uživateli se tedy po kliknutí na odkaz zobrazí například text – „Stal jste se obětí phishingu“.

Umístí se počitadlo na internetovou stránku, abychom měli přehled o tom, kolik přístupů tato stránka měla.



Obr. 22. EPC diagram phishingový email – IT oddělení spolupracuje

Pokud je podvodný web připraven, rozešle se email, který obsahuje odkaz na podvodnou stránku. Stejně jako tomu bylo u větve, kdy IT oddělení spolupracuje, záleží, jestli příjemce na odkaz obsažený v emailu klikne (7), nebo na tento odkaz neklikne (6).

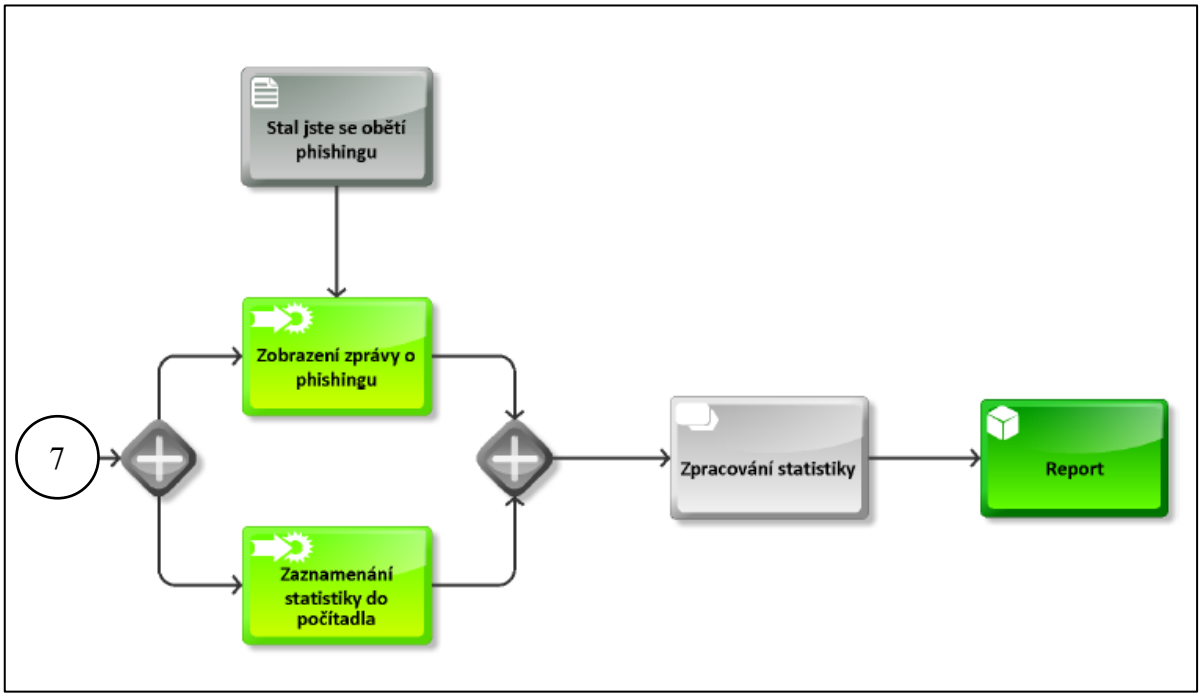


Obr. 23. EPC diagram phishingový email – příjemce neklikl na odkaz

Pokud příjemce na tento odkaz neklikl, může to být způsobené tím, že email spadl do spamu. V lepším případě uživatel tento email ignoruje, protože rozpoznal potenciální hrozbu.

Obr. 24. EPC diagram phishingový email – příjemce klikl na odkaz

V této části příjemce klikl na odkaz, který byl obsažený v emailu. Stejně jako tomu bylo u druhé větve, kdy IT oddělení spolupracuje, i zde je možné riziko, že stránka bude zablokována například antivirem. Pokud tak není, zobrazí se stránka s předem připraveným textem.



Obr. 25. EPC diagram phishingový email – zobrazení zprávy o phishingu

Poslední část v EPC diagramu větve, kde IT oddělení nespolupracuje, se liší od druhé větve. Zde není žádný formulář pro vyplnění osobních údajů. Pokud uživatel klikne na odkaz, zobrazí se mu na stránce, že se stal obětí phishingu. V rámci České Republiky je phishing trestný čin.

Počitadlo, které je umístěno na stránce v této větvi, pouze zaznamenává přístupy na tuto stránku, abychom věděli, kolik lidí na ni přišlo. Počitadlo, které je v první větvi, tedy ve větvi, kdy IT oddělení spolupracuje, zaznamenává i údaje o uživateli, jelikož se jedná o interní test.

5.2.2 Baiting pomocí USB flash disku

Druhou částí je sociotechnika, které se říká baiting. Tato technika funguje na principu návnady, kdy je připraveno médium – v tomto případě je to USB flash disk. Toto médium je upraveno tak, aby po připojení k počítači odesílalo data na námi zvolený server.

Stejně jako tomu bylo u předešlé techniky, pokud není člověk předem domluvený s firmou, u které chce tento test realizovat, jedná se o porušení zákona. V rámci firmy, kde tímto způsobem testujeme zaměstnance, můžeme tuto techniku využít.

5.2.2.1 Možný scénář

Pokud má být tato metoda účinná, musí se promyslet, kam se tento flash disk položí a jak by nejlíp tento flash disk mohl zaujmout. Taky je důležité promyslet místo, kam se flash disk odloží – nemůžeme flash disk položit na málo frekventované místo nebo na místo, kde se neshromažďuje cílová skupina, od které chceme vytěžit informace.

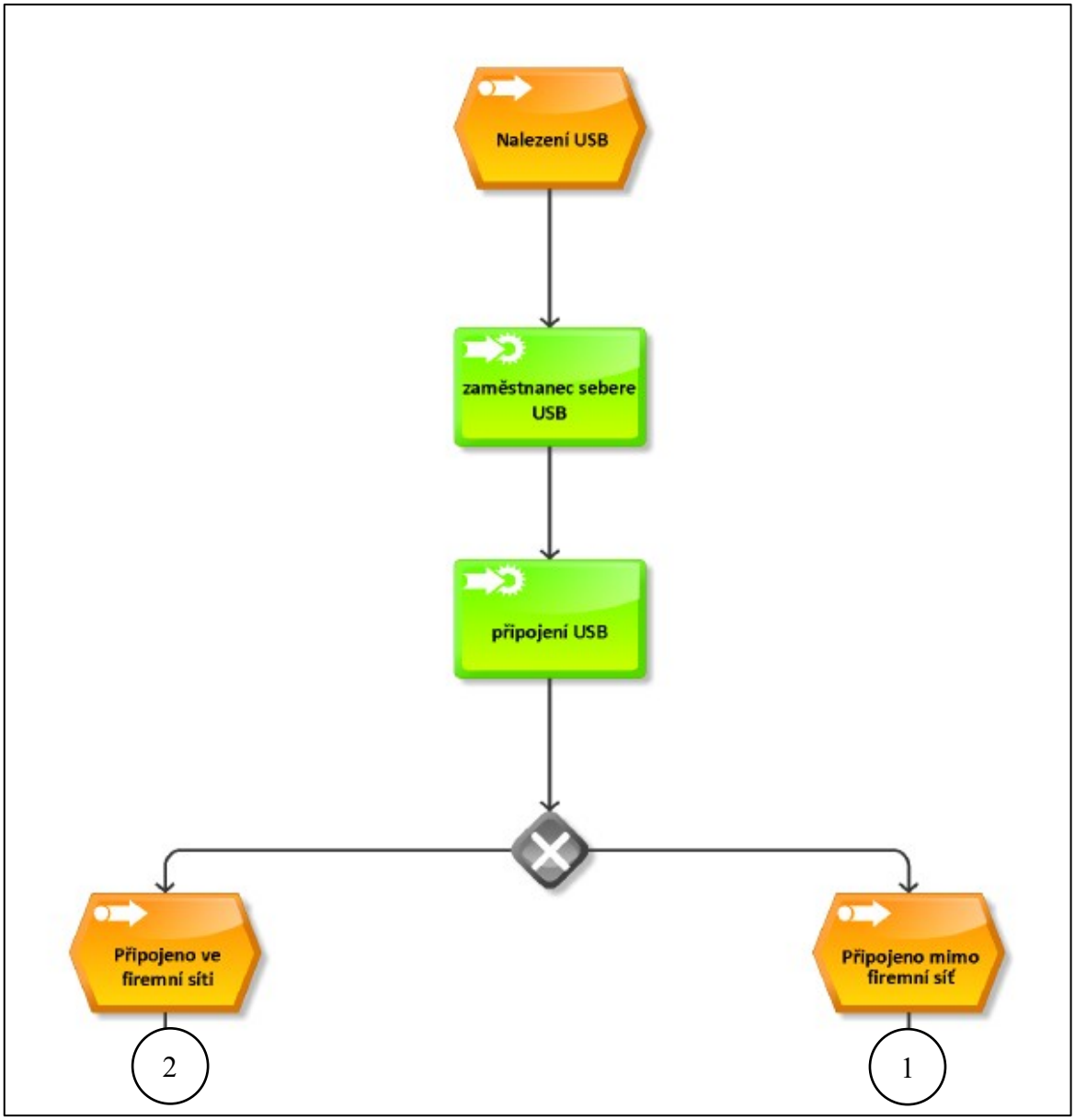
Je důležité taky vědět, od koho chceme získat důvěrné informace. Pokud se jedná o testování v rámci firmy, může být flash disk odložen ve společných prostorách nebo v chodbách na zemi. Může být také položený na pracovním stole dotyčné osoby, od které chceme získat informace. Pokud se nejedná o firemní prostory, může být flash disk položen na parkovištích nebo před hlavním vstupem.

Flash disk musí být patřičně pojmenovaný. Nejlépe tak, aby vzbudil pozornost, můžeme použít názvy jako:

- Výplaty_2018
- Dovolené_2018
- Zisk za loňský rok
- Prémie_2018

Jsou to názvy, které na první pohled zaujmou. Lidská zvědavost nezná mezí, a proto s největší pravděpodobností bude tato metoda účinná.

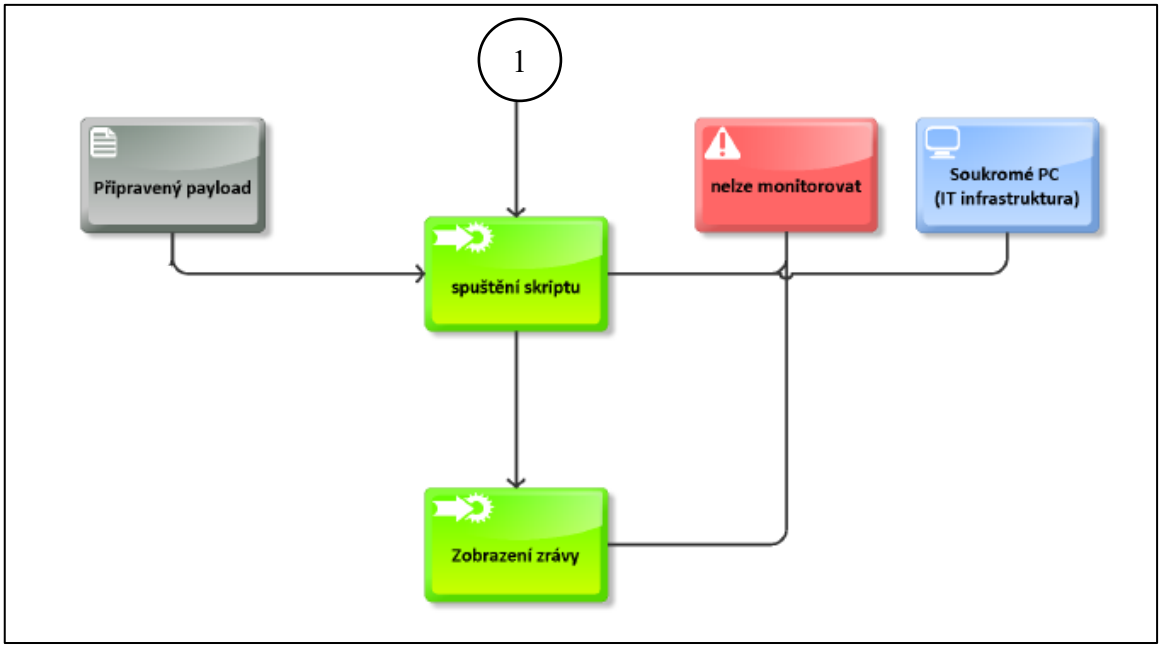
Co se týče testování širší veřejnosti, je tato metoda dost ošemetná. Pokud by byl na médiu skript, který by odesílal informace na cizí server, jedná se o trestný čin.



Obr. 26. EPC diagram USB baitingu – nalezení USB

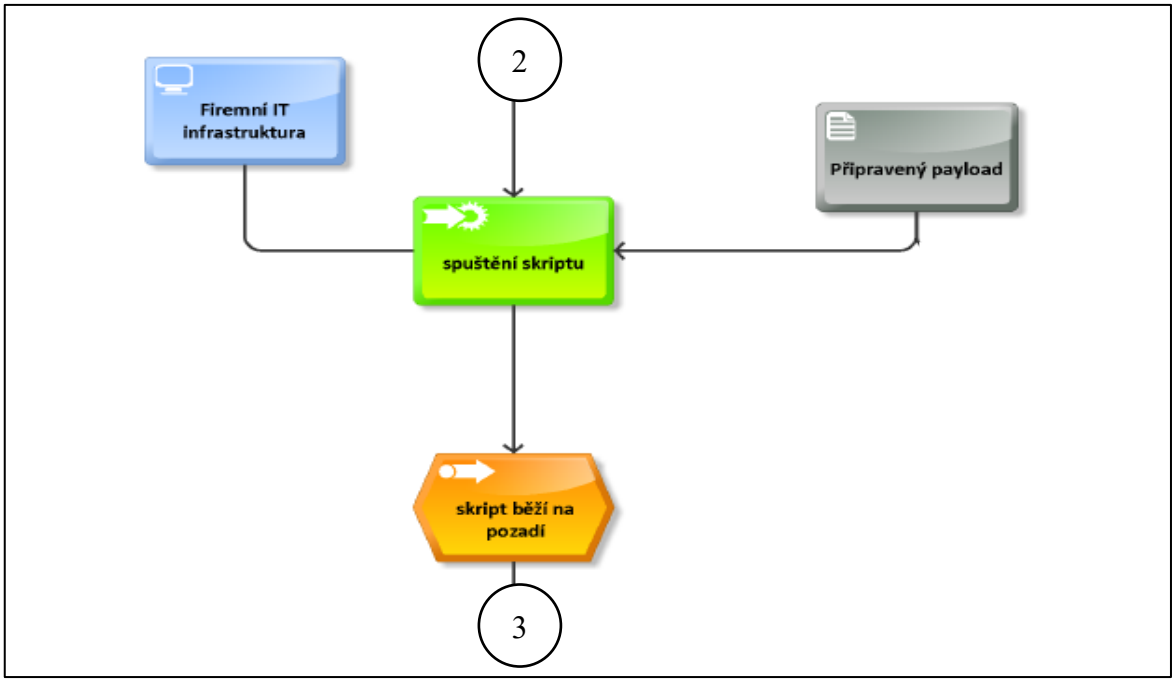
Pokud je USB flash disk nachystaný, umístíme ho na vhodné místo, kde bude s největší pravděpodobností nalezen. Jak již bylo zmíněno výše, mohou to být prostory, kde shromažďuje cílová skupina lidí, od kterých chceme senzitivní informace získat. Pokud USB flash disk nalezne zaměstnanec, pak záleží, jestli flash disk připojí ve firemní sítí (2), nebo flash disk připojí mimo firemní síť (1).

Jedná se o scénář, kdy firma spolupracuje. Vedení firmy o tomto testování ví a informace se odesílají na interní síť, kterou je firma vybavena.



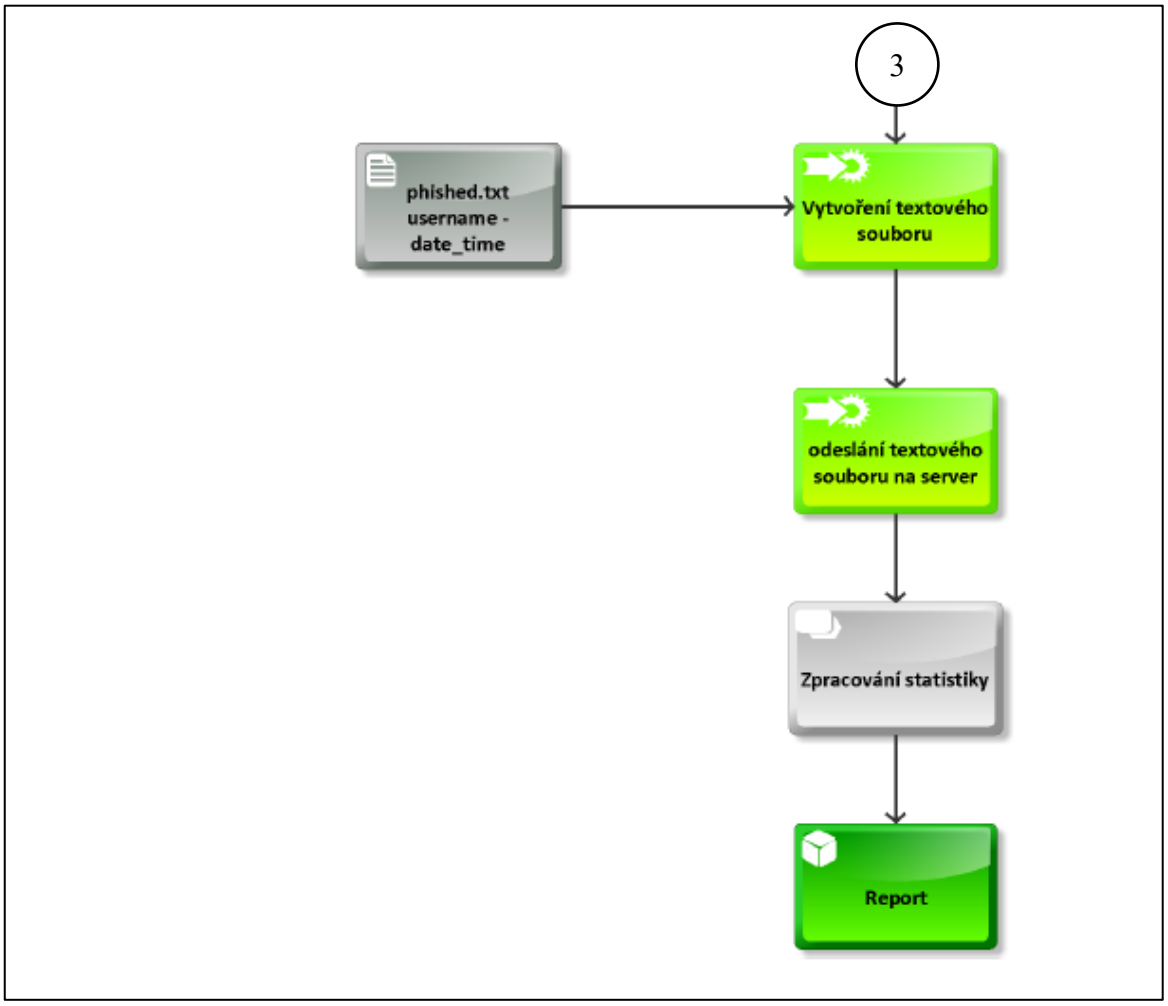
Obr. 27. EPC diagram USB baitingu – připojeno mimo firemní síť

Pokud je USB flash disk připojen mimo firemní síť, spustí se skript, který je připravený na USB flash disku. Payload jsou data, která jsou pro nás užitečná. Jsou to data, která jsou přenášena. Může nastat situace, kdy antivir daného počítače zakáže tento flash disk právě z důvodu toho, že je na něm obsažen skript, který komunikuje s cizím serverem. V EPC diagramu je tato část vyznačena červeným obdélníkem. Každopádně po připojení flash disku se zobrazí zpráva, kde je naspané „Stal jste se obětí baitingu“.



Obr. 28. EPC diagram USB baitingu – připojeno ve firemní síti

V rámci scénáře, kdy je USB flash disk připojen ve firemní síti, se postupuje podobně jako v části, kdy je USB flash disk připojen mimo firemní síť. Přes připravený payload se spustí skript, který shromažďuje senzitivní informace. Rozdílem v této částí je, že skript běží na pozadí a může shromažďovat informace, jako jsou přihlašovací údaje.



Obr. 29. EPC diagram USB baitingu – vytvoření textového souboru

V poslední fázi EPCho diagramu USB baitingu se vytvoří textový soubor, kde jsou nahrány informace, které byly odposlechnuty za dobu, kdy skript běžel na pozadí. Mohou to být informace jako přihlašovací údaje, ale mohou to být také senzitivní dokumenty, které jsou uloženy na disku vytěžovaného počítače.

Tento textový soubor je poté odeslán na předem určený server. Zpracuje se statistika o tom, jaké informace byly nalezeny a od koho tyto informace pochází. Výsledkem je report, který se předkládá firmě.

Testování zaměstnanců je rozděleno do dvou částí. První část je technicky zaměřená, jedná se o phishingový email a sociotechniku baiting, která by byla realizována pomocí USB flash

disku. V obou případech byly vytvořeny EPC diagramy, které popisují postup průběhu testování jednotlivých typů testů. Oba návrhy byly představeny vysoce postavenému manažerovi bezpečností firmy XY. Tyto návrhy se setkaly s úspěchem, bohužel nebyl čas pro realizaci kvůli internímu schvalovacímu procesu.

6 SOCIAL ENGINEERING CARD

Pro účel testování zaměstnanců byl vymyšlen soubor otázek, které byly následně použity v praxi. Cílem těchto mířených otázek bylo zjistit, zda jsou pracovníci bezpečnostních služeb ostražití při odpovídání. Za tímto účelem byl vytvořen systém testování zaměstnanců – social engineering card (dále jen SEC).

Jak již bylo zmíněno výše, cílovou skupinou jsou zaměstnanci bezpečnostních služeb, kteří mají za úkol hlídat určený prostor v obchodních domech či supermarketech. Metoda SEC byla zvolena na základě předchozích zkušeností z bakalářské práce, kde bylo vytěžování informací zpracováno pomocí otázek v dotazníkovém šetření. Karty budou malé, zhruba ve formátu A6 a budou popsány z obou stran. Čelní strana bude obsahovat sadu otázek podle zaměření a zadní strana bude obsahovat rady a tipy při pokládání těchto otázek.

V této práci jsou SEC zaměřené na získání více informací. Při konzultaci s odborníkem bylo vybráno zaměření, které je obecnější a zaměřuje se na více než jednu oblast – pracovní doba a přestávky, náplň práce, výše výdělku a typologie pachatelů. Lze však otázky v kartách upravit tak, aby bylo možné získat i jiné informace, například

- Dobré jméno firmy
- Podmínky v rámci firmy
- Komunikace s lidmi
- Překračování pracovních mezí
- Obcházení pravidel
- Vynášení informací

Všechny tyto karty by pak měly vlastní sadu otázek a trochu jiné postupy v rámci komunikace s danou osobou. Při konzultaci s odborníkem bylo vybráno zaměření, které je obecnější a zaměřuje se na více než jednu oblast – pracovní doba a přestávky, náplň práce, výše výdělku a typologie podezřelých osob.

6.1 Příprava karty

Při návrhu karty muselo být zohledněno, jakým způsobem by se měla konverzace vyvíjet a jakým způsobem pokládat otázky. Bylo také důležité určit si účel, proč se vlastně s člověkem z bezpečnostní firmy bavíme. Cílem vybrané karty je zjistit, kolik peněz člověk v práci vy-

dělává a jakým způsobem pracuje, jaká je jeho náplň a typologie podezřelých osob. Odpověďmi na tyto otázky můžeme získat senzitivní informace, které by se daly využít ve prospěch tazatele. Jsou to informace typu:

- Slepé místa kamer
- Kdy jsou přestávky a zda se zaměstnanci střídají
- Trasa, kterou zaměstnanec chodí
- Výše výdělku
- Kamery v objektu a jejich zorné pole
- Typologie podezřelých lidí

Pokud bude pachatel například vědět, jaká je typologie podezřelých lidí, bude se snažit vypadat nenápadně, tak aby zapadl mezi ostatní. Získání informace typu „mrtvé“ místa kamer v objektu mohou být taky využita ve prospěch pachatele. Výše výdělku může být využita pro potenciální podplacení ostrahy.

Nejdůležitější je s člověkem navázat kontakt. Nejlepší je se za někoho vydávat, tak aby to člověku nepřišlo podezřelé a cítil, že vás to zajímá. Forma a úroveň zvoleného jazyka se bude lišit podle situace. Následující otázky jsou spíše obecné a formálního rázu, slouží pro představu, jakým směrem by se měl rozhovor ubírat.

Otázky jsou rozděleny do více kategorií a jsou uspořádány tak, aby konverzace střídala zájmové otázky s odpočinkovými a kontrolními. Zájmové otázky jsou pro nás hlavní, jsou to otázky, díky kterým můžeme získat senzitivní údaje. Odpočinkové otázky, které mají za cíl zvolnit, jsou pro nás nedůležité. Kontrolními otázkami můžeme potvrdit předešlou in-formaci. Uspořádání kategorií je následující:

- Navázání kontaktu
- Pracovní doba a přestávky
- Náplň práce
- Doplňující otázky

Navázání kontaktu slouží zejména k „prolomení ledů“ jak ze strany tazatele, tak ze strany tázaného. Z kategorie navázání kontaktu jsou dvě možnosti, buď se tazatel vrhne na náplň práce, anebo na kategorii pracovní doba a přestávky. Přesný postup není daný, záleží podle situace. Jde spíše o to, aby celkový průběh cílené konverzace navazoval a měl hlavu a patu.

Nakonec přichází doplňující otázky, které slouží k odlehčení situace a zmírnění potenciálního napětí.

Není důležité využít všechny otázky, které jsou rozepsány níže. Tyto otázky slouží jako dopomoc k tomu, aby se člověk rozpovídal a abychom tohoto člověka dostali tam, kam potřebujeme. Otázky jsou spíše jako vodítko k tomu, aby člověk získal informace, které potřebuje.

6.1.1 Navázání kontaktu

Podle situace a předpřipraveného scénáře

1) Chtěl bych dělat jako bezpečnostní pracovník, nabíráte?
2) Jak to tu chodí?
3) Jak dlouho tady musíš stát?
4) To je docela mazec stát celý den na nohách ...
5) Jak dlouho to teda je …

6.1.2 Pracovní doba a přestávky

Obsahuje sadu otázek na pracovní dobu a přestávky:

6) Můžete aspoň na cigáro ven?
7) Jaká je tvoje pracovní doba?
8) Jak dlouho pracujete jako bezpečnostní pracovník?
9) Musí být náročné celou dobu stát/chodit …
10) Máte nějaké přestávky?
11) Střídáte se s někým? Nebo jste/jsi tu sám?

6.1.3 Náplň práce

Obsahuje sadu otázek dotazujících se na náplň práce:

12) Pokud bych tu dělal, co bych dělal?
13) Staráte se zároveň i o kamery?
14) Střídáte se u kamer?
15) Stává se, že by zloděj nebyl zachycen kamerou přímo při krádeži?

6.1.4 Otázky na výši výdělku a doplňující otázky

Obsahuje otázky mířené na výši výdělku, také jsou zde doplňující otázky.

16) Tak kolem dvanácti tisíc bych si tady mohl vydělat, ne?
17) Možná trochu osobní, ale můžu se zeptat, jaký máte plat? Vyžijete?
18) Stíháte nějaké koníčky i mimo práci?
19) Já jsem třeba kuřák, máte čas i na kouřovou přestávku?
20) Jaký je šéf, je v klidu?

Výše uvedené otázky, spolu s úvodní částí této kapitoly byly sestaveny ke konzultaci s odborníkem – zástupcem bezpečnostní firmy XY.

6.2 Konzultace s odborníkem

V rámci toho, jakým způsobem hovořit s lidmi z bezpečnostních služeb, jaké informace jsou vlastně senzitivní a jak mají být otázky sestaveny, byla domluvena schůzka s vysoce postaveným manažerem bezpečnostní firmy XY, která má v České republice velké zastoupení. V rámci konzultace s odborníkem bylo získáno nespočet rad a zkušeností, jakým způsobem s dotyčnými lidmi mluvit a jakým způsobem se jich ptát. Následně bylo doporučeno, aby byl tento test vyzkoušen na nečisto pro účely „prolomení ledů“ samotného tazatele, jelikož není tak jednoduché přijít za někým a ptát se ho na otázky, které směřují k získání senzitivních informací. Proběhlo testování na nečisto, jehož výsledkem bylo upravení otázek do přijatelné podoby. Zejména se jednalo o úprava jazyka, který byl použit původně při vytváření otázek. Ze spisovné češtiny na spíše hovorovou až slangovou češtinu. Také byla pozměněna posloupnost otázek, některé otázky byly přidány nebo upraveny.

Testování na nečisto bylo provedeno u jiných bezpečnostních firem, než je firma XY.

6.3 Upravení karet

Díky konzultaci byly některé otázky upraveny a pozměněny. Přibyly například otázky:

- Jak probíhají přestávky?
- Máte danou trasu obchůzky?
- Máte pravidelné přestávky?

Tyto otázky byly následně rozčleněny do patřičných kategorii. Byly přidány z důvodu toho, že pokud se člověk rozmluví, může být získáno mnoho informací. Dále byly upraveny otázky, které neodpovídaly žargonu, který se používá v rámci bezpečnostních pracovníků. Byly to otázky:

- Chtěl bych dělat jako bezpečnostní pracovník, nabíráte?

- Jak dlouho pracujete jako bezpečnostní pracovník?
- Tak kolem dvanácti tisíc bych si tady mohl vydělat, ne?

Tyto otázky v rámci osobních zkušeností odborníka byly přepracovány na otázky:

- Chtěl bych dělat v „sekurity“ nabíráte?
- Jak dlouho pracujete/pracuješ jako bezpečák?
- Tak tu dvanáctku bych si tady mohl vydělat, ne?

Dále byla u každé otázky doplněna možnost tázat se vykáním anebo tykáním.

V rámci konzultace s odborníkem byly vytvořeny kartičky, které sebou může tazatel nosit a nechat se inspirovat. Kartičky jsou vytvořený tak, aby byly srozumitelné pro laika a zároveň slouží také jako manuál. Karty byly navrhnuty tak, aby byly nenápadné a byly na nich umístěny ty nejužitečnější informace. Jsou navrženy ve formátu A6, kde z jedné strany jsou otázky, které spadají do dané kategorie, a na druhé stránce jsou stručné poznámky týkající se postupu při kladení těchto otázek.

6.3.1 Karta – Navázání kontaktu

Karta, kde jsou otázky z kategorie navázání kontaktu. Pořadí nebo výběr těchto otázek není daný. Záleží na situaci, ve které se bude tazatel nacházet. Je důležitá jistá míra improvizace. Karty nejsou ve finální grafické podobě. Budou se upravovat s pomocí grafika.

- Chtěl bych dělat v „sekurity“, nabíráte?
- Jak to tu chodí?
- Jak dlouho tady musíš stát?
- To je docela mazec stát celý den na nohách …
- Jak dlouho to teda je …

Obr. 30. Karta navázání kontaktu – přední strana

- Informativní otázky sloužící k navázání kontaktu
- Je potřeba prolomit ledy – důvěra tázaného
- Přizpůsobit styl vyjadřování
- Promyslet tykání a vykání

Obr. 31. Karta navázání kontaktu – zadní strana

Informace, které jsou obsaženy na zadní straně jsou informativní a slouží k připomenutí nejdůležitějších bodů, kterých je třeba se v průběhu cílené konverzace držet.

Před samotnou fází navázání kontaktu je důležité si člověka prohlédnout a usoudit, jakým způsobem se s tímto člověkem bavit. Zda zvolit spíše tykání nebo vykání a jakým způsobem se představit. Otázky ze sekce navázání kontaktu jsou informativní, slouží k vytvoření jakéhosi pouta mezi vámi a člověkem, od kterého chcete získat informace, navázání kontaktu. Aby byla metoda co nejúčinnější, je potřeba získat důvěru dané osoby a zároveň aby bylo možné naladit se na jeho reakce. Říká se tomu neurolingvistické programování. Vzbuzení důvěry je důležité k získání co nejvíce informací v následujících otázkách. Důležité je také přizpůsobit styl vyjadřování člověku, se kterým se bavíme.

6.3.2 Karta – Pracovní doba a přestávky

Stejně jako tomu bylo v předchozí části i tady je kartička popsaná z obou stran. V rámci této kategorie je důležité, aby si člověk dával pozor na návaznost těchto otázek a zbytečně nepřeskakoval. Může se stát, že člověk, na kterého je tato konverzace cílena, může pojmout podezření.

- Můžete/můžeš aspoň na cigáro ven?
- Jaká je vaše/tvoje pracovní doba?
- Jak dlouho pracujete/pracuješ jako bezpečák?
- Musí být náročné celou dobu stát/chodit …
- Máte/máš nějaké přestávky?
- Jak probíhají přestávky?
- Máte/máš pravidelné přestávky?
- Střídáte/střídáš se s někým? Nebo jste/jsi tu sám?

Obr. 32. Karta pracovní doba a přestávky – přední strana

- Návaznost otázek
- Pozorně naslouchat a filtrovat důležité informace
- Využít příležitost, kdy se člověk komunikačně otevře
- Zbytečně neklást důraz na posloupnost otázek
- Nechat konverzaci spíše volný průběh

Obr. 33. Karta pracovní doba a přestávky – zadní strana

V této kategorii je důležité nechat tázaného rozmluvit. Tato část je klíčová pro navázání na další sadu otázek a naopak. Druhá a třetí sada otázek může být v rámci cíleného rozhovoru přehozena. Pokud je tedy použita třetí sada otázek, pak je tato sada klíčová pro navázání na druhou sadu otázek.

Z první třetiny otázek je možné se dozvědět, na kolik hodin člověk chodí do práce anebo naopak kdy v práci končí. Zároveň se můžeme dozvědět o tom, jak zkušený tento člověk je, tzn., pokud řekne, že pracuje pouze chvíli, můžeme předpokládat, že bude tento člověk více otevřený diskuzi než člověk, který je více zkušený, tudíž může být více odolný vůči citlivějším otázkám.

Z druhé třetiny otázek je možné se dozvědět, zda má pracovník nějaké přestávky a kdy tyto přestávky má. V kombinaci s otázkou na pravidelnost těchto přestávek se tak potencionální pachatel může dozvědět, v jakém čase je objekt nejzranitelnější. Stejně tak pokud tazatel odpoví, že se s nikým nestřídá nebo že je zrovna kolega nemocný a není nikdo, kdo by ho zaskočil.

V poslední části karty je důležitá pro potvrzení předešlých informací z pohledu pachatele. Může si tak potvrdit nebo vyvrátit, zda ve chvíli přestávky může dojít k potencionálnímu útoku, či nikoli.

6.3.3 Karta – náplň práce

Jak již bylo zmíněno výše, pořadí druhé a třetí sady otázek není směrodatné. Tazatel může klidně po úvodní kartě – navázání kontaktu pokračovat kartou náplň práce místo karty pracovní doba a přestávky.

- Pokud bych tu makal, co bych dělal?
- Máte/máš danou trasu?
- Staráte/staráš se zároveň i o kamery?
- Střídáte/střídáš se u kamer?
- Stává se, že by zloděj nebyl zachycen kamerou přímo při krádeži?
- Jak poznáte/poznáš zloděje?

Obr. 34. Karta náplň práce – přední strana

- Je důležité vycítit vhodnou příležitost pro kladení otázek z této kategorie
- Druhou polovinu otázek v kartě použít za předpokladu, že je člověk komunikačně otevřený
- Snažit se odlehčit situaci

Obr. 35. Karta náplň práce – zadní strana

Konverzace se vyvíjí pokaždé úplně jinak, proto je důležité zachovat si chladnou hlavu a zbytečně nepanikařit. Co se týče této kategorie obzvlášť, pokud vidíme, že tázaný je z našich otázek v rozpacích, je potřeba situaci odlehčit a zkusit ji vést jiným směrem.

Z první dvojce otázek může být vytvořen přehled o tom, jaká je pracovní náplň pracovníka bezpečnostní služby, tzn., co všechno přes den musí stihnout a jaké jsou jeho povinnosti. Potencionální pachatel si tak může sestavit harmonogram pracovníka bezpečnostní služby.

Ze zbylých otázek je možné se dozvědět, zda mají pracovníci, pokud jsou dva, plný přehled nad objektem díky kamerám, které jsou v objektu nainstalovány. Poslední otázka směřuje na typologii podezřelých osob v objektu.

6.3.4 Karta na výši výdělku a doplňující otázky

Doplňující otázky neslouží pouze pro ukončení cílené konverzace, ale také jako odlehčení v podobě otázek, které nesouvisí se získáváním senzitivních informací. V rámci této karty jsou také otázky, které směřují na výši výdělku.

- Tak tu dvanáctku bych si tady mohl vydělat, ne?
- Možná trochu osobní, ale můžu se zeptat, jaký máte/máš plat? Vyžijete/vyžiješ?
- Stíháte/stíháš nějaké koníčky i mimo práci?
- Já jsem třeba kuřák, máte/máš čas i na kouřovou přestávku?
- Jaký je šéf, je v klidu?

Obr. 36. Karta doplňující otázky – přední strana

- Odlehčení situace
- Otázky mohou být použity i v případě, že bude hrozit odhalení
- Příprava na konec konverzace

Obr. 37. Karta doplňující otázky – zadní strana

Nejčastější problém, který může při dotazování nastat je ten, že někteří tázaní bezpečnostní pracovníci nechtějí odpovídat na otázky směřované na výdělek, je jim to hodně nepříjemné.

Díky doplňujícím otázkám je možné zjistit, jestli je zde možnost pracovníka uplatit. Také můžeme výši výdělku pracovníka bezpečnostní služby chápat jako jakousi rovnici. Čím víc peněz vydělává, tím větší motivaci k práci může mít, tzn., že bude nejspíš odvádět svoji práci

více svědomitě a s větší precizností. Naopak pracovník, který vydělává málo peněz může mít sklon k nekvalitně odvedené práci nebo třeba k častějším a delším přestávkám. Otázky na výši výdělku je důležité, pokud je k tomu správná situace, použít na konec. Ne vždy se podaří na tuto otázku získat odpověď.

Doplňující otázky jsou důležité z pohledu uklidnění situace. Mají za úkol, aby nebyl v bezpečnostním pracovníkovi vzbuzen pocit nátlaku a aby se po celou dobu cílené konverzace cítil komfortně.

6.4 Testování

Otázky byly sestaveny tak, aby se tazatel dozvěděl věci, které by zaměstnanec bezpečnostní firmy neměl sdělovat. Otázky jsou zaobalené tak, aby byly nenápadné, ale zároveň na ně nesmí být jednoznačná odpověď typu ano, ne. Jsou to informace, které jsou známy pouze pracovníkům ostrahy a dají se použít ve vlastní prospěch.

Social engineering card test byl vyzkoušen celkem na 25 zaměstnancích bezpečnostních služeb. Z toho 6 zaměstnanců bezpečnostní firmy neposkytlo žádné informace, respektive informace, které by byly nějakým způsobem užitečné. Bylo to způsobeno chybami ze strany tazatele. Tyto nepovedené testy byly spíše ze začátku testování, ale postupem času byly chyby eliminovány a SEC se setkala spíše s úspěchy než neúspěchy. Pro testování těchto karet byly vybrány obchodní centra v Brně, Olomouci, Zlíně a Vsetíně.

Chyby ze strany tazatele se týkaly spíše malé sebedůvěry, takže konverzace většinou končila tím, jestli nabírají a jestli je tato práce náročná. Ve dvou případech pracovníci odmítali sdělit informace, které se týkaly konkrétně kamer. Odvětili, že na toto téma se mnou nemůžou hovořit a tím byl v podstatě rozhovor u konce.

V průběhu testování nevyplynulo ze strany bezpečnostních pracovníků žádné podezření o tom, že by byli nějakým způsobem vytěžováni.

Otázky jsou sestaveny tak, aby vytvářely určitou posloupnost. Ve většině případů se konverzace nevyvíjí tak, jak se předpokládá na začátku. Je potřeba při rozhovoru hodně naslouchat a mnohokrát se například stalo, že z otázky, která byla mířená na kamery, jsme se dostali až k fotopastím, které se umisťují v lesích, nebo na otázku, zda mají v průběhu směny čas na cigaretu, jsme se dostali ke špatnému zdravotnímu stavu rodinného příslušníka.

Celkově bylo zjištěno 37 různých druhů informací, které se dají považovat za senzitivní. Informace se převážně opakovaly, tudíž byly zařazeny do pěti kategorii:

- Kamery – slepá místa
- Výše výdělku
- Přestávky – obsluha kamerového systému
- Typologie podezřelých lidí
- Prohlídka kamerové místnosti

Při testování zaměstnanců byly nejvíce sdělovány informace, které souvisí se slepými místy kamer v objektu. Nejpočetnější skupinou pracovníků, kteří sdělovali tento typ informace, byli kuřáci. Když byli dotázaní, zda chodí kouřit ven a kam, odpověděli, že chodí tam, kde kamery nevidí. Mimo zmiňované kuřáky byli někteří zaměstnanci ochotni sdělit i slepá místa kamer, které se nacházely přímo ve střeženém objektu. Někteří z nich si stěžovali, že se občas na těchto místech odehraje nějaká potyčka a nejsou tak schopni z kamerového záznamu zjistit, kdo je viníkem.

Další kategorií, která byla hojně sdělována bezpečnostními pracovníky, byla kategorie výše výdělku. Otázky směřující na výši výdělku spadají do poslední kategorie v rámci social engineering card – tedy doplňující otázky. Záměrně byly tyto otázky vloženy do této kategorie, protože poležením těchto otázek se staly dvě věci. V prvním případě bezpečnostní pracovníci zareagovali kladně a otázku zodpověděli, a dokonce se i rozpovídali. V druhém případě na otázku odmítali odpovědět a hned poté bylo cítit napětí, v důsledku toho byla konverzace ukončena.

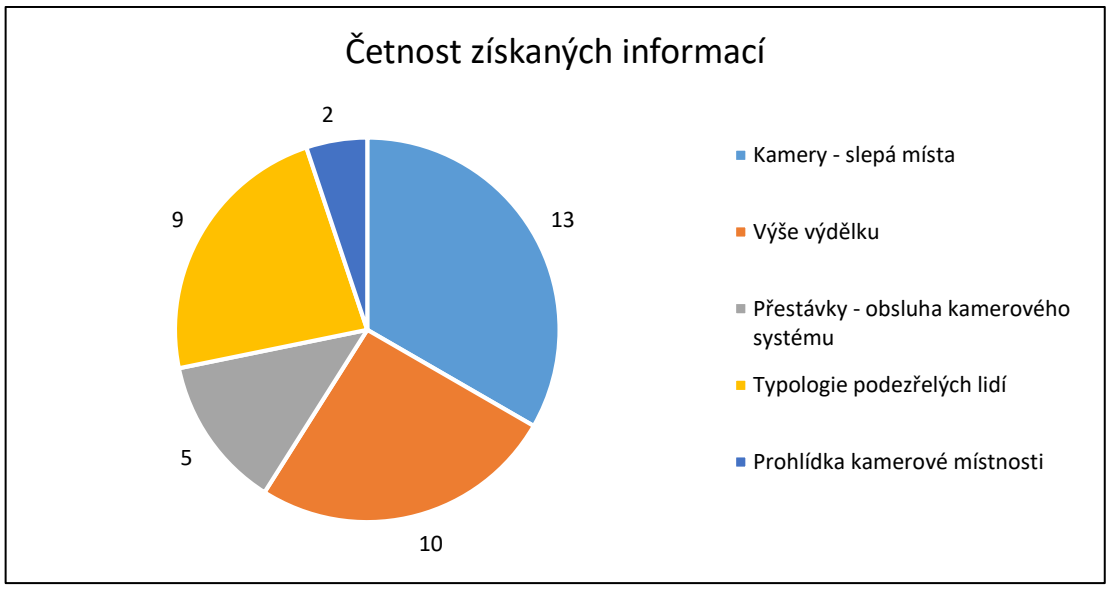
Někteří zaměstnanci byli ochotní poskytnout informace o tom, kdy má přestávku člověk, který dohlíží na kamery v kamerové místnosti. Za normálních okolností by tohoto pracovníka vystřídal jiný pracovník, který má zrovna stejnou směnu. Skutečnost je taková, že tito pracovníci si udělají přestávku ve stejnou chvíli. Na místě tak zůstávají pracovníci, kteří dělají obchůzky.

Dalším zajímavým zjištěním v průběhu testování bezpečnostních pracovníků byla typologie podezřelých lidí. Někteří pracovníci se rozpovídali o tom, jakým způsobem si tipují lidi, kteří mohou být potencionálními pachateli. Všichni popisovali potencionální pachatele dost podobně na základě vlastních zkušeností:

- Osoby pod vlivem omamných látek
- Menšiny
- Dospívající děti ve skupinkách

- Lidé s podezřelým chováním

Osoby pod vlivem omamných látek mají spíše tendenci být agresivní a svému okolí nebezpeční. Dospívající děti ve skupinkách jsou taky podle pracovníků častým problémem, protože se rádi před kamarády předvádí. A lidé s podezřelým chování mohou být lidé, kteří jsou nervózní, často se ohlíží, jestli je nikdo nevidí, vyhledávají uličky, kde nejsou žádní lidé apod.



Graf 1. Celkový podíl získaných informací

Tab. 1. Získané informace

Druh informace	Počet
Kamery – slepá místa	13
Výše výdělku	10
Přestávky – obsluha kamerového systému	5
Typologie podezřelých lidí	9
Prohlídka kamerové místnosti	2
Celkem informací	39

6.5 Komunikace (typy lidí)

V rámci předchozí kapitoly testování je důležité také popsat, jakým způsobem komunikovat s lidmi. V následující podkapitole budou vysvětleny způsoby mluvy s bezpečnostními pracovníky.

Je zásadní si dávat pozor, jakým způsobem mluvíme s dotyčnou osobou, od které chceme získat informace. Nejdůležitější je prvotní analýza tohoto člověka, v našem případě se jedná o bezpečnostního pracovníka. Musíme sledovat jeho postoj, musíme číst jeho reakce a v neposlední řadě musí být předem dobře připravený tázající.

Nejenom, že musejí být „prolomeny ledy“ u dotyčné osoby, kterou chceme vytěžovat, ale tyto ledy musejí být nejdříve prolomeny u tázajícího. Tato disciplína vyžaduje určitou míru praxe a verbálních zkušeností.

6.5.1 Způsob mluvy

Jak již bylo zmíněno výše, je důležité, aby člověk „prolomil ledy“. K tomu dojde, pokud se člověk bude chovat přirozeně a nebude se nad dotyčnou osobou chovat povýšeně. Zároveň nesmí být vzbuzeno podezření, že se snažíme získat informace, které bychom mohli využít v náš prospěch. Všechny tyhle podmínky je těžké splnit, avšak každý rozhovor je úplně jiný a nedá se jednoznačně dopředu říct, jakým směrem se rozhovor bude ubírat. Je hodně proměnných, na které je potřeba si dávat v průběhu rozhovoru pozor. Nejdůležitější je tak improvizace, improvizace na základě vlastních zkušeností. I přesto, že je důležitá určitá míra improvizace, dá se řídit podle těchto základních pravidel:

- Naslouchat
- Dorovnat se na jazykovou úroveň tázaného
- Prokládat projev vlastními emocemi
- Ukázat známku nedokonalosti (pokory)

Naslouchat je důležité. Můžete se setkat s lidmi, kteří mohou být nadšeni z toho, že máte zájem o tuto práci a začnou mluvit – a mluví hodně. Pokud se člověk dostane do tohoto bodu, je to to nejlepší, co se může stát. Člověk, který se rozmluví o své práci jako bezpečnostní pracovník a je plný emocí, např. hněv na svého šéfa, stává se tak nejlepším subjektem pro vytěžování. V této pozici stačí pouze naslouchat. Na druhou stranu není jednoduché naslouchat a pak reagovat. Člověk musí mít jistou míru empatie, aby dokázal v průběhu této jednostranné konverzace reagovat na podněty mluvícího. Podněty, které dáváme takto rozmluvenému člověku, by měly směřovat k otázkám, na které chceme znát odpověď anebo ho popíchnout směrem, u kterého by bylo pak jednoduché se k otázkám, na které chceme znát odpověď, dostat. V tomto bodě musí být člověk opatrný, nesmí dojít k podezření ze strany pracovníka, že se z něho snažíme vydolovat senzitivní informace.

Dalším bodem je dorovnání se na jazykovou úroveň tázaného. Je důležité si po reakci na první odpověď bezpečnostního pracovníka všimnout, jakým jazykem mluví – spisovným, nespisovným a snažit se přizpůsobit. Není to podmínkou, ale z praxe bylo vypozorováno, že je větší šance člověka rozpovídat, pokud mluvíme stejným jazykem jako on. Například přizpůsobení otázky, místo „Chtěl bych pracovat jako bezpečnostní pracovník" je možné použít také „Chtěl bych dělat v sekurity.". Nebo místo „Nabíráte u vás?" může být použito „Berete?" apod. Podstatným bodem v této části je tykání a vykání. Je důležité rozpoznat, kdy vykat a kdy tykat. Pokud se jednalo o konverzaci dvou mladých lidí, bylo by divné, kdyby tazatel začal vykat. Kdyby na druhou stranu byl dotazovaný starší, je důležité, abychom vykali, jelikož starší generace si potrpí na úctu ke staršímu.

Stejně jako výše zmíněné body, které jsou nejdůležitější, je také důležité projevovat emoce při komunikaci s bezpečnostním pracovníkem. Tyto emoce nemusejí být nijak silné, ale měly by přitakávat pocitům a projevu mluvícího. Jedná se například o to, když si pracovník stěžuje na podmínky, které musí v rámci své pracovní náplně vykonávat. Měli bychom ho v tom podpořit v rámci utužení vztahu a tomu, aby nám víc věřil a byl ochotný sdělit více informací. Tento postup se v praxi potvrdil.

Není ostudou také ukázat jistou známku pokory. Tím můžeme v pracovníkovi vzbudit pocit toho, že dělá práci, na kterou nemáme, anebo práci, které si vážíme, či dokonce obdivujeme. Tento případ neplatí pro všechny rozhovory. Celý proces je hodně o improvizaci. Stejně jako v předchozím případě, musíme poznat, s kým máme tu čest a přizpůsobit tomu tak celou následující konverzaci. Člověku, kterého jsme nezaujali, bude hrát do karet to, když mu řekneme např. „Musí být těžké makat jako bezpečák, nevím, jestli to zvládnu". V tomto případě by jednoduše odvětil „Tak to nedělej" a rozhovor je v podstatě u konce. V některých případech nám tak pokora může pomoct a v některých nikoli.

6.5.2 Typy lidí

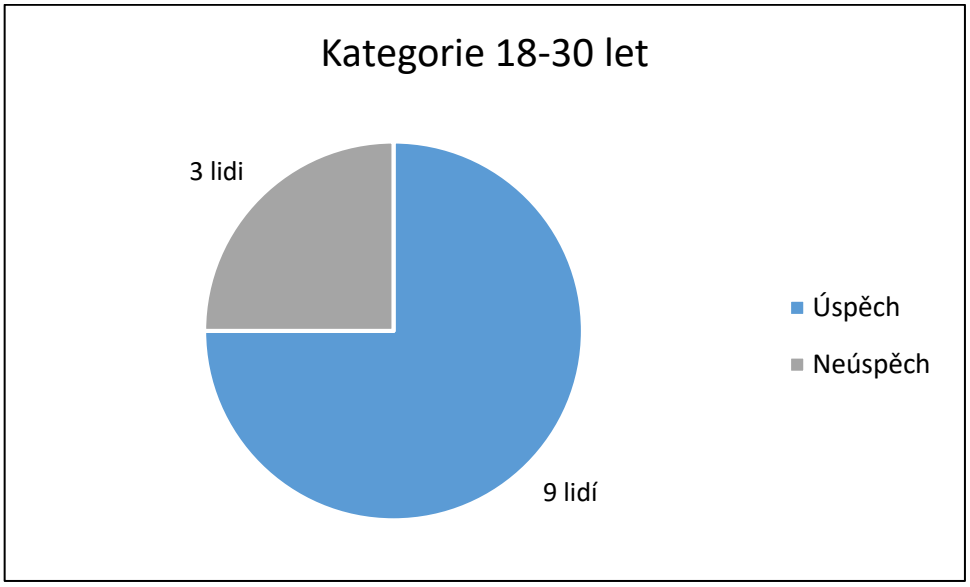
V průběhu sběru dat, kdy bylo vytěžováno mnoho osob, se dají tyto osoby zařadit odhadem do věkových kategorií. Jsou to kategorie lidí, kteří se pohybují v oblasti průmyslu komerční bezpečnosti, a to konkrétně jako bezpečnostní pracovníci na určeném místě (obchod, obchodní centrum, parkoviště). Díky prvotně získaným zkušenostem, které byly získány při vypracovávání social engineering card, bylo možné v pozdější fázi testování odhadnout, jak budou lidé zhruba reagovat a zda bude řízený rozhovor úspěšný.

Všechny kategorie by se potom dále daly rozdělit na další skupiny, které jsou již v rámci této práce nepodstatné, jelikož dat není mnoho. Jsou to lidé, kteří jsou přesvědčeni o tom, co dělají a jen těžko se dají z těchto lidí získat nějaké informace. Jsou to lidé zapálení pro své povolání a dá se říct, že jsou svým způsobem paranoidní. Paranoidní ve smyslu, že celý den hlídají a sledují lidi, zda něco neukradli. Pozorují lidi, kteří se zdají být podezřelí a sledují jejich chování tak, aby eliminovali potenciální hrozbu. Díky této vlastnosti je kdokoli, koho neznají, v podstatě podezřelý, tím pádem si drží odstup.

Díky těmto získaným zkušenostem můžeme tedy rozdělit lidi do následujících věkových kategorii.

6.5.2.1 Lidé 18–30 let

Předpokladem úspěchu u lidí v této věkové kategorii je fakt, že autor patří do stejné věkové kategorie, tudíž bylo jednodušší navázat kontakt s těmito lidmi. Důležité je získat důvěru. U většiny dotázaných byla použita forma tykání. Většina dotázaných lidí z této věkové kategorie byli ochotní ke konverzaci.



Graf 2. Úspěšnost kategorie 18–30 let

Tab. 2. Shrnutí kategorie 18–30 let

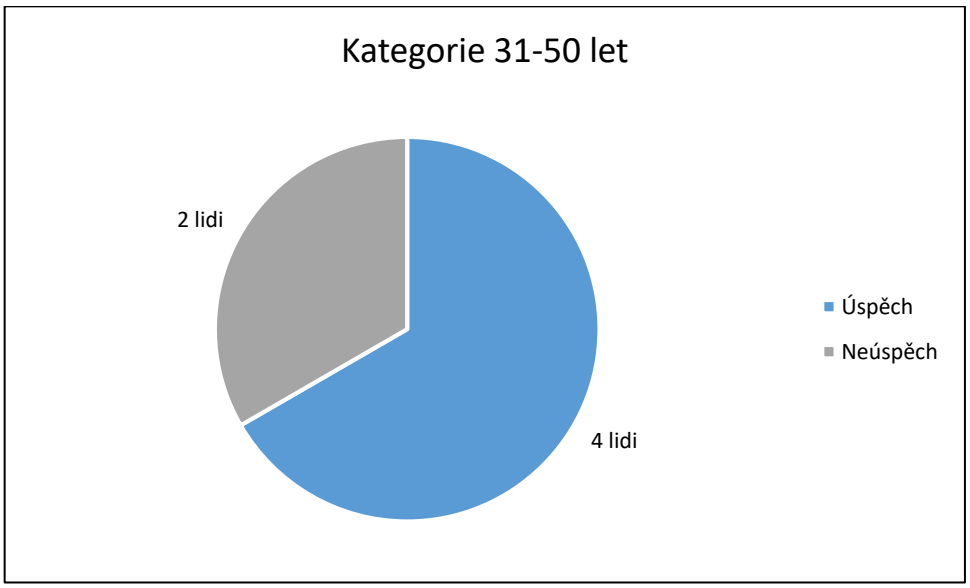
Kategorie	Úspěch	Neúspěch	Úspěšnost
18-30	9	3	75 %

V rámci této kategorie byla vysoká úspěšnost – 75 %. Je to nejspíš z výše zmíněného důvodu a to toho, že tazatel je ve stejné kategorii.

6.5.2.2 Lidé 31–50 let

Co se týče kategorie lidí 31–50, tak v této kategorii se nejvíce pohybují lidé, kteří jsou oddaní svému zaměstnání ve smyslu, že si dávají velký pozor na to, co řeknou.

V porovnání s předchozí kategorií je složitější z těchto lidí dostat nějaké informace. Vzhledem k věkové kategorii autora práce může dojít ke snížení pravděpodobnosti úspěchu. I přesto, že byla tato kategorie nejobtížnější, tak úspěšnost byla velká – v rámci počtu oslovených lidí a obtížnosti.



Graf 3. Úspěšnost kategorie 31–50 let

Neúspěchy, které jsou znázorněny v grafu výše, byly v obou případech u lidí, kteří jsou svým způsobem „paranoidní“. Striktně dodržují pravidla a soustředí se pouze na pracovní náplň a nenechají se ničím rozptýlit.

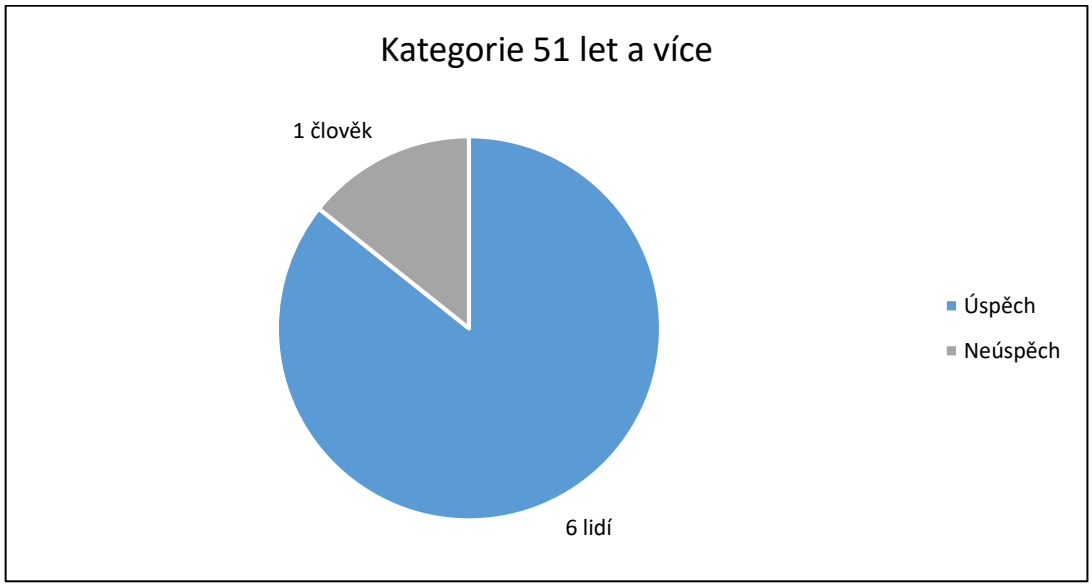
Tab. 3. Shrnutí kategorie 31–50 let

Kategorie	Úspěch	Neúspěch	Úspěšnost
31-50	4	2	66 %

6.5.2.3 Lidé 51 let a více

Co se týče lidí této kategorie, dá se říct, že bylo nejjednodušší dostat se k senzitivním informacím právě u nich. Výhodou zde byl věk autora práce.

Stačilo projevit určitou míru pokory, díky tomu se lidé v této věkové kategorii k autorovi chovali spíše jako k vlastnímu dítěti a rozpovídali se tak o nepříjemných i příjemných údělech této práce. Díky tomu protřídění těchto informací vedlo k získání informací, které nemají povoleno sdílet s ostatními lidmi.



Graf 4. Úspěšnost kategorie 51 let a více

Obecně starší lidé více mluví a snaží se být přátelští, může to být způsobeno tím, že mají před důchodem nebo si chtějí jenom ukrátit dlouhou chvíli od svých pracovních povinností. Důležité je také u této věkové kategorie projevit známku pokory. Díky tomu stoupneme v ceně. Lidé v této věkové kategorii si tak mohou myslet, že si jejich práce vážíme.

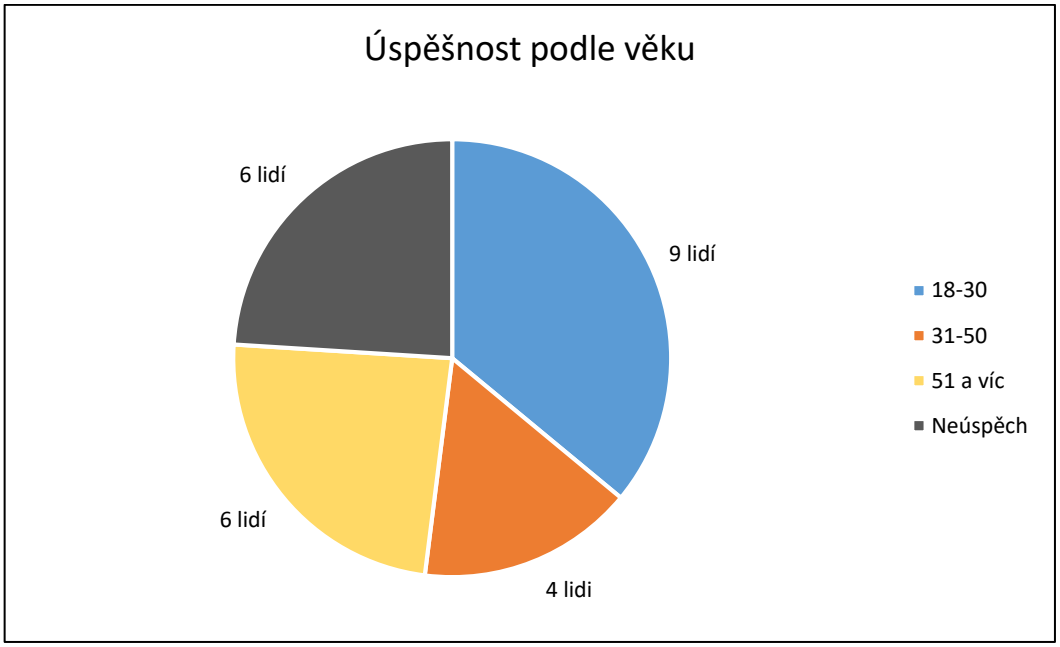
Tab. 4. Shrnutí kategorie 51 let a více

Kategorie	Úspěch	Neúspěch	Úspěšnost
51 a více	6	1	85 %

6.5.3 Shrnutí

Celkově byla tato experimentální metoda použita na 25 lidech. Z celkového počtu 25 oslovených lidí bylo pouze 6 pokusů neúspěšných, což tvoří 24 % z celkového počtu. V rámci neúspěšných pokusů šlo o chybu autora, které vedly k dřívějšímu ukončení rozhovoru. Nebo se jednalo o typ výše zmiňovaných lidí, kteří jsou paranoidní, a tak nevěří nikomu.

Věkové kategorie hrají důležitou roli v souvislosti s věkem tázající se osoby. Spolu s tím jsou také důležité verbální zkušenosti a velká míra improvizace.



Graf 5. Shrnutí všech lidí

Obecně se dá z těchto výsledku usoudit, že nejvyšší úspěšnost byla v kategorii 51 let a více – tedy 85 %. V této kategorii bylo nejjednodušší navázat kontakt, většina lidí z této kategorie byla vstřícná a komunikativní. Co se týče ostatních kategorii, nejhůře dopadla kategorie 31–50 let. Může to být způsobeno tím, že nebylo možné získat více vzorků z této věkové kategorie. Zároveň však u lidí z této kategorie, u kterých nebyl tento experiment úspěšný, bylo zaznamenáno paranoidní chování a sami tito lidé v určitém momentu stopli konverzaci a nechtěli dále komunikovat.

Tab. 5. Shrnutí všech lidí

Kategorie	Lidi	Podíl
18-30	9	36 %
31-50	4	16 %
51 a víc	6	24 %
Neúspěch	6	24 %
Celkem	25	100 %

Social engineering card je systém testování zaměstnanců bezpečnostních firem. Cílem je získání senzitivních informací, které by mohly poškodit zájmy firmy nebo osob, kterých se to týká. Jedná se například o informace ohledně slepých míst kamer, výši výdělku nebo typologii potencionálních pachatelů.

Celé testování proběhlo na 25 zaměstnancích různých bezpečnostních firem. Z toho 6 testů se nepovedlo. Bylo to způsobeno buď chybami na straně tazatele, nebo neochotou ze strany bezpečnostních pracovníků. Návrh karet, které byly použity v praxi v rámci cíleného rozhovoru, bylo náročné. Před tím, než byl test započat, bylo nutné si vyzkoušet na nečisto, jestli jsou tyto otázky vhodně poskládány. Výsledkem této fáze bylo upravení karet do finální podoby, která byla použita v ostrém testování.

Social engineering card bylo rozděleno na více částí – kategorií. První kategorii je navázání kontaktu, kde je potřeba si bezpečnostního pracovníka proklepnout a zjistit jeho jazykovou úroveň a přizpůsobit se. V následujících dvou kategoriích jsou otázky, které jsou směřovány k získání senzitivních informací – informací, které by neměly být sděleny veřejnosti. Poslední kategorie jsou doplňující otázky, které mohou a nemusí být položeny, záleží na situaci, ve které se tazatel nachází.

V rámci této kapitoly byly také zpracovány obecné tipy pro komunikaci s lidmi, pokud chceme vytěžovat informace. Jsou to tipy, které jsou založené na osobních zkušenostech autora z průběhu využívání social engineering card v praxi. Nejdůležitější je, jak se říká „prolomit ledy“, a tím odbourat komunikační bariéru jak u tazatele, tak u dotazovaného.

Díky uzpůsobení našeho verbálního projevu můžeme jednodušeji tyto ledy probourat. Všechno je to stavěno na určité míře improvizace a předešlých zkušeností. Nelze tak jednoznačně říci, že se bude rozhovor ubírat jasně daným směrem. Pokaždé bude rozhovor úplně jiný. Dají se však určit jednoduchá pravidla, kterých se člověk v průběhu konverzace může držet. Jsou to zásady jako – naslouchat, dorovnat se na jazykovou úroveň tázaného, prokládat projev vlastními emocemi nebo reakcemi a v neposlední řadě také ukázat známku nedokonalosti a pokory. Většina lidí, na kterých byl proveden tento experiment, se nakonec rozmluvila a člověku tak nezbývá nic jiného než naslouchat. V rámci procesu naslouchání je také důležité vychytat správnou chvíli a popostrčit tak člověka k tématu nebo informaci, kterou chceme, aby nám sdělil.

Zkušenosti, které byly získány v průběhu zpracovávání této práce, umožnily rozčlenit tázané lidi do třech kategorii. Kategorie jsou podle věku a to od 18 do 30 let, od 31 do 50 let a nakonec lidé 51 let a více. Tito lidé byli zařazení do výše zmíněných kategorií na základě odhadu. Největší úspěšnost byla dosažena v poslední kategorii – konkrétně kategorie 51 let a více. Je to s největší pravděpodobností způsobeno tím, že lidé v této kategorii byli více výřeční v porovnání s ostatními kategoriemi. Celkem byl experiment proveden u 25 lidí a

z toho u 6 lidí byl tento experiment neúspěšný. Bylo to způsobeno jak chybou autora, která vedla k odhalení záměru celého rozhovoru, ale také povahou některých dotázaných – nejvíce v kategorii 31–50 let.

7 NÁVRH OPATŘENÍ

Školení bezpečnostních pracovníků má za cíl předejít možnému vytěžování informací, ke kterému může dojít během každodenního pracovního nasazení. Školení je rozděleno do více částí, které jsou různě časově náročné.

7.1 Úvodní část školení

V první části školení jde o seznámení se sociálním inženýrstvím. Školení bude trvat 90 minut a bude se držet následujících bodů:

1) Co to je sociální inženýrství
2) Techniky, které jsou spojené se sociálním inženýrstvím
3) Dělení sociálního inženýrství
4) Využití sociálního inženýrství v průmyslu komerční bezpečnosti

Důležité je seznámit pracovníky, kteří se zúčastní školení, se sociálním inženýrstvím jako takovým, co to sociální inženýrství je, jak se sociální inženýrství dělí a jaké je jeho využití v průmyslu komerční bezpečnosti. Cílem úvodní části školení je dostat sociální inženýrství do povědomí bezpečnostních pracovníků.

7.2 Druhá část školení: Seznámení školitele s prostředím

Druhá část školení je zaměřena na samotného školitele, která se skládá z následujících částí:

1) Obhlídka objektu
2) Zjištění senzitivních informací
3) Podezřelé předměty
4) Nastavení procesů pro reakci

7.2.1 Obhlídka objektu

V rámci obhlídky objektu je důležité zjistit, jaké jsou hrozby daného objektu z pohledu školitele. Podstatnou částí je také seznámit se s režimem daného objektu. Cílem této části je, aby školitel poznal, v jakém prostředí pracovníci bezpečnostní služby pracují, s jakými lidmi se setkávají, jaká je náplň jejich práce atd.

7.2.2 Zjištění senzitivních informací

Důležité je zjistit, s jakými senzitivními informacemi pracovníci pracují a sestavit možné otázky, se kterými se mohou při výkonu povolání setkat. Příkladem mohou být otázky typu:

- Střídáte/střídáš se s někým? Nebo jste/jsi tu sám?
- Máte/máš danou trasu obchůzky?
- Stává se, že by zloděj nebyl zachycen kamerou přímo při krádeži?
- Můžete/můžeš aspoň na cigáro ven?
- Jak to tu chodí?

7.2.3 Podezřelé předměty/podezřelý email

Co se týče podezřelých předmětů a podezřelé elektronické pošty, je důležité zjistit z pohledu školitele jaké mohou být nástrahy daného prostředí. Důležité je, aby zaměstnanci měli dostatečné povědomí o tom, že je možné získat senzitivní informace pomocí sociotechnik. Sociotechniky, které se v praxi využívají, mohou být baiting nebo phishing. U baitingu je důležité nenechat se nachytat odloženými přenosovými médii. Může se jednat o CD nebo USB flash disk. Tyto zařízení mohou být popsané následujícími názvy:

- Výplaty_2018
- Rozpis_dovolené_2018
- Zisk za loňský rok
- Prémie_2018

Při vložení přenosových médii do počítače může dojít k odposlouchávání nebo odesílání senzitivních dat na server pachatele.

Elektronická pošta bývá většinou filtrována příslušnou doménou, u které je samotný email zaregistrovaný. Toto není však pravidlo a sem tam může nějaký phishingový email do schránky přistát. Phishingové emaily bývají většinou špatně napsané nebo jsou podezřelé samotným požadavkem, který se v obsahu zprávy nachází. Je potřeba si dávat pozor na následující požadavky:

- Změna hesla
- Aktualizace stávajícího zabezpečení – potřeba přihlášení
- Zaplacení neznámého poplatku

7.2.4 Nastavení procesů pro reakci

Vytvoření vhodné reakce na dané problémy je klíčové.

Při rozhovoru s jakýmkoli cizím člověkem je důležité si dávat pozor na otázky, které by mohly směřovat k získání senzitivních informací. Tyto otázky se mohou lišit v rámci různých pracovních pozic. Obecně však tyto otázky mají za cíl získat informace, které nejsou dostupné pro veřejnost – pouze pro interní zaměstnance nebo zaměstnance pověřené.

Pokud pracovník zjistí, že se stal obětí vytěžování informací, je důležité tuto situaci nahlásit. Pokud se jedná o phishingový email nebo odložený předmět, tuto situaci nahlásit na ICT oddělení. Pokud se jedná o cílený rozhovor. Může být tato konverzace ukončena následujícími způsoby:

- K čemu ti tato informace bude?
- Proč to potřebuješ vědět?
- Zrovna teď tu někde šéf pobíhá, můžete/můžeš se ho zeptat sám.
- Omlouvám se, musím pokračovat v práci
- Nemůžu se s Vámi/tebou dále bavit.

7.3 Školení pro bezpečnostní pracovníky na pozici strážný

Ve třetí části školení jde o uvědomění bezpečnostního pracovníka, jaké jsou možné hrozby na pracovišti, které jsou spojené se sociálním inženýrstvím. Co jsou to senzitivní informace a jaké jsou rizikové faktory na pracovišti. Školení navazuje na úvodní část, kde byly poskytnuty obecné informace o sociálním inženýrství. Cílem tohoto školení je poskytnout konkrétní informace, s čím se mohou pracovníci setkat u nich v práci a jak na to reagovat. Tato část bude trvat 3 hodiny a je zaměřená na pozici strážný a bude se zabývat následujícími body:

1. Senzitivní informace
2. Otázky, směřující k získání senzitivních informací
3. Jak se bránit proti sociálnímu inženýrství
4. V případě zjištění efektivně ukončit konverzaci

7.3.1 Senzitivní informace

Pro bezpečnostního pracovníka je důležité si uvědomit, jaké jsou senzitivní informace. Pokud bezpečnostní pracovník bude mít povědomí o tom, jaké jsou senzitivní informace, měl

by se tam vyvarovat jejich sdílení s veřejností nebo člověkem, který se s nimi bude při dlouhé chvíli v práci vybavovat. Za senzitivní informace můžeme považovat:

- Slepá místa kamer
- Kdy jsou přestávky a zda se zaměstnanci střídají
- Trasa, kterou zaměstnanec chodí
- Výše výdělku
- Kamery v objektu a jejich zorné pole
- Typologie podezřelých lidí

Všechny tyto informace mohou být využity ve prospěch člověka, který se tyto informace snaží získat.

7.3.2 Otázky, směřující k získání senzitivních informací

Otázky, které mohou směřovat k získání senzitivních informací mohou být různé. Záleží, v jaké prostředí bezpečnostní pracovník působí – tedy jaké informace jsou považovány za senzitivní v daném prostředí. Obecně to mohou být otázky typu:

- Střídáte/střídáš se s někým? Nebo jste/jsi tu sám?
- Máte/máš danou trasu obchůzky?
- Stává se, že by zloděj nebyl zachycen kamerou přímo při krádeži?
- Můžete/můžeš aspoň na cigáro ven?
- Jak to tu chodí?

Otázky se mohou na první pohled zdát jako nedůležité nebo nezajímavé. Ale při položení této otázky ze strany tazatele je důležité zbystřit a dávat si pozor na to, co odpovědět.

7.3.3 Obrana proti vytěžování informací

Pokud je položena jedna z výše uvedených otázek – mohou to být i jiné otázky, které jsou spojené se získáním senzitivních informací daného pracoviště. Je důležité zachovat chladnou hlavu. V situaci, kdy je zjištěno možné vytěžování, jsou dvě možnosti, buď je převzata kontrola nad konverzací se snahou zjistit, proč chce člověk tento typ informací anebo je možné konverzaci ukončit protiotázkami. Možné typy protiotázek:

- Proč je pro vás/tebe důležité toto vědět?
- K čemu ti tato informace?

- Proč to potřebuješ vědět?

Druhou možností je snaha ukončit tuto konverzaci. Možné typy odpovědí/reakcí:

- Pokud chceš u nás dělat, zavolám šéfa.
- Zrovna teď tu někde šéf pobíhá, můžete/můžeš se ho zeptat sám.
- Omlouvám se, musím pokračovat v práci
- Nemůžu se s Vámi/tebou dále bavit.

Školení má za cíl seznámit pracovníky bezpečnostních služeb s tím, co to sociální inženýrství je a jakým způsobem může být sociální inženýrství aplikováno v praxi právě na pracovníky bezpečnostních služeb.

Školení je rozděleno do tři část, každá část je různě časově náročná. Úvodní část je určena pro všechny pracovníky bezpečnostních služeb a trvá 90 minut. Druhá část je zaměřená pro školitele. Z pohledu školitele je důležité si udělat obhlídku místa, kde bezpečnostní pracovníci pracují, vytvořit otázky, se kterými by se mohli v rámci služby setkat. Třetí část je mířená pro bezpečnostní pracovníky na pozici strážný a trvá 3 hodiny. Třetí část obsahuje možné otázky, se kterými se může bezpečnostní pracovník v praxi sekat.

ZÁVĚR

V diplomové práci byly vysvětleny základní pojmy, které jsou spojeny se sociálním inženýrstvím. Byly také popsány nejvyužívanější techniky. Sociální inženýrství není fenomén, který se využívá pouze přes internet, ale je možné ho využít i jako metodu pro vytěžování informací pomocí fyzického kontaktu útočníka s obětí. Tyto techniky jsou obecně popsány, avšak neslouží jako návod. Pro úspěšné použití těchto technik je třeba improvizace přímo na místě, kde je tato technika použita.

V teoretické části byla mimo jiné shrnuta neverbální komunikace a její praktické využití. Tento fenomén je využíván každodenně všemi lidmi. Projevy neverbální komunikace jsou řazeny do kategorií a pracuje se s pojmy, jako jsou ilustrátory nebo adaptory. Důležitou částí jsou také emoce a jejich charakteristika. Emoce hrají klíčovou roli při pochopení vnitřních pocitů člověka a zároveň korektní identifikací momentálního rozpoložení člověka můžeme vést verbální komunikaci příslušným směrem. Dalším přínosem teoretické části je legislativa, která se opírá o sociální inženýrství. V dnešní době neexistuje legislativa, která by vymezovala sociální inženýrství jako takové. Proto byla potřeba analýza současné legislativy a vytáhnout nejdůležitější zákony, které se o tuto problematiku opírají.

V praktické části diplomové práce je navrhnut systém testování zaměstnanců. Testování zaměstnanců je rozděleno do dvou částí. První část je technicky zaměřená, jedná se o phishingový email a sociotechniku baiting, která by byla realizována pomocí USB flash disku. V obou případech byly vytvořeny EPC diagramy, které popisují postup průběhu testování jednotlivých typů testů. Oba návrhy byly představeny vysoce postavenému manažerovi bezpečností firmy XY. Tyto návrhy se setkaly s úspěchem, bohužel nebyl čas pro realizaci kvůli internímu schvalovacímu procesu.

V další části praktické části byl představen systém testování pomocí social engineering card. Cílem je získání senzitivních informací, které by mohly vést k použití těchto informací ve prospěch tazatele. Celé testování proběhlo na 25 zaměstnancích různých bezpečnostních firem. Z toho 6 testů se nepovedlo. Použití social engineering card bylo rozděleno na více fází. První fáze je navázání kontaktu, kde je potřeba si bezpečnostního pracovníka proklepnout a zjistit jeho jazykovou úroveň a přizpůsobit se. V následujících dvou krocích jsou otázky, které jsou směřovány k získání senzitivních informací – informací, které by neměly být sděleny veřejnosti. Poslední kategorie jsou doplňující otázky, které mohou a nemusí být položeny, záleží na situaci, ve které se tazatel nachází.

Následuje kapitola, kde byly zpracovány obecné tipy pro komunikaci s lidmi. Jsou to tipy, které jsou založené na osobních zkušenostech z průběhu využívání social engineering card v praxi. Nejdůležitější je, jak se říká „prolomit ledy“ a tím odbourat komunikační bariéru, jak u tazatele, tak u tázajícího. Díky uzpůsobení našeho verbálního projevu můžeme jednodušeji tyto ledy probourat. Všechno je to stavěno na určité míře improvizace a předešlých zkušeností. Nelze tak jednoznačně říci, že se bude rozhovor ubírat jasně daným směrem. Dají se však určit jednoduchá pravidla, kterých se člověk v průběhu konverzace může držet. Jsou to zásady jako – naslouchat, dorovnat se na jazykovou úroveň tázaného, prokládat projev vlastními emocemi nebo reakcemi a v neposlední řadě také ukázat známku nedokonalosti a pokory. Většina lidí, na kterých byl proveden tento test, se nakonec rozmluvila a člověku tak nezbývá nic jiného než naslouchat.

V poslední kapitole byl představen návrh školení zaměstnanců. Školení má za cíl seznámit pracovníky bezpečnostních služeb s tím, co to sociální inženýrství je a jakým způsobem může být sociální inženýrství aplikováno v praxi právě na pracovníky bezpečnostních služeb. Školení je rozděleno do tři část, každá část je různě časově náročná. Úvodní část je určena pro všechny pracovníky bezpečnostních služeb a trvá 90 minut. Druhá část je zaměřená pro školitele. Z pohledu školitele je důležité si udělat obhlídku místa, kde bezpečnostní pracovníci pracují, vytvořit otázky, se kterými by se mohli v rámci služby setkat. Třetí část je mířená pro bezpečnostní pracovníky na pozici strážný a trvá 3 hodiny. Třetí část obsahuje možné otázky, se kterými se může bezpečnostní pracovník v praxi sekat.

SEZNAM POUŽITÉ LITERATURY

[1] What is Social Engineering? In: WEBROOT [online]. [cit. 2018-03-13]. Dostupné z: http://www.webroot.com/hk/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

[2] GOODCHILD, Joan. Social engineering techniques: 4 ways criminal outsiders get inside. CSO Online [online]., 3 [cit. 2018-03-13]. Dostupné z: https://www.csoonline.com/article/2125205/social-engineering/social-engineering-techniques--4-ways-criminal-outsiders-get-inside.html

[3] ROUSE, Margaret. Social engineering. SearchSecurity [online]., 2 [cit. 2018-03-13]. Dostupné z: http://searchsecurity.techtarget.com/definition/social-engineering

[4] GOODCHILD, Joan. History's infamous social engineers. Networkworld [online]. [cit. 2018-03-13] Dostupné z: https://www.networkworld.com/article/2287427/network-security/history-s-infamous-social-engineers.html#slide5

[5] Citlivé informace. KTD – Česká terminologická databáze knihovnictví a informační vědy [online]. [cit. 2018-05-17]. Dostupné z: 000000388.htm

[6] ZPRAVODAJSKÝ VÝKLADOVÝ SLOVNÍK – sjednocená verze – Agentura EXANPRO. Odborná způsobilost, nezávislost, nezaujatost [online]. [cit. 2018-05–17]. Dostupné z: http://www.exanpro.cz/odborne-slovniky/79-zpravodajskyvykladovy-slovnik-.

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

[8] POLÁŠEK, Adam. Sociální inženýrství v průmyslu komerční bezpečnosti [online]. Zlín, 2016 [cit. 2018-05-17]. Dostupné z: http://digilib.k.utb.cz/handle/10563/38609. Bakalářská práce. Univerzita Tomáše Bati.

[9] WHITAKER, Andrew. Top 10 Social Engineering Tactics. InformIT [online]., 10 [cit. 2018-03-13]. Dostupné z: http://www.informit.com/articles/article.aspx?p=1350956&seqNum=8

[10] DAVEK. Pretexing Like a Boss. In: TrustedSec [online]. 2014 [cit. 2018-03-13]. Dostupné z: https://www.trustedsec.com/march-2014/pretexting-like-boss/

[11] MIJARES, Alejandro. Social engineering: Employees could be your weakest link [online]., 2 [cit. 2018-03-13]. Dostupné z: http://www.computerworld.com/ar-

ticle/2996606/cybercrime-hacking/social-engineering-employees-could-be-your-weakest-link.html

[12] CRYSSMAN. Ukázka typického phishing e-mailu s vysvětlením. Wikipedia [on-line]. [cit. 2018-03-13]. Dostupné z: https://cs.wikipedia.org/w/in-dex.php?title=Phishing&oldid=13356873#/media/File:Jak_snadno_poznat_phishing.png

[13] MCDOWELL, Mindi. Avoiding Social Engineering and Phishing Attacks. In: US-CERT [online]. [cit. 2018-03-13]. Dostupné z: https://www.us-cert.gov/ncas/tips/ST04-014

[14] Social Engineering: Would You Take the Bait? In: Dara Security [online]. [cit. 2018-03-13]. Dostupné z: https://www.darasecurity.com/article.php?id=32

[15] Social Engineering: What is baiting? In: Blog Mailfence [online]. [cit. 2018-03-13]. Dostupné z: https://blog.mailfence.com/2015/11/18/what-is-baiting-in-social-engineering/

[16] KEYWORTH, Marie. Vishing and smishing: The rise of social engineering fraud. BBC News [online]., 6 [cit. 2018-03-13]. Dostupné z: http://www.bbc.com/news/business-35201188

[17] BRISSON, David. 5 Social Engineering Attacks to Watch Out For. In: TripWire [online]. [cit. 2018-03-13]. Dostupné z: http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

[18] CHARLEY, Craig. Management the Steve Jobs way – Learning from Steve Jobs' Management Style. In: Silicon Beach Training [online]. [cit. 2018-03-13]. Dostupné z: https://www.siliconbeachtraining.co.uk/blog/steve-jobs-management-style

[19] LONG, Johnny a Kevin MITNICK. No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. 1. Rockland: Syngress, 2008, 384 s. ISBN 978-1597492157

[20] SANDINEJS. Newton Security TDAR mantrap with piggybacking detected. In: Youtube [online]. [cit. 2018-03-13]. Dostupné z: https://www.youtube.com/watch?v=CS3ufPRkXuk

[21] EKMAN, Paul. Odhalené emoce. Jan Melvil Publishing, 2015. ISBN 9788087270813.

[22] MITCK, Kevin a William SIMON. Umění klamu. HELION, 2003. ISBN 83-7361-210-6.

[23] NAVARRO, Joe a Marvin KARLINS. Jak prokouknout druhé lidi: Příručka býva-lého experta FBI. Grada, 2010. ISBN 978-80-247-3350-0.

[24] Neverbální komunikace [online]. [cit. 2018-05-02]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=45110

[25] CIALDINI, B. Robert. Zbraně vlivu. Jan Melvil Publishing, 2012. ISBN 978-80-87270-32-5.

[26] DOMINGUEZ, Romi. Part 1 Symbols: The "OK" sign [online]. [cit. 2018-03-13]. Dostupné z: http://minagirl78.blogspot.cz/2016/04/part-1-symbols-ok-sign.html

[27] BARROW, Johnny. 14 Body Language Rules You Need To Know Before The In-terview. Rate My Job [online]. [cit. 2018-03-13]. Dostupné z: https://www.ratemyjob.com/career/36261/14-body-language-rules-you-need-to-know-before-the-interview

[28] B, Jessica. Week Five – Face of depression. Rate My Job [online]. [cit. 2018-03-13]. Dostupné z: https://www.flickr.com/photos/jessia-hime/3038466793

[29] ARBAOUI, Larbi. The concept of Hshuma (shame) in Moroccan society [online]. [cit. 2018-03-13]. Dostupné z: http://www.moroccoworldnews.com/2013/09/104788/the-concept-of-hshuma-shame-in-moroccan-society/

[30] HADNAGY, Christopher. Social engineering: The Art of Human Hacking. Indianapolis: Wiley Publishing, 2011, 408 s. ISBN 978-0-470-63953-5.

[31] EKMAN, Paul. Emoce pod maskou. BIZBOOKS, 2015. ISBN 9788026504221

[32] Zákon č. 40/2009 Sb. ve znění pozdějších změn a novel (trestní zákon)

[33] Zákon č. 89/2012 Sb. ve znění pozdějších změn a novel (Zákon občanský zákoník)

[34] Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

EPC Event-process-chain

USB Universal serial bus

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM TABULEK