

Sociální inženýrství jako nástroj pro testování bezpečnosti PC systémů

Social Engineering as a Tool for Testing Computer Systems
Security

Bc. Peter Bubelíny

Diplomová práce
2012



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Peter BUBELÍNÝ**
Osobní číslo: **A10894**
Studijní program: **N 3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Sociální inženýrství jako nástroj pro testování bezpečnosti PC systémů**

Zásady pro vypracování:

1. Vypracujte rešerši technik a prostředků, které jsou používány v oblasti sociálního inženýrství.
2. Navrhněte metodiky pro ochranu před těmito útoky.
3. Vypracujte metodiku pro identifikaci možných slabín PC systémů a jejich zneužití pomocí sociálního inženýrství.
4. Provedte testy modelových situací.
5. Sestavte postupy pro identifikaci potenciálních útoků a pro prevenci před takovými útoky.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BARCELÓ, Marta a Pete HERZOG. ISECOM. The Open Source Security Testing Methodology Manual [online]. 3. vydanie. 2010, 211 s. [cit. 2012-01-18]. Dostupné z: <http://www.isecom.org/mirror/OSSTMM.3.pdf>**
2. **BASKIN, Brian, Kent NABORS a Jayson E. STREET. Dissecting the Hack: The F0rb1dd3n Network. Boston: Syngress Publishing, 2010, 360 s. ISBN 978-1-59749-478-6.**
3. **HADNAGY, Christopher. Social engineering: The Art of Human Hacking. Indianapolis: Wiley Publishing, 2011, 408 s. ISBN 978-0-470-63953-5.**
4. **LONG, Johnny, Kevin D. MITNICK, Scott PINZON a Jack WILES. No Tech Hacking: A guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Burlington: Syngress Publishing, 2008, 384 s. ISBN 978-1-59749-215-7.**
5. **MITNICK, Kevin D. a William L. SIMON. The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley Publishing, 2003, 368 s. ISBN 0-7645-4280-X.**

Vedoucí diplomové práce:

Ing. David Malaník

Ústav informatiky a umělé inteligence

Datum zadání diplomové práce:

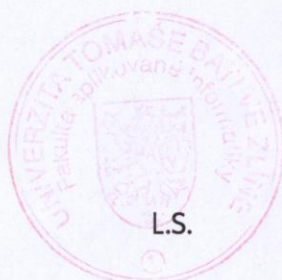
24. února 2012

Termín odevzdání diplomové práce:

15. května 2012

Ve Zlíně dne 24. února 2012

prof. Ing. Vladimír Vašek, CSc.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práca si klade za cieľ preštudovať a zdokumentovať problematiku sociálneho inžinierstva ako nástroja prostredníctvom ktorého testovať a zvyšovať informačnú bezpečnosť. V práci je spracovaný prehľad netechnických a technických metód, ktoré sú používané pri útokoch sociálnym inžinierstvom a taktiež sú spomenuté nástroje, ktoré sociálni inžinieri používajú. Práca ďalej ponúka návrh opatrení ako sa brániť pred netechnickými a technickými útokmi. Ďalšia časť práce prezentuje postupy pomocou ktorých identifikovať možné bezpečnostné slabiny a zraniteľnosti a to formou testov sociálnym inžinierstvom. Ďalej sú prezentované výsledky z testov modelových situácií, pričom návrh práve týchto testov, ktoré odrážajú skutočnú potrebu ich realizácie, sa opiera o vyjadrenia oslovených bezpečnostných odborníkov v oblasti sociálneho inžinierstva. Na záver práce sú poskytnuté návrhy bezpečnostných opatrení zamerané na identifikáciu, prevenciu a ochranu pred útokmi sociálnym inžinierstvom.

Kľúčové slová: sociálne inžinierstvo, sociálny inžinier, sociotechnik, útok, penetračný test, informačná bezpečnosť, bezpečnostná politika, fyzický prienik, prenosné médium, tvorba scenárov, riziko, zraniteľnosť, prevencia, piggybacking, phishing, pharming, Caller-ID/SMS spoofing, road apples, FOCA, Maltego

ABSTRACT

The master thesis aims to study and document the social engineering as a tool by which can test and improve information security. The thesis presents overview of the non-technical and technical methods that are used for social engineering attacks, and also tools used by social engineers. The master thesis also offers draft of the measures how to defend against non-technical and technical attacks. The next part presents the procedures by which help to identify a potential security weaknesses and vulnerabilities with the social engineering tests. Next are presents the results of model situations tests, which proposal of these tests reflect the actual need for their realization. The proposal these tests is based on the opinions of the security experts at social engineering field. Finally, are offered proposals of security policies to identify, prevent and protect against social engineering attacks.

Keywords: social engineering, social engineer, attack, penetration test, information security, security policy, physical penetration, pendrive, creating scenarios, risk, vulnerability, prevention, piggybacking, phishing, pharming, Caller-ID/SMS spoofing, road apples, FOCA, Maltego

Bc. BUBELÍNY P. *Sociální inženýrství jako nástroj pro testování bezpečnosti PC systémů.*
Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2012. 100 s. Vedoucí
diplomové práce Ing. David Malaník, Ph.D.

POĎAKOVANIE

Ďakujem svojmu konzultantovi Ing. Davidovi Malaníkovi, Ph.D. za jeho vecné pripomienky a odporúčania pri písaní diplomovej práce a taktiež svojej snúbenici za jej nesmierne veľkú podporu.

V Zlíně dňa

.....

(Podpis autora)

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

Bruce Schneier

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská 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/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na 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

.....
podpis diplomanta

OBSAH

ÚVOD	11
I TEORETICKÁ ČASŤ	13
1 SOCIÁLNE INŽINIERSTVO	14
1.1 CHARAKTERISTIKA A MOTIVÁCIA SOCIÁLNEHO INŽINIERA	14
1.2 FÁZY SOCIÁLNEHO INŽINIERSTVA	15
1.2.1 Zhromažďovanie informácií.....	16
1.2.2 Budovanie vzťahov a dôvery	17
1.2.3 Využitie dôvery	18
1.2.4 Realizácia a zneužitie	18
2 SPÔSOBY A NÁSTROJE SOCIÁLNEHO INŽINIERSTVA	19
2.1 NETECHNICKÉ SPÔSOBY ÚTOKOV	19
2.1.1 Trashing.....	19
2.1.2 Spying.....	19
2.1.3 Techie Talk.....	20
2.1.4 NLP.....	20
2.1.5 Ten attack	20
2.1.6 Piggybacking	21
2.2 TECHNICKÉ SPÔSOBY ÚTOKOV.....	21
2.2.1 Phishing	21
2.2.2 Pharming.....	22
2.2.3 Caller-ID a SMS spoofing.....	22
2.2.4 Road apples.....	23
2.2.5 Whaling attack.....	23
2.2.6 Mumble attack.....	23
2.2.7 Vishing.....	23
2.2.8 Reverse social engineering	24
2.3 NÁSTROJE POUŽÍVANÉ V SOCIÁLNO M INŽINIERSTVE.....	24
2.3.1 Sociálne a internetové média.....	24
2.3.2 SHODAN	24
2.3.3 Creepy.....	25
2.3.4 FOCA.....	25
2.3.5 Maltego.....	26
2.3.6 Social-Engineer Toolkit	26
2.3.7 Common User Password Profiler	28
2.3.8 Caller-ID/SMS Spoof.....	28
2.3.9 USB Rubber ducky.....	28
2.3.10 Portable Wi-Fi Node.....	28
2.3.11 Mini kamera	29
2.3.12 Keylogger.....	29
II PRAKTICKÁ ČASŤ	30
3 OCHRANA PRED ÚTOKMI SOCIÁLNYM INŽINIERSTVOM	31

3.1	NÁVRH OPATRENÍ PROTI NETECHNICKÝM ÚTOKOM	32
3.2	NÁVRH OPATRENÍ PROTI TECHNICKÝM ÚTOKOM.....	34
4	IDENTIFIKÁCIA SLABÍN ZABEZPEČENIA PROSTREDNÍCTVOM TESTOV SOCIÁLNYM INŽINIERSTVOM	38
4.1	SPÔSOBY REALIZÁCIE TESTOV	38
4.2	METODIKA TVORBY TESTOV A ICH REALIZÁCIA	40
4.2.1	Identifikácia cieľov.....	42
4.2.2	Preskúmanie	42
4.2.3	Tvorba predstieraných scenárov.....	43
4.2.4	Vykonanie samotného útoku	44
4.3	SPRACOVANIE VÝSLEDKOV VYKONANÝCH TESTOV	44
4.4	OBMEDZUJÚCE FAKTORY TESTOV	45
5	TESTY MODELOVÝCH SITUÁCIÍ.....	47
5.1	SCENÁR Č. 1 – ROZPOSIELANIE PHISHINGOVÝCH EMAILOV	47
5.2	SCENÁR Č. 2 – ZÍSKANIE CITLIVÝCH A DÔVERNÝCH INFORMÁCIÍ.....	49
5.3	SCENÁR Č. 3 – BEZPEČNOSTNÉ SPRÁVANIE SA ZAMESTNANCOV PRI NÁJDENÍ PRENOSNÉHO MÉDIA.....	52
5.4	SCENÁR Č. 4 – PREVERENIE ZVEREJNENÝCH INFORMÁCIÍ	56
5.5	SCENÁR Č. 5 – TEST FYZICKÉHO PRIENIKU DO ORGANIZÁCIE	60
6	NÁVRH BEZPEČNOSTNEJ POLITIKY PRE IDENTIFIKÁCIU, PREVENCIU A OCHRANU PRED ÚTOKMI SOCIÁLNYM INŽINIERSTVOM.....	63
6.1	IDENTIFIKÁCIA ÚTOKOV	63
6.1.1	Varovné náznaky napadnutia	64
6.1.2	Typické ciele a obeť útokov.....	64
6.2	PREVENCIA	65
6.3	BEZPEČNOSTNÁ POLITIKA	66
6.3.1	Klasifikácia dát.....	67
6.3.2	Pravidlá autentifikácie.....	68
6.3.3	Manažment	70
6.3.4	Ľudské zdroje	71
6.3.5	Informačné a komunikačné technológie	72
6.3.6	Fyzická bezpečnosť	78
6.3.7	Hlásenie bezpečnostných incidentov	79
	ZÁVER.....	81
	ZÁVER V ANGLIČTINE	83
	ZOZNAM POUŽITEJ LITERATÚRY	85
	ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK.....	88
	ZOZNAM OBRÁZKOV	89
	ZOZNAM PRÍLOH	91

ÚVOD

Dnešná moderná doba nám prináša nesmierne veľký a rýchly pokrok technológií a človek je súčasťou informačnej spoločnosti plnej pokroku, v ktorej je samozrejmosťou každodenné používanie informačnej a komunikačnej techniky (IKT). IKT nám uľahčuje život a my sa stávame čoraz viac pohodlnejšími, privyknutými a úplne na ňu spoliehame. Musíme si však uvedomiť, že používanie IKT mnohokrát so sebou prináša aj isté riziká v podobe cielených útokov, ktorých účelom je napríklad získanie informácií s veľkou hodnotou.

Nakoľko je používanie IKT v dnešnej dobe úplnou samozrejmosťou a taktiež aj pripojenie k internetu je k dispozícii takmer úplne všade, rastie neustála potreba zavádzať všetky dostupné formy bezpečnostných technológií a udržiavať ich stále aktuálne. V oblasti informačnej bezpečnosti je potrebné sa zastaviť a zamyslieť nad tým, či skutočne iba technológie určené na ochranu sú tým konečným riešením. Práve v tejto chvíli do popredia vystupujú používatelia, pretože práve tí používajú všetky dostupné technológie a technológie robia vždy len to, čo im človek „prikáže“ a spôsob bezpečného správania sa súčasných používateľov IKT možno charakterizovať nasledovnými slovami, dnešní používatelia používajú technológie zajtrajška, s vedomosťami v oblasti informačnej bezpečnosti včerajška. Vďaka týmto atribútom je v rámci bezpečnosti ľudský faktor najzraniteľnejší, nakoľko za zlyhaním používaných bezpečnostných technológií, je a bude vždy zodpovedný človek.

Sociálne inžinierstvo je zamerané na človeka a jeho bezpečné správanie sa, nakoľko veľká dôvera ľudí môže spôsobovať nemalé problémy, a taktiež na skutočnosti, že ľudia si nie sú vedomí hodnoty informácií, ktoré vlastnia a z tohto dôvodu si často vôbec neuvedomujú, aká dôležitá je potreba ich ochraňovať a dbať na ich bezpečnosť. Techniky útokov sociálnym inžinierstvom možno okrem negatívneho použitia využiť aj na zlepšenie či zvýšenie informačnej bezpečnosti v oblasti zlyhania ľudského faktora, nakoľko do budúcnosti budú všetky veci okolo nás čoraz viac závislé na informáciách a sociálne inžinierstvo bude predstavovať čoraz väčšiu hrozbu pre akékoľvek bezpečnostné systémy.

Cieľom tejto diplomovej práce je navrhnúť opatrenia pred útokmi sociálnym inžinierstvom a navrhnúť postupy ako identifikovať možné bezpečnostné slabiny a potenciálne útoky. Práca je rozdelená na teoretickú a praktickú časť, pričom prvá časť práce je zameraná na teóriu v oblasti sociálneho inžinierstva, opisu techník a prostriedkov používaných v sociálnom inžinierstve. Druhá praktická časť práce je zameraná na spôsoby identifikácie bezpečnostných slabín, ktoré možno využiť pri útokoch sociálnym inžinierstvom,

prostřednictvím testování. Dále je v práci prezentována realizace a výsledky testů modelových situací a sestavení návrhu postupů při identifikaci potenciálních útoků a opatření pro útoky realizované sociálním inženýrstvím.

I. TEORETICKÁ ČASŤ

1 SOCIÁLNE INŽIERSTVO

Sociálne inžinierstvo alebo inak nazývané sociotechnika je spôsob manipulácie ľudí, ktorého cieľom je získať dôverné informácie prípadne prinútiť ľudí k vykonaniu požadovanej činnosti, prostredníctvom ktorej možno potom získať prístup k citlivým a dôverným informáciám.

Sociálne inžinierstvo sú systematicky používané vedomosti ľudského chovania a umenia presvedčať, aby užívateľ či obeť urobil to, čo by za normálnych okolností, pri dodržiavaní všetkých bezpečnostných pravidiel nikdy neurobil. Tým sú samotným ľudským faktorom prelomené technologické a organizačné bezpečnostné opatrenia a je umožnený kybernetický útok. [11]

Kevin Mitnick, v minulosti jeden z najhľadanejších a najväčších hackerov na svete a momentálne vyhľadávaný expert na zabezpečenie počítačových systémov definoval sociálne inžinierstvo ako ovplyvňovanie a presvedčanie ľudí s cieľom oklamať ich tak, aby uverili, že sociotechnik je osoba s totožnosťou, ktorú predstiera a ktorú si vytvoril pre potreby manipulácie. Vďaka tomu je sociálny inžinier schopný využiť ľudí, s ktorými hovorí, prípadne dodatočné technologické prostriedky, aby získal hľadané informácie. [18]

V oblasti informačnej bezpečnosti je sociálne inžinierstvo charakterizované ako netechnická forma prelomenia bezpečnostných postupov, nakoľko takýto útok je založený na schopnosti ovplyvňovania, zavádzania a klamania ľudí. Sociálne inžinierstvo je založené a ťaží z potenciálneho zlyhania ľudského faktora, ktorý je neoddeliteľnou súčasťou informačnej bezpečnosti. Súhrnne je sociálne inžinierstvo technika útoku, pri ktorom sa útočník – sociotechnik snaží využitím psychologických hier, manipulácie, vyhrážok narušiť vnútorné prostredie organizácie či získať citlivé informácie od obeť útoku.

1.1 Charakteristika a motivácia sociálneho inžiniera

Sociálny inžinier, inak nazývaný sociotechnik je hacker, ktorý pri svojich útokoch využíva svoje vedomosti, charizmu, vystupovanie či inteligenciu namiesto iba počítačovej sily. Všeobecne sociálny inžinier využíva prirodzenú tendenciu jednotlivca uveriť alebo nechať sebou manipulovať, teda zlyhanie ľudského faktora, než diery v počítačových systémoch a sieťach. Práve z tohto dôvodu je sociálne inžinierstvo realizovateľné a uskutočniteľné pre útočníkov, ktorí nemajú až také hlboké technické znalosti.

Motivácia sociálneho inžiniera k uskutočneniu útoku sociálnym inžinierstvom môže byť rôzna. Predmetom motivácie, môžu byť napríklad:

- finančný zisk
- osobné záujmy
- vydieranie – tlak z vonkajšieho prostredia
- úmyselné poškodenie
- dokazovanie schopností sebe, či iným
- pomsta

Úroveň znalostí a vedomostí útočníka – sociotechnika určuje aj to, akým spôsobom a na akej úrovni je schopný útok realizovať. Charakter sociálneho inžiniera možno rozdeliť do nasledovných dvoch kategórií: [24]

- sociálny inžinier bez technických a počítačových znalostí
- sociálny inžinier s technickými a počítačovými znalosťami

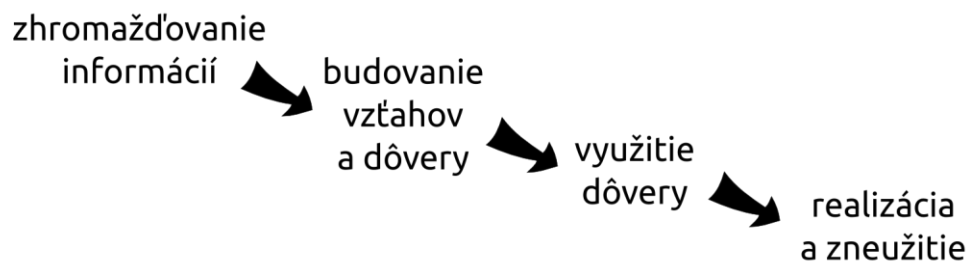
Sociálny inžinier bez technických a počítačových znalostí využíva na získanie dôverných informácií iba svoje osobnostné vlastnosti a schopnosti: charisma, vystupovanie, inteligencia a v neposlednom rade určite schopnosť manipulovať ľuďmi aj pomocou metód vychádzajúcich z neurolingvistického programovania. Na druhú stranu, sociálny inžinier s technickými a počítačovými znalosťami, vie k svojim osobnostným vlastnostiam a schopnostiam pripojiť aj vedomosti a vie pri útoku v maximálnej miere využiť aj dostupné technické prostriedky.

Od týchto kategórií sa odvíjajú aj techniky a spôsoby sociálneho inžinierstva, ktoré sú bližšie popísané v kapitole 2. Spôsoby a nástroje sociálneho inžinierstva.

1.2 Fázy sociálneho inžinierstva

Útok sociálnym inžinierstvom sa skladá zo štyroch nasledovných fáz, ktoré tvoria základ a sú akousi vzorovou schémou pre realizáciu útoku a dosiahnutie stanoveného cieľa:[1, 23]

- zhromažďovanie informácií
- budovanie vzťahov a dôvery
- využitie dôvery
- realizácia a zneužitie



Obrázok 1.1: Fázy sociálneho inžinierstva

1.2.1 Zhromažďovanie informácií

Prvá fáza, zhromažďovanie informácií, je jedna z kľúčových fáz, pretože zhromaždené a získané informácie útočníkovi dokážu poskytnúť potrebný profil a obraz o obeti alebo o organizácii. Predmetom zhromažďovania a získavania môžu byť nasledovné informácie:

- telefónne čísla
- mená a priezviská
- dátumy narodenia
- emailové adresy
- akékoľvek osobné údaje
- usporiadanie organizačnej štruktúry
- pracovné zaradenia či pozície
- vizitky
- informácie o dodávateľoch alebo partneroch

Informácie je možné zhromažďovať rôznymi technikami a metódami. Jednou z najzákladnejších a najjednoduchších metód je prehľadávanie a preskúmavanie voľne prístupných informácií ako sú kontaktné informácie, finančné výsledky, katalógy, články, obsah webových prezentácií či smetných košov. Ďalšími metódami a technikami sú napríklad využívanie automatizovaných „data mining“ nástrojov, akými sú napríklad Maltego alebo FOCA. Problematike nástrojov využívaných pri sociálnom inžinierstve sa venuje kapitola 2.3. Takto všetky získané a zhromaždené informácie možno potom ďalej využiť pri ďalšej fáze.

[17, 26]

1.2.2 Budovanie vzťahov a dôvery

Druhou fázou sociálneho inžinierstva je budovanie vzťahov a dôvery s obeťou alebo obeťami útoku. Sociálny inžinier je na základe získaných znalostí a informácií schopný bez obmedzenia využívať dôverčivosť napadnutého za jediným účelom, ktorým je vytvorenie si vzťahu s ním. Počas rozvíjania vzťahu, je cieľom útočníka si vybudovať dôvernú pozíciu voči napadnutému, ktorú bude neskôr môcť využiť.

Na vytvorenie si čoraz väčšej dôvery môže sociálny inžinier použiť napríklad tieto typické sociotechnické techniky [18]:

- Vydávanie sa za pracovníka tej istej firmy.
- Vydávanie sa za zástupcu dodávateľa, partnerskej firmy alebo štátneho úradu.
- Vydávanie sa za niekoho, kto má moc.
- Vydávanie sa za nového pracovníka, ktorý prosí o pomoc.
- Vydávanie sa za predstaviťa či dodávateľa operačného systému a doporučovanie neodkladnej aktualizácie.
- Ponúknutie pomoci v prípade nejakého problému, vyvolanie tohto problému a ovplyvnenie obeti, aby sama zatelefonovala s prosbou o pomoc.
- Zaslanie bezplatnej aktualizácie programu k inštalácii.
- Zaslanie vírusu alebo trójskeho koňa v prílohe pošty.
- Použitie falošného dialógového okna, zobrazujúceho žiadosť o opakované prihlásenie alebo o zadanie hesla.
- Zaznamenávanie stlačených kláves pomocou špeciálneho programu.
- Podstrčenie prenosných médií s nebezpečnými programami (malware) v okolí pracoviska obeti.
- Používanie vnútropodnikovej terminológie a žargónu s úmyslom vybudovať si dôveru.
- Ponúkание odmeny za registráciu na internetovej stránke, spojenú s vložením užívateľského mena a hesla.
- Podstrčenie dokumentu alebo súboru v podateľni firmy, aby dorazil na určené miesto ako vnútorná pošta.

- Zmena hlavičiek faxu, aby vypadal ako kedy pochádzal zvnútra firmy.
- Žiadosť na recepcnú, aby prijala fax a poslala ho ďalej.
- Žiadosť o prenos súboru na zdanlivo vnútornú adresu.
- Nastavenie hlasovej schránky tak, že je pri spätnom volaní útočník identifikovaný ako osoba zvnútra.
- Vydávanie sa za zamestnanca z inej lokality a žiadosť o dočasne e-mailové konto.

1.2.3 Využitie dôvery

Vo fáze využitie dôvery je už obvykle medzi sociálnym inžinierom a obeťou vytvorená taká dôvera, že obeť dôveruje sociálnemu inžinierovi natoľko, že sa nechá zmanipulovať k správaniu, ktoré priamo vedie k bezpečnostnému zlyhaniu. Takýmto zlyhaním je napríklad prezradenie rôznych citlivých a dôverných informácií (napr. heslo), ktoré sociotechnik potrebuje získať, alebo vykonanie požadovaných úkonov či činností (napr. vytvorenie užívateľského prístupu/konta, vpustenie útočníka do budovy), ktoré by za normálnych okolností neurobil. V priebehu tejto fázy môže sociotechnik obeť zmanipulovať aj tak, že obeť sama poprosí o pomoc. V prípade, že sociálny inžinier počas tejto fázy dosiahne svoj cieľ, môže to znamenať koniec útoku. [26]

1.2.4 Realizácia a zneužitie

Poslednou štvrtou fázou sociálneho inžinierstva je samotná realizácia útoku a zneužitie. Po uskutočnení všetkých predchádzajúcich fáz sociálny inžinier dokončí svoj útok a manipuláciu požiadanimi obeť, aby mu prezradila dôležité, citlivé či dôverné informácie, alebo aby vykonala ním zadané a požadované činnosti pre dosiahnutie požadovaného cieľa. Ak sú získané informácie alebo vykonané činnosti iba medzikrokom a približovaním sa k cieľu, tak sociotechnik opakuje predchádzajúce fázy tak dlho, kým nedosiahne svoj cieľ, inak sa útok touto fázou končí.

2 SPÔSOBY A NÁSTROJE SOCIÁLNEHO INŽINIERSTVA

Pri útokoch sociálnym inžinierstvom môže sociálny inžinier použiť k dosiahnutiu svojho cieľa rôzne techniky a triky. V nasledujúcich kapitolách sú uvedené rôzne viac, či menej používané techniky a spôsoby útokov sociálnym inžinierstvom, ktoré majú buď netechnický, alebo technický charakter. Netechnické techniky nevyužívajú žiadne technické a informačné prostriedky a naopak technické techniky v maximálnej miere využívajú všetky dostupné technické a informačné prostriedky, ktoré sú podrobnejšie opísané v podkapitole 2.3 Nástroje používané v sociálnom inžinierstve.

Všetky techniky, netechnické i technické, je možné vzájomne ľubovoľne kombinovať a sú vždy realizované buď aktívnym sociálnym inžinierstvom, pod ktoré spadá fyzický prienik do organizácie a pohyb v nej alebo fyzický kontakt s obeťou, alebo je to sociálne inžinierstvo realizované prostredníctvom telekomunikačného, mobilného či internetového kanálu.

2.1 Netechnické spôsoby útokov

2.1.1 Trashing

Trashing, alebo inak nazvané „Dumpster diving“ je metóda, pri ktorej útočník prehľadáva smetné koše a z odpadkov vyberá vyhodené spisy, hlavičkové papiere, vizitky, vytlačené emaily, zmluvy, faktúry, telefónny zoznam, poznámky, rozdelenie zamestnaneckej hierarchie a iné dokumenty, prípadne vyhodené optické médium či pevný disk za účelom získať čo najväčšie množstvo informácií o svojej obeti – osobe alebo organizácii.

2.1.2 Spying

Veľmi jednoduchým spôsobom ako zistiť citlivé informácie, je postavenie sa útočníka za obeť a sledovanie hesla ktoré píše na klávesnici. Podobne je ďalej možné odkukať heslo, ktoré má obeť napísané na lístočku, ktorý môže byť nalepený na monitore alebo položený na stole. Tento spôsob útoku sa môže tiež nazývať „Shoulder surfing“. Tak ako je možné sledovať zadávanie hesla na klávesnici, je možné ak to situácia dovoľuje a umožňuje, aby sa útočník dostal do primeranej vzdialenosti, prípadne do prostredia, kde môže počúvať či odpočúvať rozhovory zamestnancov technickej podpory. V prípade, že smernice nejakej organizácie dovoľujú telefonicky prideliť nové či obnoviť zabudnuté heslo užívateľovi, môže sa takto útočník ľahko dostať k heslu.

2.1.3 Techie Talk

Táto metóda predstavuje pre útočníka možnosť zneužiť neznalosť a nedostatok technických znalostí obeť pri komunikácii. Útočník môže voči obeť vystupovať ako servisný technik, ktorý potrebuje odstrániť problém na sieti prípadne na osobnom počítači obeť, ktorá ako technicky málo zdatná bez akýchkoľvek otázok pustí útočníka k svojmu počítaču. Ďalej môže napríklad útočník vystupovať ako zamestnanec podpory (helpdesk), pričom obeť vyzve k tomu, aby si okamžite kvôli bezpečnosti zmenila heslo a zároveň útočník priamo obeť navrhne aké heslo je bezpečné a pomôže jej ho zmeniť, túto „pomoc“ môže realizovať buď telefonicky alebo osobným kontaktom.

2.1.4 NLP

Neurolingvistické programovanie (NLP) je veľmi silný spôsob, akým je možné s ľuďmi manipulovať. Ide o dômyselný a premyslený spôsob používania a výberu slov, ktoré útočník pri komunikácii so svojou obeťou použije. NLP je taktiež založené na tzv. reči tela, prostredníctvom ktorej je schopný útočník vyvolať v obeť pocit falošnej bezpečnosti, súcitu alebo dôveru. Pokiaľ útočník správne skombinuje NLP s osobnostným štýlom a profilom správania sa obeť, je útok s prostredníctvom NLP veľmi úspešný. NLP sa hlavne využíva pri osobnej alebo telefonickej komunikácii a jej realizácia si vyžaduje určitú prax. Túto techniku je vhodné použiť napr. v situáciách, ak útočník vystupuje ako autorita a potrebuje zvýšiť svoju dôveryhodnosť voči obeť, potrebuje vytvoriť pre obeť stresovú situáciu, potrebuje v obeť vytvoriť súcit, presvedčiť ju o pravdivosti predkladaných informácií alebo potrebuje obeť zmanipulovať tak, aby spravila nejaký úkon, ktorý by inak neurobila.

2.1.5 Ten attack

Útok „Ten attack“ spočíva v snahe odpútať pozornosť bezpečnostného personálu od práve prebiehajúceho útoku, napríklad od pokusu druhého útočníka dostať do budovy alebo kancelárie. Spôsobov ako odpútať pozornosť je viacej, napríklad pre rozptýlenie bezpečnostného personálu je vhodné použiť vzhľadovo atraktívnu osobu, alebo falošné upozornenie na nejakú udalosť. Útočník môže taktiež bezpečnostných pracovníkov alebo zamestnancov uviesť do omylu tým, že bude prestierať, že je údržbár, upratovač či umývač okien.

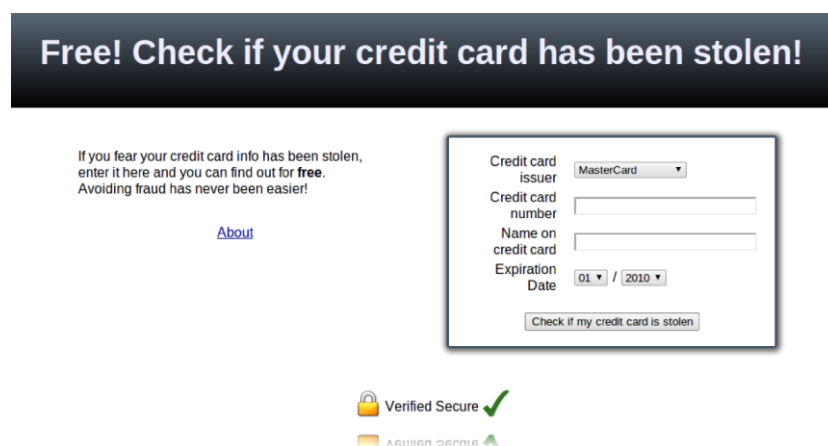
2.1.6 Piggybacking

Jednoduchým spôsobom ako sa môže dostať útočník do budovy organizácie bez overenia je vytvorenie situácie, pri ktorej útočník potrebuje pomôcť s otvorením dverí, pretože nesie veľkú škatuľu a ostatných ľudí alebo zamestnancov poprosí, aby mu podržali dvere. Ďalším spôsobom, ktorý patrí pod túto techniku je nenápadné sa pripojenie útočníka k skupinke fajčiarov, ktorí obvykle používajú zadné alebo bočné vchody, kde sa nevykonávajú vstupné bezpečnostné kontroly. Spolu s touto skupinou, alebo tesne za ňou sa dokáže útočník takto ľahko dostať do budovy bez akéhokoľvek overenia.

2.2 Technické spôsoby útokov

2.2.1 Phishing

Tento spôsob útoku možno považovať za najrozšírenejší a najznámejší. Je charakteristický pokusom útočníka získať od obete osobné alebo iné citlivé informácie, akými sú napríklad číslo a heslo bankového účtu či heslo do emailovej schránky prostredníctvom falošného emailu alebo webovej stránky, ktorá pôsobí na prvý pohľad dôveryhodne, ale v skutočnosti tomu tak nie je. V podvrhnutej – falošnej emailovej správe, môže útočník napríklad obeť vyzvať k tomu, aby si zmenila svoje heslo kliknutím na falošný odkaz, pričom tento odkaz bude nasmerovaný na „dôveryhodnú“ webovú stránku útočníka. Útočník najčastejšie svoju obeť kontaktuje s cieľom finančného obohatenia sa, alebo zneužitia platobných služieb.



Obrázok 2.1: Príklad formy phishingu z osvetovej webovej stránky <http://ismycreditcardstolen.com>, ktorý stavia na ľudskej dôverčivosti

2.2.2 Pharming

Útoku pharming je podobný ako útoku typu phishing, ale rozdiel je v tom, že tento spôsob útoku je sofistikovanejší a nebezpečnejší. Tak ako pri phishingu, aj v tomto prípade je hlavným cieľom útočníka finančné obohatenie, a preto najčastejšími terčami pharmingu sú banky. Hlavná časť tohto útoku spočíva v napadnutí DNS, takým spôsobom, že ak obeť do prehliadača napíše adresu *www.nejakabanka.com*, nedôjde k prekladu na správnu IP adresu, ale na falošnú – podvrhnutú. Takouto zmenou DNS záznamu, by bola obeť presmerovaná na falošnú webovú stránku, ktorú by bolo na prvý pohľad veľmi ťažké rozpoznať od originálnej. Útočník by sa takto dostal k prihlasovacím údajom množstva klientov napadnutej banky.

Pharming je o to nebezpečnejší, že útok sa dá zrealizovať aj lokálne, upravením súboru *hosts*, kde je možné zmeniť alebo pridať riadky s falošnou IP adresou, odpovedajúcou k adrese *www.nejakabanka.com*.

The image shows two terminal windows side-by-side. The left window shows a user named 'beliny' at 'xubuntu-laptop' running a ping command to 'fai.utb.cz'. The output shows successful pings with various response times. The right window shows a user named 'root' at 'xubuntu-laptop' running a ping command to 'google.com', which also succeeds. Then, the user runs 'cat /etc/hosts' showing the default localhost entry. Next, they add a new entry: '173.194.35.161 fai.utb.cz'. Finally, they run 'ping fai.utb.cz' again, and the output shows that the ping now goes to the IP address 173.194.35.161, which is the IP for google.com.

```

beliny@xubuntu-laptop:~$ ping fai.utb.cz -c 4
PING fai.utb.cz (195.178.88.67): 56(84) bytes of data:
64 bytes from fai.utb.cz (195.178.88.67): icmp_req=1 ttl=248 time=25.1 ms
64 bytes from fai.utb.cz (195.178.88.67): icmp_req=2 ttl=248 time=29.4 ms
64 bytes from fai.utb.cz (195.178.88.67): icmp_req=3 ttl=248 time=25.7 ms
64 bytes from fai.utb.cz (195.178.88.67): icmp_req=4 ttl=248 time=26.1 ms

--- fai.utb.cz ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 25.148/26.623/29.460/1.676 ms
beliny@xubuntu-laptop:~$

root@xubuntu-laptop:~/home/beliny# ping google.com -c 3
PING google.com (173.194.35.161) 56(84) bytes of data:
64 bytes from muc03s02-in-f1.1e100.net (173.194.35.161): icmp_req=1 ttl=53 time=40.4 ms
64 bytes from muc03s02-in-f1.1e100.net (173.194.35.161): icmp_req=2 ttl=53 time=39.8 ms
64 bytes from muc03s02-in-f1.1e100.net (173.194.35.161): icmp_req=3 ttl=53 time=39.5 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 39.578/39.948/40.432/0.425 ms
root@xubuntu-laptop:~/home/beliny#
root@xubuntu-laptop:~/home/beliny# cat /etc/hosts
127.0.0.1    localhost

# The following lines are desirable for IPv6 capable hosts
::1        ip6-localhost ip6-loopback
fe00::0    ip6-localnet
ff00::0    ip6-mcastprefix
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters

# FALOSNA IP ADRESA
173.194.35.161 fai.utb.cz

root@xubuntu-laptop:~/home/beliny# ping fai.utb.cz -c 4
PING fai.utb.cz (173.194.35.161) 56(84) bytes of data:
64 bytes from fai.utb.cz (173.194.35.161): icmp_req=1 ttl=53 time=41.4 ms
64 bytes from fai.utb.cz (173.194.35.161): icmp_req=2 ttl=53 time=39.6 ms
64 bytes from fai.utb.cz (173.194.35.161): icmp_req=3 ttl=53 time=40.2 ms
64 bytes from fai.utb.cz (173.194.35.161): icmp_req=4 ttl=53 time=39.9 ms

--- fai.utb.cz ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 39.601/40.320/41.429/0.725 ms
root@xubuntu-laptop:~/home/beliny#

```

Obrázok 2.2: Ukážka úpravy súboru hosts a presmerovanie na falošnú IP adresu

2.2.3 Caller-ID a SMS spoofing

Tento užitočný spôsob umožňuje útočníkovi falšovať telefónne alebo mobilné čísla z ktorých potom uskutočňuje telefónne hovory alebo posiela SMS správy z akýchkoľvek čísel. Preto napríklad, ak obeť obdrží zo sfalšovaného čísla SMS správu, v mobilnom telefóne sa jej bude zobrazovať akoby bola od osoby, ktorej číslo má uložené v kontaktoch.

2.2.4 Road apples

Ťažisko útoku nazvaného „road apples“ spočíva v infikovaní USB kľúča alebo CD/DVD média vírusom, trójskym koňom, malware alebo iným škodlivým kódom, napr. key logger, pomocou ktorého možno získať citlivé údaje, ba dokonca kontrolu nad počítačom obeť. Takto infikované médium potom útočník zanechá na mieste, napr. dvere pred kanceláriou či parkovisko, ktoré je viazané na obeť a je vysoká pravdepodobnosť, že práve obeť nájde toto médium.

2.2.5 Whaling attack

Whaling attack je priamo zameraný na vysokopostavených manažérov, vedúcich zamestnancov alebo osoby ktoré pôsobia na top pracovných postoch. Cieľom je získať a vylákať čo najviac citlivých informácií o danej osobe, prípadne prostredníctvom nej čo najviac citlivých informácií o organizácii. S využitím phishingu, kedy obeť obdrží exkluzívnu pozvánku napríklad na športový turnaj a sú po nej požadované citlivé informácie, ktoré je možné potom neskôr zneužiť. Podobne môže byť obeť prostredníctvom odkazu v emailovej správe presmerovaná na webovú stránku, ktorá pôsobí „dôveryhodne“ a na nej umiestnený formulár do ktorého je potrebné zadať osobné údaje, firemné údaje alebo číslo kreditnej karty.

2.2.6 Mumble attack

Útočník pri telefonickej komunikácii predstiera, že zastupuje osobu (napr. zákazník), ktorá má rečové problémy, pretože sama nedokáže napríklad požiadať o svoje osobné záznamy. V prípade, že obeť útoku, ktorá je schopná takéto informácie podať požiada k telefónu práve osobu s poruchou reči, útočník si je schopný pomocou mechanického zariadenia zdeformovať hlas tak, že potom pôsobí ako osoba s poruchou reči.

2.2.7 Vishing

Tento spôsob útoku je podobný ako phishing, whaling s tým rozdielom, že sa realizuje telefonicky. V praxi útočník využíva automatické vytáčanie čísel, pričom obeť je vždy prehraná zaznamenaná hlasová správa. Obeť môže byť prostredníctvom tejto správy nepravdivo informovaná falošným zamestnancom banky, že sa stala obeťou podvodníkov a jej kreditná karta bola zneužitá. Na to aby obeť vyriešila tento problém je vyzvaná, aby zavolała na telefónne číslo, ktoré reálne patrí útočníkovi, a nadiktovala číslo svojej kreditnej karty, pin,

adresu a rôzne iné citlivé informácie. Tieto citlivé údaje môže obeť nadiktovať aj na prípadný záznamník, ktorý môže útočník opäť využiť.

2.2.8 Reverse social engineering

Táto metóda obsahuje tri základné kroky: sabotáž, reklama a pomoc. Prvým krokom útočník spôsobí sabotážou úmyselnú škodu všetkými možnými dostupnými nástrojmi (napr. napadnutie webovej stránky, počítačovej siete či operačného systému). Potom sa následne snaží pred obeťou čo naj dôveryhodnejšie prezentovať ako odborník a presvedčiť ju, že práve on vie daný problém vyriešiť. Posledný tretí krok znamená poskytnutie pomoci, teda realizáciu – nápravu a odstránenie problému, čo útočník v plnom rozsahu zneužije nakoľko má plný priestor a prístup k sieti, serverom alebo počítačom.

2.3 Nástroje používané v sociálnom inžinierstve

V tejto časti sú opísané základné nástroje, ktoré nesmú chýbať vo výbave každého sociálneho inžiniera. Nástrojov, ktoré možno v sociálnom inžinierstve použiť je podstatne viac, počnúc mechanickými nástrojmi (skrútkovače, kľúče, kliešte a iné), rôznymi pomôckami (falošné ID karty, RFID cloner, laser a iné) až po rôzne softvérové vybavenie, napr. CD médium s live systémom.

2.3.1 Sociálne a internetové médiá

Medzi základné nástroje sociálneho inžiniera patria všetky dostupné internetové zdroje. Výhodou týchto nástrojov je, že útočníka nič nestoja a má ich prakticky úplne kedykoľvek po ruke. Najčastejšie útočník prehliada webové stránky s rôznymi pre útočníka dôležitými informáciami. Ďalej útočník môže využiť sociálne siete akými napríklad sú LinkedIn, Facebook, Twitter alebo Yatedo. Práve vďaka verejným zdrojom má útočník prístup k rôznym zaujímavým informáciám, ktoré ďalej dokáže pri útoku využiť.

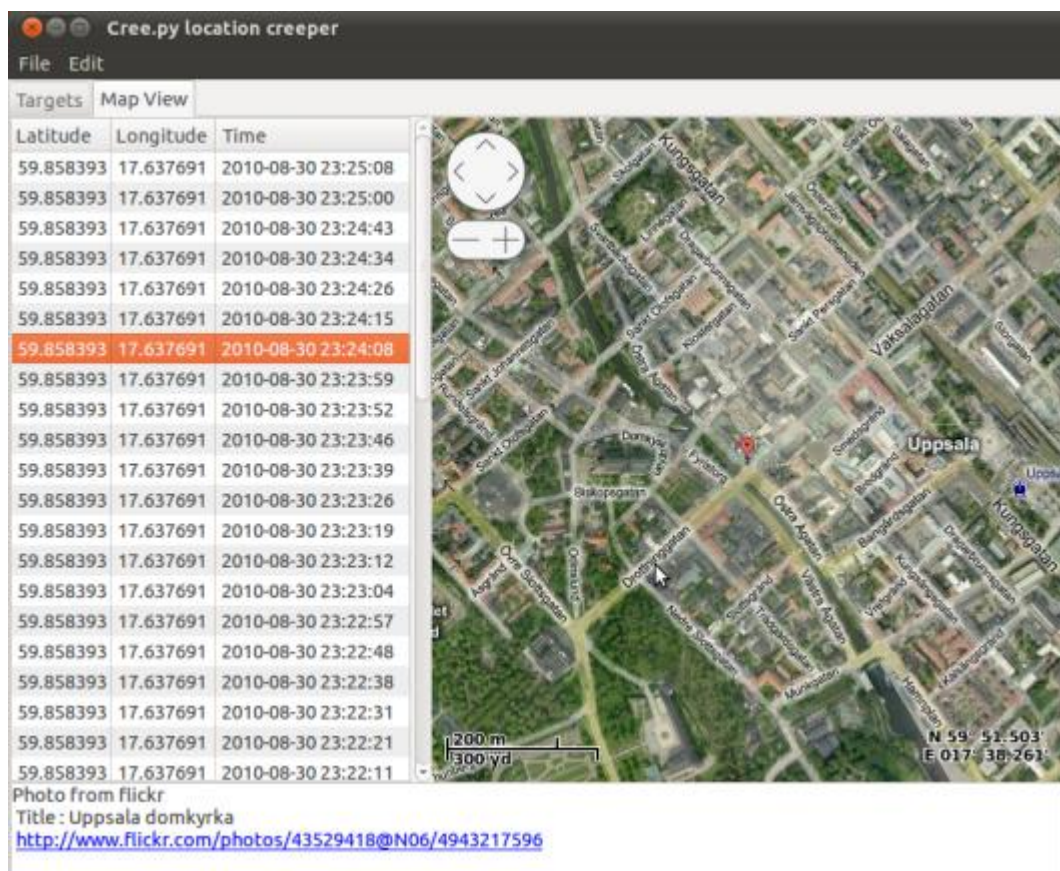
2.3.2 SHODAN

Vyhľadávač SHODAN umožňuje vyhľadávať a nájsť konkrétne počítače, servery, smerovače a iné sieťové zariadenia, ktoré sú pripojené k internetu, pričom vyhľadávanie môže byť založené na meste, štáte, zemepisnej šírke a dĺžke, názve počítača, IP adrese alebo operačnom systéme. Útočník prostredníctvom tohto nástroja dokáže získať podrobnejšie informácie

napríklad o tom, aké verzie webových serverov obet' používa, či sa medzi nimi nachádzajú aj také, ktoré nie sú aktualizované a je možné ich napadnúť.

2.3.3 Creepy

Nástroj Creepy slúži ako geolokačný informačný agregátor, nakoľko pomocou tohto nástroja možno získať geolokačné údaje súvisiace s informáciami o užívateľoch zo sociálnych sietí alebo obrázkov. Všetky takto získané údaje sú zobrazené na mape, čo ilustruje obrázok 2.3.

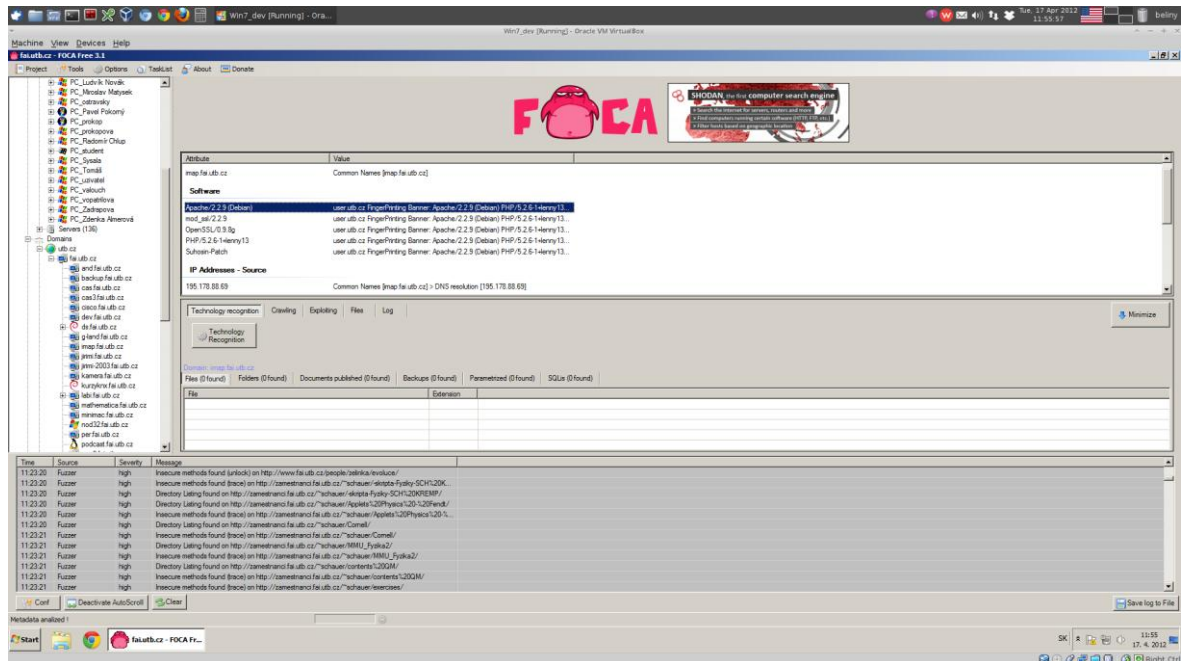


Obrázok 2.3: Nástroj Creepy [16]

2.3.4 FOCA

FOCA je nástroj primárne určený na zhromažďovanie informácií a to pomocou prehľadávania serverov, domén, URL liniek a verejných dokumentov. FOCA sa snaží nachádzať nezabezpečené HTTP metódy, prehľadávať dostupné priečinky či aktívnu cache v DNS alebo dokumenty z ktorých následne dokáže extrahovať metadata. Na základe týchto nájdených a

získaných informácií útočník môže pomocou FOCA získať a vytvoriť stromovú štruktúru o serveroch, počítačoch, dokumentoch svojej obete.



Obrázok 2.4: Nástroj FOCA

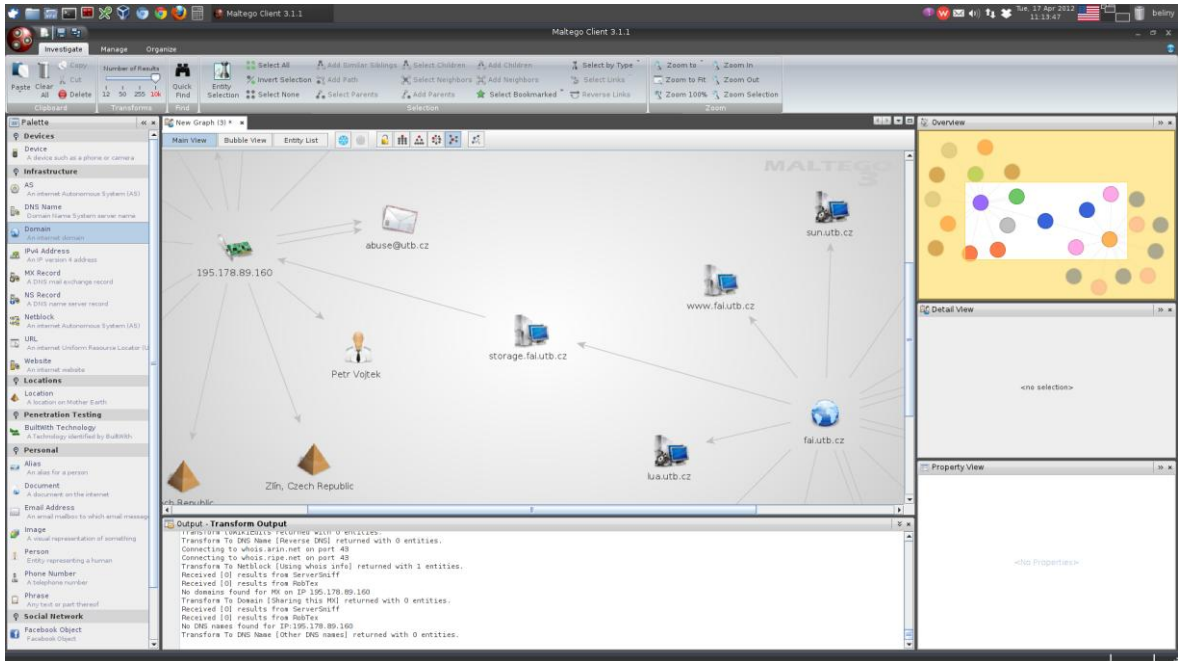
2.3.5 Maltego

Nástroj Maltego je taktiež primárne určený na zhromažďovanie informácií a slúži útočníkovi na určenie vzťahov či väzieb medzi ľuďmi, sociálnymi sieťami, spoločnosťami, organizáciami, webovými stránkami, dokumentmi, súbormi a informačnej infraštruktúry – domény, DNS, netbloky, IP adresy. Tento nástroj dokáže vyhľadávať informácie podľa požiadaviek útočníka a vizuálne ich vyjadriť, čo útočníkovi ďalej pomôže v tom, že všetky väzby a vzťahy hľadaných položiek si dokáže lepšie predstaviť a pochopiť.

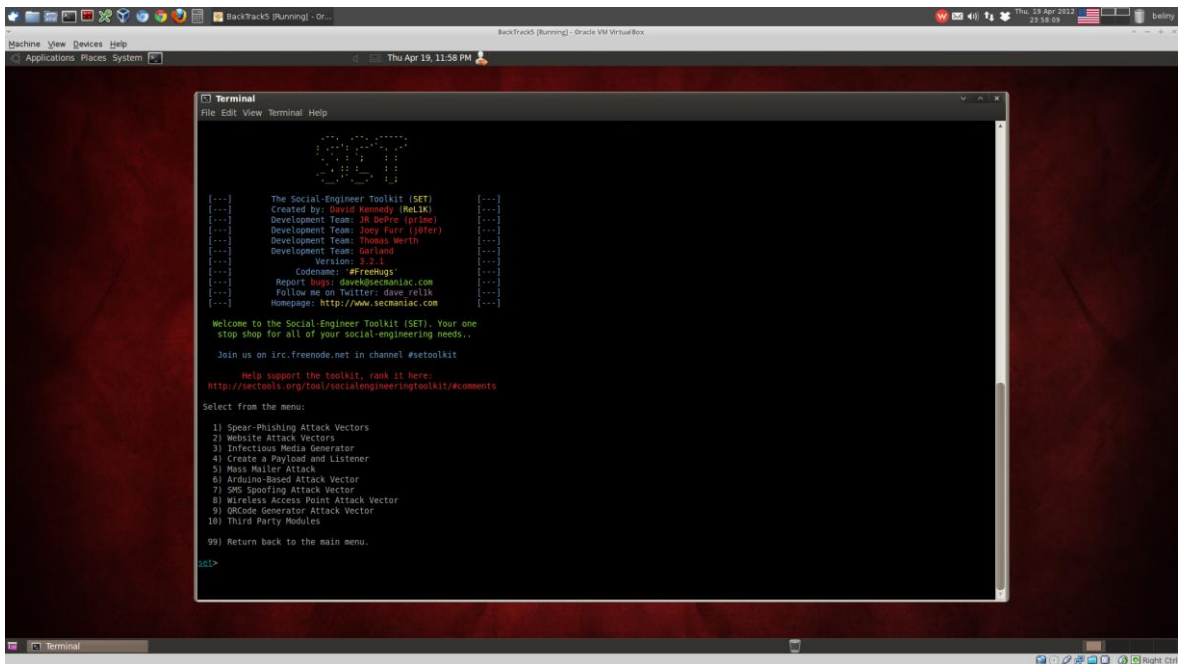
2.3.6 Social-Engineer Toolkit

Social-Engineer Toolkit (SET) je nástroj špeciálne navrhnutý pre tvorbu pokročilých útokov akými napríklad sú vytváranie phishingových emailov obsahujúcich prílohu s malware, škodlivých java appletov, vytváranie falošných webov s cieľom získať prihlasovacie meno a heslo alebo tvorba infikovaného kódu, ktorý sa vloží do USB média a takéto médium môže útočník použiť pri útoku metódou Road apples. Tento nástroj je štandardom a základom

každého sociálního inženýra. SET pri tvorbe útokov využíva aj nástroj Metasploit Framework, ktorý je určený na tvorbu exploitov.



Obrázok 2.5: Nástroj Maltego



Obrázok 2.6: Nástroj SET

2.3.7 Common User Password Profiler

Nakoľko každá bežná autentifikácia je založená na prihlasovacom mene a hesle, a užívatelia mnohokrát používajú jednoduché heslá, existuje nástroj Common User Password Profiler (CUPP) ktorý umožňuje útočníkovi na základe získaných informácií o obeti vytvoriť zoznam potenciálnych hesiel, ktoré obeť môže používať. Môže ísť o kombináciu čísel slov ktoré možno jednoducho priradiť k obeti. Zoznam hesiel je vygenerovaný zo vstupných dát, ktoré obsahujú napríklad meno a priezvisko obeť, meno manželky/manžela/detí, dátum narodenia, prezývku a iné.

2.3.8 Caller-ID/SMS Spoof

Pri falšovaní Caller-ID pri telefonickej alebo mobilnej komunikácii môže útočník využiť ponuku komerčných firiem, ktoré ponúkajú túto službu. Pri telefonovaní, je možné využiť službu SpoofCard a pri posielaní falošných SMS správ je možné využiť službu ArmSMS. Je vhodné pripomenúť, že nasledovné služby fungujú tzv. iba jedným smerom, takže ak obeť zavolá, alebo napíše SMS správu na podvrhnuté číslo, útočník sa k ich odpovedi nedostane.

2.3.9 USB Rubber ducky

USB Rubber ducky je veľmi zaujímavý hardvér. Je to zariadenie, ktoré je podobné USB médiu, pričom obsahuje výkonný procesor a je možné s jeho pomocou prostredníctvom jednoduchého skriptovacieho jazyka zasahovať do nastavení operačného systému, získavať dáta či vytvoriť si backdoor. Stačí aby sociálny inžinier toto zariadenie pripojil k počítaču a pripravený plnoautomatizovaný skript vykoná v priebehu niekoľkých sekúnd všetky príkazy ktoré má.

2.3.10 Portable Wi-Fi Node

Toto malé, jednoduché a veľmi výkonné zariadenie, si môže vyhotoviť ktokoľvek, nakoľko samotný základ, teda hardvéru je cenovo prístupný. Základným kameňom je Wi-Fi smerovač, ktorý podporuje platformu OpenWrt – linuxový systém pre sieťové zariadenia. Po aktualizácii firmware si útočník dokáže tento systém ľubovoľne upraviť tak, samozrejme vždy s ohľadom na technické a výkonnostné parametre, že toto zariadenie môže obsahovať rôzne nástroje akými sú napríklad Nmap, Tcpdump, Netcat, Aircrack-ng, dsniff a iné. Podstatou je, že ak sa sociálnemu inžinierovi podarí takto upravené zariadenie pripojiť do siete svojej obeť, má pre

seba vytvorený priamy prístup k celej sieťovej infraštruktúre, čo pre obeť predstavuje obrovské riziko.

2.3.11 Mini kamera

Ďalším užitočným zariadením vo výbave sociálneho inžiniera je mini kamera. Takéto zariadenie možno využiť pri obhliadke prostredia a vytváraní si obrazových záznamov, z ktorých si môže útočník detailnejšie prezrieť prostredie v ktorom sa bude pohybovať, alebo môže takto rýchlejšie zaznamenať – odfotografovať zapísané heslá či obsah citlivých dokumentov. Mini kamera môže byť ukrytá v kravate, v gombíku, alebo môže byť ako zamaskované ako pero, okuliare či diaľkové ovládanie od auta.



Obrázok 2.7: Mini kamera v tvare diaľkového ovládania od auta.

2.3.12 Keylogger

Posledným asi najznámejším zariadením je hardvérový keylogger. V dnešnej dobe sú dostupné rôzne typy takýchto zariadení, čo je ale pre všetky charakteristické je to, že dokážu zaznamenávať celú komunikáciu ktorá cez ne prechádza. Útočník sa ho vždy snaží umiestniť medzi počítač a vstupné zariadenie, ktorým je klávesnica.

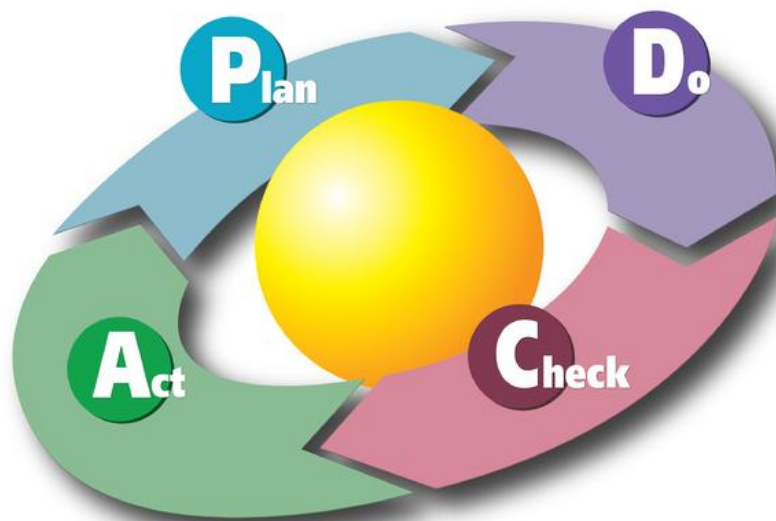
II. PRAKTICKÁ ČASŤ

3 OCHRANA PRED ÚTOKMI SOCIÁLNYM INŽINIERSTVOM

Tak ako pred každým počítačovým útokom, tak aj pred útokmi, ktoré sú realizované sociálnym inžinierstvom je potrebné sa brániť a vytvoriť určitú líniu ochrany.

Nakoľko je sociálne inžinierstvo charakteristické manipuláciou a ovplyvňovaním ľudského konania, je potrebné, aby všetky navrhnuté bezpečnostné opatrenia boli zamerané na obmedzenie či úplné zamedzenie možností a predchádzanie vzniku situácií, ktoré by mohol sociálny inžinier pri útoku využiť. Navrhnuté opatrenia by mali taktiež slúžiť v prípade bezpečnostného incidentu na jednoznačnú identifikáciu útokov vedených sociálnym inžinierstvom a v neposlednom rade, by mali slúžiť ako prevencia a zvyšovať bezpečnostné povedomie.

Bezpečnostné opatrenia by mali byť definované súborom pravidiel – bezpečnostnou politikou. Ďalej by mali byť striktné dodržiavané a toto dodržiavanie aj pravidelne kontrolované a vyhodnocované. Taktiež je potrebné aby zavedená bezpečnostná politika bola v pravidelných intervaloch prehodnocované a v prípade potreby sa aktívne pristúpilo k jej zlepšeniu. Práve tento PDCA cyklus možno aplikovať z medzinárodnej normy ISO/IEC 27001, ktorej úlohou je zriadiť, implementovať, prevádzkovať, monitorovať, preskúmať, udržiavať a zlepšovať informačnú bezpečnosť.



Obrázok 3.1: PDCA cyklus [19]

Samotný návrh opatření by mal vždy predchádzať dôležitému rozhodnutiu čo sa bude chrániť a akým spôsobom sa to bude chrániť. V nasledujúcich podkapitolách bude poskytnutý všeobecný návrh na ochranu pred jednotlivými netechnickými a technickými útokmi, ktoré boli uvedené v kapitolách 2.1 a 2.2. Tieto návrhy vychádzajú z normy ISO/IEC 27001 z časti Príloha A – Ciele riadenia a opatrenia, taktiež sa opierajú o vlastné praktické skúsenosti autora práce so sociálnym inžinierstvom a neskôr budú slúžiť ako podklad pre návrh bezpečnostnej politiky.

3.1 Návrh opatření proti netechnickým útokom

Ako bolo spomenuté v kapitole 2.1 medzi netechnické útoky patria Trashing, Spying, Techie Talk, NPL, Ten attack a Piggybacking. Všetky tieto techniky majú spoločné to, že útočník pri ich realizácii nepotrebuje veľké technické znalosti a vybavenie, ba naopak postačujú mu skutočne minimálne.

Prvým útokom Trashingom môže sociálny inžinier získať rôzne množstvo informácií, ktoré dokáže využiť napríklad pri tvorbe personálnej štruktúry či získavaní kontaktov a následne ich použiť pri realizácii útoku. Na to aby sa zamedzila možnosť a prístup útočníkovi k rôznym informáciám je vhodné prijať a zaviesť klasifikáciu informácií a dokumentov, ktorou sa dosiahne rozdelenie dokumentov napr. na verejné, citlivé, dôverné alebo tajné, podľa potreby organizácie. Na základe tejto klasifikácie bude presne určené, aké typy dokumentov sa majú skartovať na vyčlenenom skartovacom zariadení a ktoré je možné vyhodiť do smetného koša. Klasifikácia musí byť uplatnená na všetky typy informácií – v papierovej podobe i elektronickej podobe. Je preto potrebné, aby taktiež bola dodržiavaná elektronická skartácia dát napríklad pomocou voľne dostupného softvéru Eraser, alebo v prípade skartácie hardvéru – optické alebo magnetické médiá, ich fyzickým zničením. Za skartovacie zariadenie by mala byť určená jedna zodpovedná osoba, ktorá bude môcť pristupovať aj k takto znehodnoteným informáciám a predovšetkým by táto osoba mala mať na zodpovednosti hlavne fyzické zničenie médií s dátami. Ďalším návrhom je zavedenie riadenia prístupu k informáciám, ktoré zabezpečí, že užívatelia budú k informáciám, dátam a dokumentom pristupovať na základe určitej úrovne oprávnenia.

Ďalším útokom, ktorý patrí medzi netechnické je Spying. Ako už bolo spomenuté, prostredníctvom tohto útoku je útočník schopný odpozeraním či odpočúvaním získať heslo prípadne inú citlivú informáciu. Pri návrhu opatření pred týmto typom útoku, je vhodné zaviesť pravidlo čistého stola, ktoré by mal striktne dodržiavať každý užívateľ. Pravidlo čistého

spočíva v tom, že v pracovnom priestore, tj. pracovný stôl, počítač prípadne iné zariadenia, sa nachádzajú iba také dokumenty, kde pri ich odpozeraní alebo prečítaní informácií útočníkom nedôjde k žiadnej komprimácii. Je vhodné na stoloch použiť nepriehľadné boxy na dokumenty. Je potrebné, aby sa striktno dodržiavalo pravidlo, že žiadny užívateľ nebude mať vo svojom pracovnom priestore na lístočku napísané svoje heslo. Takéto citlivé informácie sa v žiadnom prípade nesmú nachádzať na miestach akými sú monitor, klávesnica alebo stôl.

Ďalším útokom, ktorý sa radí medzi netechnické je Techie Talk. Tento typ útoku je najzraniteľnejší hlavne voči nedostatočne technicky znalým užívateľom. Je potrebné si uvedomiť, že útočník je pre dosiahnutie svoju cieľu schopný spraviť čokoľvek a pri útoku sa nemusí vydávať len za zamestnanca podpory (helpdesk), či partnera tretej strany ale za kohokoľvek. Základným opatrením v tomto prípade je naučiť užívateľov, že v prípade výskytu akéhokoľvek problému, musí kontaktovať iba určité osoby a zároveň iba od nich môže prijať pomoc. Každý užívateľ by mal poznať túto osobu, v prípade malých organizácií sa zväčša všetci vzájomne poznajú, ale v prípade veľkých organizácií je vhodné aby sa užívateľ v rámci nástupu do organizácie oboznámil okrem svojich povinností, zodpovednosti či pracovnej náplne aj s človekom (skupinou osôb) ktorý môže a bude pomáhať pri riešení jeho problémov. V prípade, že daný užívateľ je v komunikácii s treťou stranou, je ďalším opatrením nariadenie, že užívateľ smie konať a komunikovať s tretími strany iba v rámci svojho poverenia nadriadeným.

Technika neurolingvistického programovania je spôsob ktorý umožňuje s ľuďmi manipulovať a preto je pomerne náročné sa voči tejto technike brániť, ale zároveň treba spomenúť, že úspech tohto útoku spočíva na pokročilých komunikačných skúsenostiach útočníka a dlho získavanej praxi. V tomto prípade schopnosť obrany a ochrany závisí iba od samotnej obeť a jej individuálnych schopností intuitívne odhaliť zlé úmysly útočníka. Na útok technikou NLP pri fyzickom kontakte sociotechnika a obeť je vhodné aplikovať jednoduchú zásadu, byť obozretný a nedôverovať cudzím a neznámym osobám. V prípade telefonického kontaktu by sa mala obeť pokúsiť získať od útočníka určité autentifikačné údaje, ktoré by útočník nemal poznať a na základe týchto zistení by obeť mala dokázať odhaliť útok.

Zo série netechnických útokov je ďalším Ten attack, pri ktorom dochádza k vniknutiu útočníka do budov, priestorov či kancelárií. Pri zabezpečení priestorovej a fyzickej bezpečnosti je potrebné prijať opatrenia pre fyzický prístup a striktno dodržiavať nasledovné návrhy. V prípade budovy je vhodné, aby bezpečnostný personál vždy mal pod dohľadom

hlavné klúčové priestory cez ktoré je možné vstúpiť do objektu a monitoroval či tento vstup využívajú iba autorizované osoby. Bezpečnosť ostatných všetkých vstupov do budovy by mala byť zaistená minimálne použitím vhodných technologických prvkov. Jedným z ďalších návrhov je vytvoriť takzvanú zonáciu priestorov, ktorej úlohou je definovať zóny s určitou úrovňou prístupu do ktorých budú patriť jednotlivé priestory. Na základe oprávnenia a úrovne prístupu budú môcť do jednotlivých priestorov vstupovať iba oprávnené osoby. Ďalším opatrením je, aby sa kancelárie po ukončení práce zamykali a dodržiaval klúčový režim a registrovaný výdaj klúčom iba oprávneným osobám.

Poslednou netechnickým útokom je metóda Piggybacking. Návrh predchádzajúcich opatrení možno aplikovať aj na obranu pred týmto útokom, a zároveň tiež prijať ďalší návrh, ktorého podstatou je zavedenie rozdelenia vstupov do budovy na základe účelu. Takto bude zaručené, že donáška balíkov a veľkých krabíc bude možná iba cez tento vstup, nakoľko služobný vstup bude umožňovať vstup do budovy iba osobám bez objemných a nadrozmerých nákladov. Ďalej všetky bočné alebo zadné vstupy slúžiace ako „priestor pre fajčiarov“ je vhodné zrušiť a fajčiarsky priestor presunúť na iné miesto, cez ktorý nie je možný vstup do budovy.

3.2 Návrh opatrení proti technickým útokom

Medzi technické útoky, ktoré sú opísané v kapitole 2.2 patria Phishing, Pharming, Caller-ID a SMS spoofing, Road apples, Whaling attack, Mumble attack, Vishing, Reverse social engineering. Pri realizácii týchto techník sú v maximálnej miere využívané všetky dostupné technické a informačné prostriedky a útočník musí mať určité technické znalosti a vybavenie.

Prvým útokom, ktorý patrí medzi technické je pomerne známy a rozšírený Phishing. Aj napriek tomu, že v dnešnej dobe proti Phishingu existuje pomerne veľa foriem ochrany je potrebné, okrem aktualizovaného antivírusového softvéru, dodržiavať nasledujúce pravidlá, pri ktorých je úspešnosť útoku nižšia.

- Byť podozrievavý voči emailovým správam s urgentnou žiadosťou o osobné alebo finančné informácie.
- Nevypĺňať akýkoľvek formulár v emaily, ktorý požaduje osobné alebo finančné informácie.
- Neklikat' na odkazy v prijatom emaily, pokiaľ si nie sme istý, že správa je overená alebo nepoznáme odosielateľa.

- Vždy sa uistiť, že používame zabezpečené webové stránky pri predkladaní či postúpení citlivých informácie prostredníctvom webového prehliadača.
- Všimnúť či zabezpečené webové stránky majú URL v tvare https:// a riadok pre písanie URL adresy obsahuje obrázok bezpečnostného zámku.
- Vždy skontrolovať použitý certifikát webovej stránky.
- Používať doplnky webového prehliadača, napr. nástroj Netcraft Anti-Phishing Toolbar, pomocou ktorého možno odhaliť dôveryhodnosť webovej stránky.
- Vždy požívať najaktuálnejšiu verziu webového prehliadača so všetkými bezpečnostnými záplatami.

Tieto pravidlá sa dajú aplikovať aj na útok nazvaný Whaling attack, nakoľko jeho realizácia je podobná Phishingu, ale v ochrane pred týmto útokom je potrebné aby bezpečnostné opatrenia boli striktne zavedené a kontrolované voči vrcholovému a riadiacemu manažmentu.

Druhým technickým útokom je Pharming. Tak ako pri obrane pred Phishingom aj pri obrane pred Pharmingom je potrebné dodržiavať vyššie spomenuté pravidlá. Okrem týchto pravidiel je taktiež potrebné prijať také bezpečnostné opatrenia, aby nikto nedôveryhodný a neoprávnený nemohol manipulovať s DNS záznamami na DNS servery. V prípade pokusu o lokálny útok, je dobré dbať na to, aby žiadna neznáma a neoprávnená osoba nemala prístup k počítaču, ktorý môže byť cieľom tohto útoku.

Ako ďalším útokom patriacim do kategórie technický patrí Caller-ID a SMS spoofing. Aj napriek tomu, že sa technicky nedá zamedziť, aby útočník používal sfaľované pevné alebo mobilné čísla, je možné aplikovať určité bezpečnostné opatrenia, prostredníctvom ktorých sa dá zamedziť tomu, aby útočník dosiahol svoj cieľ. Pri akejkoľvek komunikácii, telefonickej alebo cez SMS, v prípade, že útočník požaduje prostredníctvom telefónu citlivé informácie, je vhodné mu napríklad zatelefonovať naspäť na pevnú linku alebo mobilný telefón a overiť si, či skutočne komunikujeme s pravým človekom. Ďalej je vhodné zaviesť autentifikačné mechanizmy napríklad vo forme overovacích otázok, napríklad: *Aké je Vaše ID zamestnanca alebo osobné číslo?* A následne si túto informáciu overiť. V prípade že útočník osloví človeka, ktorý pozná skutočnú osobu za ktorú sa vydáva, bude útočník vždy odhalený. Pri prijatí falošnej SMS správy je potrebné si taktiež overiť inými komunikačnými kanálmi skutočnosti uvedené v prijatej SMS správe.

Útok „Road apples“ sa síce radí medzi technické útoky – príprava trojského koňa, malware či iného škodlivého kódu, ale jeho realizácia sa vykonáva netechnickým spôsobom, nakoľko je snahou útočník rozmiestniť a zanechať infikované USB kľúče alebo optické média na miestach s vysokou pravdepodobnosťou nálezu cieľovej obete. Pri nájdení takého média, ktoré je voľne položené je potrebné sa držať týchto bezpečnostných zásad. Nepripájať takéto zariadenie do akéhokoľvek počítača či notebooku. V prípade nálezu v priestoroch organizácie – chodba, toaleta, parkovisko, atď. a odovzdať toto zariadenie nadriadenému alebo inému zodpovednému pracovníkovi. Zo samotného etického správania sa vyplýva aj to, že by sme vždy akýkoľvek nález mali ohlásiť určitej zodpovednej osobe, nakoľko ak by niekto takéto zariadenie stratil a v rámci organizácie to nahlásil, v dohľadnej dobe by sa prišlo na to komu prenosné zariadenie patrí. Ak by toto prenosné zariadenie bolo nájdené mimo priestorov organizácie určite sa treba vždy držať pravidiel, nepripájať toto zariadenie do pracovného počítača či notebooku a ďalej je už na osobnom zvážení každého človeka, či sa takto zachová aj vo svojom súkromí.

Ďalším útokom, ktorý patrí medzi technické útoky je Mumble attack. Nakoľko sa tento útok realizuje cez telefón a útočník prakticky zneužíva možné rečové postihnutie človeka, je dosť problematické odhaliť útok sociálnym inžinierstvom. V tomto prípade je ale možné, aby ak existujú osobné a citlivé záznamy či informácie o osobe, ktorá má rečové postihnutie bola v rámci záznamov evidovaná aj osoba, ktorá ma moc zastupovať túto osobu, aby sa pri požiadavke poskytnutia citlivých informácií komunikovalo iba s osobou, ktorá je na to oprávnená. Táto oprávnená osoba by mala byť jediná, ktorá bude poznať odpovede aj na prípadné bezpečnostné a overovacie otázky.

Voči Vishingu je vhodné a potrebné sa držať jedného základného pravidla, a tým je nikomu neposkytovať svoje osobné citlivé a dôverné informácie. Vždy je potrebné pamätať, že v prípade banky akýkoľvek pracovník nikdy pri riešení rôznych vzniknutých situácií nevyžaduje citlivé informácie, akými napríklad sú číslo kreditnej karty a PIN. Pri akomkoľvek probléme je znalosť týchto citlivých informácií nepodstatná a preto v prípade otázok orientovaných na číslo karty a PINu je potrebné sa začať správať mimoriadne opatrne a obozretne.

Posledným útokom, ktorý bol opísaný v kapitole 2.2 je Reverse social engineering. Ochrana voči tomu typu útoku spočíva hlavne v bezpečnom správaní sa obete, nakoľko základné kroky: sabotáž, reklama a pomoc postupujú za sebou v pomerne krátkom časovom slede. Takto „náhodne“ načasovaná reklama a pomoc pri akomkoľvek probléme môže byť

obeti podozrivá a môže takúto situáciu odhaliť. V prípade technických problémov pokiaľ v organizácii neexistuje oddelenie, ktoré zabezpečuje technickú podporu – obvykle všetci zamestnanci zodpovedné osoby za technickú podporu poznajú, je vhodné vždy riešiť vzniknuté problémy so známou a overenou osobou, ktorú poznáme a pravidelne vykonáva technický servis či opravy, to platí aj v situáciách akou je napríklad časová tieseň.

4 IDENTIFIKÁCIA SLABÍN ZABEZPEČENIA

PROSTREDNÍCTVOM TESTOV SOCIÁLNYM INŽINIERSTVOM

Sociálne inžinierstvo môže vo veľkej miere zlepšiť a zvýšiť bezpečnosť v akejkoľvek organizácii a to prostredníctvom testovania, ktoré sa opiera práve o prvky sociálneho inžinierstva. Práve takéto testy umožnia identifikovať slabiny a zraniteľnosti, ktoré by mohol potenciálny útočník zneužiť. V tejto kapitole a ďalších sú tiež ďalej uvedené aj vyjadrenia, názory a skúsenosti certifikovaných odborníkov v oblasti informačnej bezpečnosti, ktorí majú skúsenosti aj so sociálnym inžinierstvom. Na získanie ich názorov bol použitý elektronický dotazník – Social engineering survey for master thesis – „Social engineering as a tool for testing computer systems security“, príloha A.1, kde sú uvedené všetky odpovede na otázky, ktoré boli obsahom dotazníka. Spolu boli oslovení 6 odborníci, Sharon Conheady, Nick Drage, Pavol Lupták, Eszter Oroszi, Martin Psársky, Jason E. Street, pričom všetci okrem Sharon Conheady odpovedali na otázky v dotazníku, ktorého sumár je uvedený v prílohe A.2. Napriek tomu, že každý z oslovených pracuje v bezpečnostnej spoločnosti, odpovede v dotazníku, sú založené na ich osobnom názore a osobnej skúsenosti, v žiadnom prípade nejde o prezentovanie názoru danej spoločnosti.

4.1 Spôsoby realizácie testov

Tak ako sa pristupuje k realizácii penetračných testov webových aplikácií či serverov alebo testov sieťovej infraštruktúry, rovnako aj realizácia testov sociálnym inžinierstvom sa môže vykonávať podľa rôznej úrovne znalostí, ktoré máme. Testami sociálnym inžinierstvom možno simulovať také situácie, ktoré sa v realite veľakrát vyskytujú a z ktorých možno reálny útok aj realizovať. Testami dokážeme simulovať napríklad tieto situácie:

- útok reálneho útočníka, ktorý nemá žiadne informácie – blackbox test
- útok napríklad bývalého zamestnanca či obchodného partnera, ktorý má čiastočné nie úplne aktuálne informácie – greybox test
- útok vlastného zamestnanca, ktorý disponuje aktuálnymi a úplnými informáciami, či fyzickým prístupom do organizácie – whitebox test

Samotné testovanie je možné realizovať s nástrojmi, ktoré sú opísané v kapitole 2.3 a rôznymi komunikačnými kanálmi:

- internetový kanál (email, webová stránka, atď.)
- telekomunikačný kanál – (pevná linka, fax, atď.)
- mobilný kanál – (SMS, atď.)
- fyzický kanál – (fyzický kontakt, rozhovor, atď.)

V dotazníku, ktorý bol realizovaný bola jedna otázka zameraná na zistenie, aký komunikačný kanál respondenti preferujú pri realizácii sociálneho inžinierstva. Z ich vyjadrení, ktoré sú uvedené nižšie, nemožno jednoznačne určiť, ktorý komunikačný kanál je najpoužívanejší, nakoľko každý z respondentov odpovedal na základe svojich osobných skúseností, ale jednotlivé komunikačné kanále možno aspoň odhadom usporiadať podľa používania, pričom internetový kanál je prvom mieste, za ním môže spoločne nasledovať telekomunikačný s fyzickým a posledným je mobilný kanál.

- Nick Drage: 30 % – internetový kanál, 10 % – telekomunikačný, 10% mobilný kanál, 50 % – fyzický kanál
- Pavol Lupták, C|EH, CISSP: 90 % – internetový kanál, 10 % – telekomunikačný/mobilný kanál, 0 % – fyzický kanál
- Eszter Oroszi, CISA: 90 % – internetový kanál, 5 % – telekomunikačný kanál, 5% – fyzický kanál
- Martin Psársky, CISA: 30 % – internetový kanál, 20 % – telekomunikačný kanál, 20 % – mobilný kanál, 30 % – fyzický kanál
- Jason E. Street, C|EH, CISSP, ECIH, GSEC, GCIH, IEM, IAM, etc... : väčšinou iba fyzické testy na mieste

Od týchto komunikačných kanálov sa ďalej odvíjajú jednotlivé spôsoby realizácie testov, ktoré možno rozdeliť nasledovne [14]:

- phishingový test
- telefonický test
- test s prenosnými médiami
- fyzický prienik do priestoru organizácie

- prehľadávanie odpadkov
- preverenie zverejnených informácií

Ďalšia otázka v dotazníku bola orientovaná na zistenie, aké útoky respondenti realizujú keď vykonávajú testy sociálnym inžinierstvom. V odpovediach sú uvedené netechnické – Piggybacking, Dumpster diving a iné a aj technické útoky – Phishing, infikovaný USB kľúč a iné, pričom všetky tieto útoky spadajú pod jednotlivé spôsoby realizácie testov, ktoré sú uvedené vyššie.

Dotazník taktiež obsahoval otázku, v ktorej mali respondenti zvoliť na stupnici od 1 (najmenší potenciál) do 5 (najväčší potenciál) potenciál hrozby útokov na bezpečnosť organizácie, ktoré sú uvedené v kapitolách 2.1 a 2.2 – okrem útoku typu NPL, pretože realizácia tohto typu útoku je veľmi špecifická a náročná. Z netechnických útokov respondenti jednoznačne označili útok typu Piggybacking s najväčším potenciálom hrozby pre danú organizáciu, jeden respondent hodnotou 5 a traja respondenti hodnotou 4 a jeden respondent hodnotou 3. Z technických útokov respondenti označili s najväčším potenciálom hrozby útok typu Caller-ID a SMS spoofing, traja respondenti hodnotou 5 a jeden hodnotou 4 a taktiež jeden hodnotou 3. Ďalej s veľkým potenciálom hrozby nasledujú útoky ako Phishing, Pharming a Road apples.

A na záver dotazník obsahoval otázku, v ktorej sa mali respondenti vyjadriť, aké sú podľa ich názoru najnebezpečnejšie typy útokov sociálnym inžinierstvom. Medzi najčastejšími odpoveďami sa vyskytoval Phishing, tento útok napísali všetci štyria respondenti a z netechnických útokov to boli útoky ktoré sa realizujú pri fyzickom prieniku do organizácie. Všetky detailné odpovede všetkých respondentov sú uvedené v prílohe A.2.

Z vyjadrení a názorov oslovených bezpečnostných odborníkov možno usúdiť, že zvolené testy sociálnym inžinierstvom skutočne odzrkadľujú potrebu realizácie týchto testov z dôvodu identifikácie a odhalenia slabín, ktoré možno zneužiť práve prostredníctvom týchto rozšírených a nebezpečných útokov sociálnym inžinierstvom.

4.2 Metodika tvorby testov a ich realizácia

Na to aby testy skutočne odhalili zraniteľnosti a slabiny zabezpečenia, je potrebné pristupovať nie len k realizácii samotného testu ale aj k tvorbe a príprave testu individuálne. Ako už bolo spomenuté testy možno realizovať rôznymi komunikačnými kanálmi, ale bez ohľadu na to, aký komunikačný kanál je použitý, vždy sa testy môžu realizovať tromi formami – blackbox,

greybox alebo whitebox test a zároveň každý test by mal spĺňať atribúty reálneho útoku, teda jednotlivé fázy, ktoré sú uvedené v kapitole 1.2, pričom tieto fázy útoku sociálnym inžinierstvom by mali byť odzrkadlené pri samotnej tvorbe testov.

Prvá fáza, zhromažďovanie informácií, je v rámci testu realizovaná identifikáciou, určovaním a preskúmaním cieľov. Ďalšie dve fázy, budovanie vzťahov a dôvery a využitie dôvery, je realizovaná tvorbou predstieraných scenárov, vďaka ktorým možno špecificky zacieliť kde je najvhodnejšie vybudovať a využiť dôveru. Posledná fáza, realizácia a zneužitie je reprezentovaná vykonaním samotného útoku. [12]

Pred tým, než sa začne s testovaním je potrebné aby boli splnené určité podmienky, ktoré je potrebné definovať pred akýmkoľvek penetračným testom:

- definovať rozsah testu, aké oblasti bezpečnosti sa budú testovať
- v akom časovom intervale bude test prebiehať
- zvoliť formu testu – blackbox, greybox alebo whitebox a podľa toho dostať užitočné informácie
- či bude test prebiehať vzdialene alebo aj fyzicky
- počet realizovaných scenárov
- či si zákazník bude môcť vybrať z ponúknutých scenárov
- definovať aký okruh ľudí bude vedieť, že prebieha test
- či môže byť test odvolaný a za akých okolností
- aký okruh osôb bude vedieť, že sa realizuje test
- zákazník by sa mal zaručiť, že o teste nebude informovať zamestnancov

Ďalším potrebným bodom je to, aby sociálny inžinier – samotný tester mal list „Get Out of Jail Free Letter“, kde je potvrdené zo strany testovanej organizácie, že zodpovedné osoby o teste vedia a dali k jeho realizácii povolenie, sú na ňom uvedené kontakty na všetky strany. Vďaka tomuto listu je teda možné preveriť či ide o test alebo nie, nakoľko v priebehu testovanie môže vzniknúť aj taká situácia, že sociálny inžinier bude prichytený.

4.2.1 Identifikácia cieľov

Identifikácia cieľov patrí do prvej fázy realizácie útoku sociálnym inžinierstvom. Ide o zhromažďovanie informácií z rôznych zdrojov a výber tých podstatných, dôležitých či zaujímavých údajov, vďaka ktorým možno čo najpresnejšie identifikovať cieľ, ktorý bol zadaný pred testovaním.

Cieľom identifikácie je taktiež zistiť čo najväčšie množstvo relevantných informácií a údajov vďaka ktorým sa bude možné priblížiť k cieľu alebo tento cieľ aj dosiahnuť.

Pri získavaní informácií je vhodné použiť nástroje, ktoré sú uvedené v kapitole 2.3 a slúžia primárne na získavanie pasívnych informácií. Okrem použitia týchto nástrojov je vhodné taktiež manuálne prehliadať webové stránky a hlavne sociálne siete. Vďaka sociálnym sieťam máme na určitom mieste mnohokrát veľmi veľa informácií. Je potrebné taktiež zdôrazniť, že niekedy nehrá rolu kvantita získaných informácií, ale ich kvalita. Pri zbieraní a identifikovaní relevantných a pravých informácií je dobré ísť do hĺbky, údaje si overiť, či sa napr. sú internet v rámci viacerých zdrojov totožné a rovnaké informácie, či skutočne ide konkrétnu osobu a nie len o menovca a iné.

4.2.2 Preskúmanie

Ďalšou časťou, ktorá patrí do prvej fázy útoku sociálnym inžinierstvom je preskúmanie získavanie pasívnych informácií, pričom tieto informácie sú zameraná na fyzické budovy, zariadenia či autentifikačné mechanizmami a z toho vyplýva, že použité metódy pri preskúmaní sú viacej orientované na fyzický test. V rámci preskúmania je vhodné sa orientovať na nasledujúce body:

- kde sú bezpečnostný strážnici
- či sa fajčiari stretávajú v určitej oblasti mimo objekt
- kde sú umiestnené CCTV kamery
- sledovať pohyb zamestnancov – v akom čase opúšťajú kanceláriu či kedy chodia na obed
- či sa zamestnanci nejakým spôsobom identifikujú pri vstupe do objektu, prípadne ako prebieha vstup do objektu pre návštevy alebo prípadne technické či čistiace služby
- či je možné nejakým spôsobom skopírovať identifikačné preukazy

- preveriť bočné vstupy, núdzové východy, garáže či iné možné vstupy a výstupy
- pokúsiť sa vysledovať rôzne neobvyklé situácie v okolí objektu

4.2.3 Tvorba predstieraných scenárov

Na tvorbe predstieraného scenáru, ktorý sa bude realizuje v rámci testovania je postavený základný kameň úspechu a to z takého dôvodu, že vďaka nemu je možné vytvoriť a vybudovať dôveru a pripraviť základy pre využitie tejto dôvery. Cieľom vytvoreného scenáru by malo byť vytvorenie pocitu falošného bezpečia, z čoho následne plynie jednoduchšie vytváranie dôvery voči obeti.

Pri tvorbe scenáru je dobré pozerať napríklad na to, o akú veľkú organizáciu ide alebo s akými údajmi či informáciami narába. V prípade menších organizácii je pravdepodobné, že sa všetci zamestnanci môžu vzájomne poznať a naopak v prípade väčšej organizácie, ktorá má napríklad aj viacej pobočiek, sa zamestnanci nemusia poznať vôbec. Čo sa týka informácií, tie majú vždy nejakú úroveň hodnoty ale môže sa rozlišovať, či daná organizácia narába napríklad s údajmi, ktoré sa týkajú financií, osobných a citlivých údajov o rôznych osobách či vlastným know-how. Ak cieľová organizácia pracuje napríklad s financiami, je pravdepodobnejšie že bezpečnostné opatrenia v rámci tejto organizácie budú striktnnejšie než tam kde sa narába napríklad s osobnými údajmi. Ako už bolo ale spomenuté, informácie majú vždy nejakú hodnotu a útočník môže iba predpokladať, ako si ich jeho obeť vážia a ochraňujú.

Na základe týchto údajov, ktoré možno určiť aj na základe identifikácie a preskúmania, je možné zvážiť pri tvorbe scenárov použitie rôznych pomôcok, rekvizít či kostýmov. Ďalej je dôležité, aby predstierané scenáre boli realistické, aby samotné obeť mali čo najmenšie šance získať a mať nejaké podozrenie. Vhodnými vzorovými scenármi pri telefonickom útoku môže napríklad byť vydávanie sa za novinára, študenta, personálneho agenta, pracovníka charity, záujemcu o zamestnanie či človeka z technickej podpory. Pri fyzických útokoch sú vzorovými scenármi napríklad vydávanie sa za zamestnanca, poštára, údržbára, čističa, priateľa či priateľku. Pri tvorbe scenárov je potrebné dodržiavať pravidlo, ktorým je nevydávať sa za skutočných ľudí či organizácie, ale po dohode a so súhlasom zákazníka je možné sa vydávať iba za zamestnancov testovanej organizácie.

4.2.4 Vykonanie samotného útoku

Vykonanie samotného útoku znamená zneužitie dôvery, ktorá vznikla medzi útočníkom a obeťou. Ide o realizáciu pripraveného scenáru, vďaka ktorému útočník dosiahne svoj cieľ. Niekedy sa môže stať aj taká situácia, že nie je možné pripravený scenár zrealizovať do konca, v takom prípade je potrebné sa prispôbiť aktuálnej situácii a v rámci nej sa pokúsiť vyťažiť maximum pre dosiahnutie cieľa.

Pri realizácii a vykonaní útoku treba myslieť aj na to, že je potrebné zbierať a zaznamenávať dôkazy o tom, že sme pri testovaní skutočne dosiahli cieľ. Aj vďaka dôkazom bude následne možné spracovať výsledky a vhodne ich prezentovať. Tieto činnosti na získavanie dôkazov by mali byť nedeštruktívne a medzi takéto činnosti napríklad patrí:

- zanechanie fyzickej či elektronickej stopy
- vytvorenie fotografie či videozáznamu
- získať nejaký dôkaz z vnútra organizácie

Pri každom vykonaní pripraveného scenáru je nutné mať pripravený aj plán úniku, spôsob ako sa dostať z objektu organizácie alebo ako na seba pri skončení scenáru neupozorniť.

4.3 Spracovanie výsledkov vykonaných testov

Iba na základe získaných dôkazov možno spracovať výsledky vykonaných testov, pričom všetky tieto dôkazy sú uvedené a prezentované vo výslednej správe. Tvorba výslednej správy testu sociálnym inžinierstvom by sa mala skladať zo základných častí, medzi ktoré patrí:

- manažérske zhrnutie – aký test bol realizovaný, akou formou a v akom časovom horizonte, zhodnotenie stavu bezpečnosti a zdôraznenie, že samotné výsledky testov by nemali slúžiť trestanie zamestnancov ale na prijatie odporúčaných náprav
- rozsah testovania – uvedené metódy a techniky použité pri testovaní
- vyhodnotenie rizík – riziká sa posudzujú ako kombinácia pravdepodobnosti útoku a jeho dopadu na aktíva, hmotné a nehmotné, organizácie
- obmedzujúce faktory – faktory, ktoré ovplyvnili priebeh testu
- pasívne zhromažďovanie informácií – aké informácie a údaje boli nájdené, identifikované a preskúmané

- popis jednotlivých scenárov – čo bolo cieľom, aký sa dosiahol výsledok, pri náleze zraniteľnosti poskytnúť odporúčanie
- zhrnutie zraniteľností – vyjadrenie počtu zraniteľností

Pri tvorbe výslednej správy a spracovávaní výsledkov sa odporúča v časti kde je popísaný priebeh jednotlivých scenárov uviesť všetky získané dôkazy a dôkladne popísať akým spôsobom sa realizoval konkrétny scenár. Pri identifikácii zraniteľností možno postupovať tak, že za zraniteľnosť možno považovať vždy to, ak sa čiastočne alebo úplne podarí splniť cieľ, ktorý bol zadaný pred testom. Napríklad, ak v prípade snahy vylákať citlivé informácie od obeť, samotná obeť síce neposkytne citlivé údaje ale iba prejaví záujem a ochotu poskytnúť citlivé informácie, možno tento záujem a ochotu považovať za zraniteľnosť, nakoľko obeť neprejavila žiadne náznaky a snahu overiť si určité skutočnosti v danej situácii. Pri všetkých identifikovaných zraniteľnostiach je vhodné poskytnúť odporúčanie, ktoré eliminuje vznik zraniteľnosti.

Vo výslednej správe by nemali byť uvedené konkrétne mená zamestnancov, ktorí sa dopustili bezpečnostného incidentu, ale odporúča sa, aby títo zamestnanci boli uvedený v prílohách výslednej správy, kde sú realizované scenáre popísané detailnejšie, kto bol oslovený, konkrétne v akom čase, atď. Týmto sa zabezpečí to, že výsledná správa bude rozdelená na dve časti, prvá – hlavná časť, ktorá bude anonymná a druhá – prílohy, ktorá nebude anonymná. Zodpovedná osoba, bezpečnostný manažér alebo vedenie organizácie, podľa potreby sprístupnia a dajú prečítať autorizovaným osobám tú časť správy ako bude vhodné.

4.4 Obmedzujúce faktory testov

Obmedzujúcim faktorom je obvykle obmedzená časová dĺžka testovania, nakoľko reálny útok môže byť realizovaný v časovom horizonte niekoľkých mesiac, niekedy možno až rokov.

Podľa zvolenia jednotlivého typu testovania – blackbox, greybox alebo whitebox testovanie sa taktiež odvíjajú prípadné obmedzujúce faktory. Pri blackbox teste sa časové obmedzenie premietne hlavne do nemožnosti získať za krátky čas dostatočný a širší informačný kontext (znalosť pomerov, štruktúry, zamestnaneckej hierarchie, používaných autentifikačných či softvérových metód atď.). Aby sa znížilo toto obmedzenie odporúča sa realizovať testy sociálnym inžinierstvom formou greybox či whitebox testovania, čím sa náležitejšie preverí správanie a bezpečnostné povedomie zamestnancov, dodržiavanie či prípadné nedostatky v bezpečnostných smerniciach, nakoľko je možné vopred na základe

obdržaných bezpečnostných smerníc a politík, prípadne znalosti obsahu interného bezpečnostného školenia či predpisov – čo zamestnanci nemôžu porušovať a čo musia dodržiavať, lepšie vytvoriť a prispôbiť scenáre pri testovaní.

5 TESTY MODELOVÝCH SITUÁCIÍ

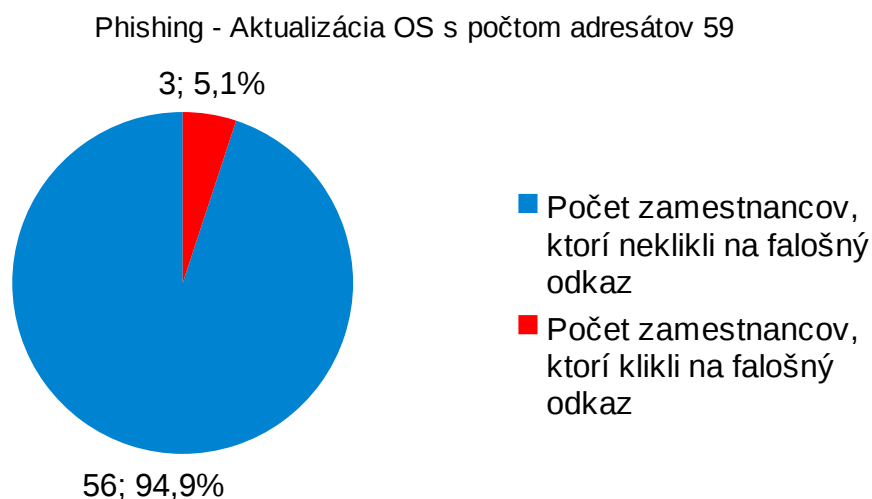
V rámci testovania modelových situácií boli zvolené také modelové situácie, ktoré sú považované za najviac nebezpečné a zároveň sú pomerne rozšírené. Niektoré testy boli realizované autorom práce v reálnom prostredí a výsledky teda pochádzajú z reálneho testu, pričom sú reprezentované iba výsledky, z dôvodu zachovania úplnej anonymity a etiky. Jeden test bol nahradený dotazníkom, pričom respondenti sú laici v oblasti informačnej bezpečnosti a pred vykonaním dotazníka neboli oboznámení s dôsledkami a nebezpečím, ktoré môže vzniknúť.

5.1 Scenár č. 1 – Rozposielanie phishingových emailov

Tento test prebehol v reálnom prostredí a z dôvodu zachovania anonymity je možné spomenúť, že bol realizovaný pre jednu európsku banku, pričom boli testovaní všetci zamestnanci a cieľom bolo overiť ich bezpečnostné správanie. Táto inštitúcia pravidelne vykonáva školenia v oblasti informačnej bezpečnosti, čo sa aj reálne premietlo do výsledkov.

Obsahom testu bolo rozposlanie phishingových emailov s unikátnym hash linkom, podľa ktorého bolo možné jednotlivito identifikovať každého jedného zamestnanca. Phishingové emaily, ktoré boli rozposlané zamestnancom neboli úplne rovnaké, nakoľko boli rozdelené a cielené na rôzne skupiny zamestnancov. Zdrojový kód skriptu napísaný v jazyku Perl, vďaka ktorému bolo možné posilať phishingové emaily s upravenou hlavičkou, je uvedený v prílohe B.1. Tento skript bol použitý aj pri ďalšom testovaní.

Prvá časť emailov obsahovala informáciu o aktualizácii operačného systému, pričom obsah phishingového emailu sa odvolával na vymyslenú informáciu, ktorú bolo možné „overiť“ na podvrhutej webovej stránke. Telo emailu obsahovalo falošný URL odkaz pre aktualizáciu, ktorý bol nasmerovaný na neškodnú webovú stránku a text s výzvou si túto aktualizáciu stiahnuť a nainštalovať. Dôveryhodnosť obsahu bola zvýšená tým, že email bol odoslaný z podvrhnutého emailového aliasu v tvare *admin@institucia.com*. Výsledky tohto testu sú reprezentované na obrázku 5.1, z 59 adresátov na odkaz klikli 3.



Obrázok 5.1: Vyhodnotenie prvej časti phishingových emailov

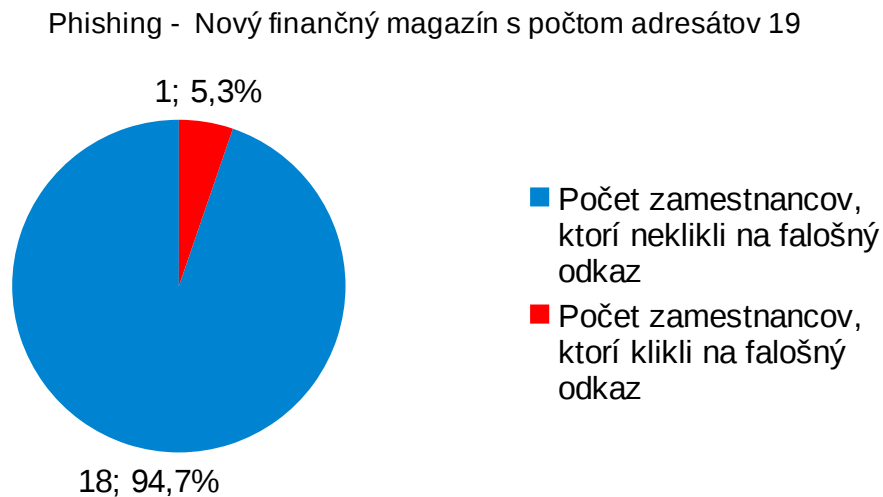
Ďalšej skupine zamestnancov bol odoslaný phishingový email s obsahom textu, ktorý sa týkal interného školenia, pričom bol odoslaný zo sfalšovanej adresy istého zamestnanca. Telo emailu obsahovalo unikátny hash odkaz, cez ktorý boli adresáti presmerovaní na stránku <http://youtube.com>. Zo 40 oslovených tento falošný odkaz navštívila iba 1 osoba, obrázok 5.2.



Obrázok 5.2: Vyhodnotenie druhej časti phishingových emailov

Poslednej časti zamestnancov bol odoslaný falošný email s informáciou o vymyslenom magazíne, s cieľom predstaviť sa prostredníctvom video upútavky. Telo phishingového

emailu obsahovalo falošný odkaz pričom adresáti boli opäť presmerovaní na stránku <http://youtube.com>. Z 19 oslovených v druhej správe odkaz navštívila taktiež iba 1 osoba.



Obrázok 5.3: Vyhodnotenie poslednej časti phishingových emailov

Všetky kliknutia boli zaznamenávané v logoch servera a nakoľko každý adresát dostal email s jedinečným odkazom obsahujúcim hash link, nebol problém s identifikovaním zamestnanci, ktorý klikol na falošný odkaz. Takéto kliknutia na podvrhnutý odkaz môžu znamenať spustenie škodlivého kódu a získanie kontroly nad napadnutým počítačom, zber údajov z napadnutého počítača, prípadne zber údajov z lokálnej siete. Keďže útočníkovi stačí len 1 kliknutie na podvrhnutý odkaz aby dosiahol svoj cieľ a získal prístup do internej siete organizácie, takto vzniknutý incident možno považovať vážny.

5.2 Scenár č. 2 – Získanie citlivých a dôverných informácií

Ďalší test bol realizovaný prostredníctvom telekomunikačného kanálu. Tak ako predchádzajúci test, aj tento test bol realizovaný v reálnom prostredí a z dôvodu zachovania anonymity je možné spomenúť, že aj tento test bol realizovaný pre finančnú inštitúciu, ktorá pravidelne pre svojich zamestnancov vykonáva školenia v oblasti informačnej bezpečnosti.

Cieľom tohto testu bolo získať citlivé a dôverné informácie, konkrétne išlo o osobné údaje klientov testovanej finančnej inštitúcie, pričom sme vystupovali ako zamestnanec z marketingového oddelenia. Náhodne vybraní zamestnanci boli telefonicky oslovení a

požiadaní o zaslanie osobných údajov na podvrhnutý firemný email a aby bola zvýšená dôveryhodnosť požiadavky, bola zamestnancom zaslaná aj sprievodná emailová správa s našiou požiadavkou zo sfalšovanej podvrhutej emailovej adresy. Odoslaná správa bola upravená tak, že obsahovala prednastavenú hodnotu Reply-To, ktorá obsahovala našu podvrhnutú firemnú adresu. Sprievodný email obsahoval nasledujúci text, pričom sú vypustené tie časti, ktoré nemožno z dôvodu zachovania anonymity zverejniť:

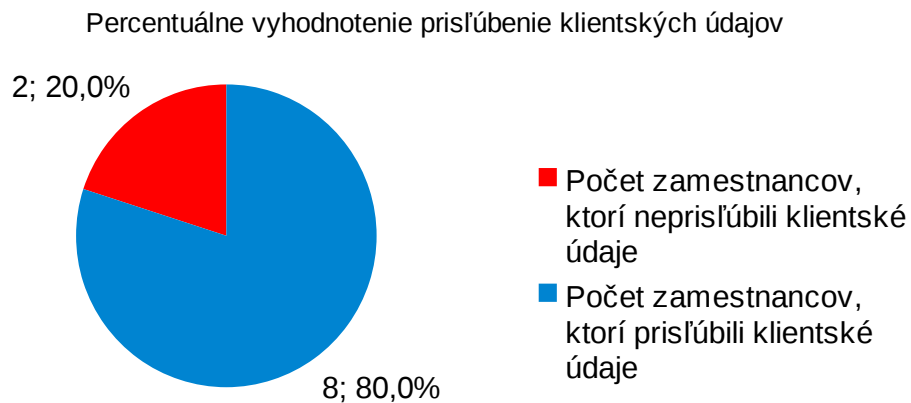
Dobry den,

na zaklade nasho telefonického rozhovoru Vas ziadam pre potreby marketingoveho oddelenia o zaslanie udajov o ...vypustená časť... klientoch, ktorí ...vypustená časť... Primarne potrebujeme meno, priezvisko, adresu, telefonny kontakt. Pokial mozno, poslite mi to prosim este dnes.

Dakujem velmi pekne.

S pozdravom ...vypustená časť...

V priebehu testovania bolo oslovených 10 náhodne vybraných zamestnancov, pričom až 8 zamestnancov bolo ochotných bez akýchkoľvek náznakov overovania poskytnúť zoznam klientov s ich osobnými údajmi. V jednom prípade bol prisľúbený zoznam nových klientov, ale následne pri overovanom telefonáte, či zamestnanec obdržal email so žiadosťou nám bolo oznámené, že nie sme zamestnanec marketingového oddelenia, za ktorého sa vydávame, v druhom prípade nám hneď pri prvom telefonickom kontakte s daným zamestnancom bolo oznámené, že nie sme zamestnanec marketingového oddelenia, za ktorého sa vydávame.



Obrázok 5.4: Prezentované výsledky zo scenáru č. 2

Nakoľko ďalej v priebehu testovania bolo prostredníctvom overovacích telefonátov zistené, že niektorí oslovení zamestnanci obdržali email s požiadavkou a niektorí tento email neobdržali, boli emailové správy opätovne rozposlané a obsah správ bol nasledovný:

Dobry den,

znovu Vam posielam email, ktory ste mozno, kvoli technickym problemom s emailom, nedostali.

S pozdravom ...vypustená časť...

Dobry den,

na zaklade nasho telefonickeho rozhovoru Vas ziadam pre potreby marketingoveho oddelenia o zaslanie udajov o ...vypustená časť... klientoch, ktorí ...vypustená časť... Primarne potrebujeme meno, priezvisko, adresu, telefonny kontakt. Pokial mozno, poslite mi to prosim este dnes.

Dakujem velmi pekne.

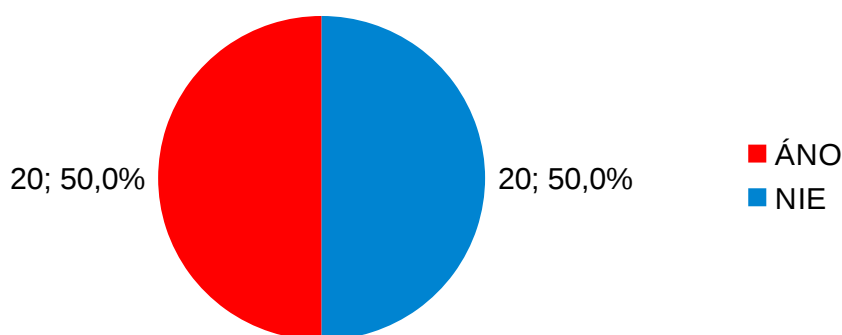
S pozdravom ...vypustená časť...

Po opätovnom overovaní, či zamestnanci obdržali email s výzvou o zaslanie osobných údajov o klientoch bolo zistené, že administrátori testovanej inštitúcie pravdepodobne zakázali prichádzajúcu poštu z IP adresy, z ktorej boli podvrhnuté emaily odoslané, a preto boli emaily opäť rozposlané z novej IP adresy, ktorá sa od tej chvíle začala používať. Do ukončenia testu neboli obdržané žiadne osobné údaje klientov, čo možno hodnotiť, že všetci oslovení zamestnanci sa zachovali správne a neposkytli nami požadované citlivé údaje.

5.3 Scenár č. 3 – Bezpečnostné správanie sa zamestnancov pri nájdení prenosného média

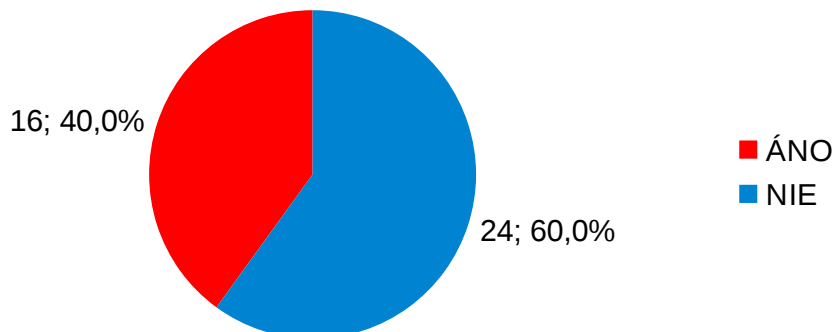
Predmetom tretieho testu bolo overiť a zistiť bezpečnostné správanie sa pri nájdení prenosného média, USB kľúč a či optického média. Test bol nahradený anonymným elektronickým dotazníkom, príloha C.1, nakoľko uvedené odpovede v dotazníku by boli ekvivalentné reálnemu konaniu zamestnancov. Dotazník obsahoval 6 otázok s možnosťou odpovede vo forme áno/nie. Dotazníku sa zúčastnilo 40 respondentov, z toho 21 mužov a 19 žien, pričom 12 respondentov bolo vo veku 20 - 29 rokov, 11 respondentov vo veku 30 - 39 rokov, 8 respondentov vo veku 40 - 49 rokov a 9 respondentov vo veku 50 - 59 rokov, viď. príloha C.2.

Otázka č.1: V prípade, že nájdete na chodbe, na ulici, na parkovisku, atď. USB kľúč, pripojili by ste ho k Vášmu vlastnému počítaču alebo notebooku?



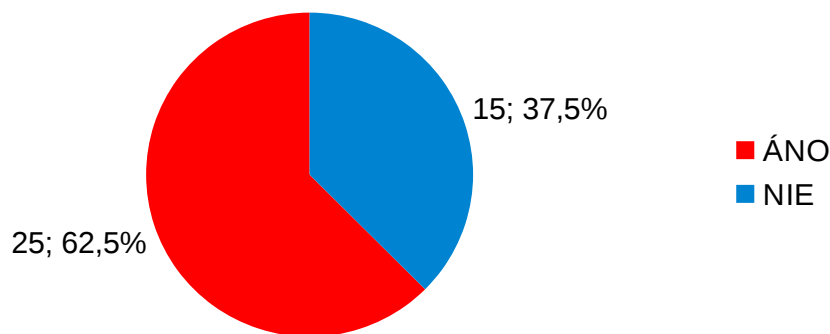
Obrázok 5.5: Vyhodnotenie otázky č. 1 z dotazníku scenára č. 3

Otázka č.2: V prípade, že nájdete na chodbe, na ulici, na parkovisku, atď. USB kľúč, pripojili by ste ho k pracovnému počítaču alebo notebooku?



Obrázok 5.6: Vyhodnotenie otázky č. 2 z dotazníku scenára č. 3

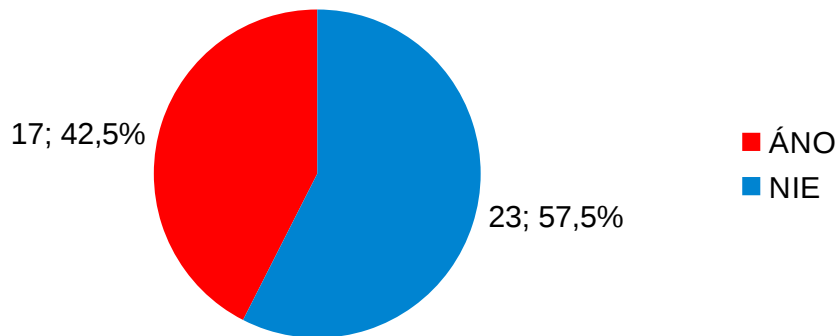
Otázka č.3: Prehliadali, pozerali by ste obsah uložený na nájdenom USB kľúči?



Obrázok 5.7: Vyhodnotenie otázky č. 3 z dotazníku scenára č. 3

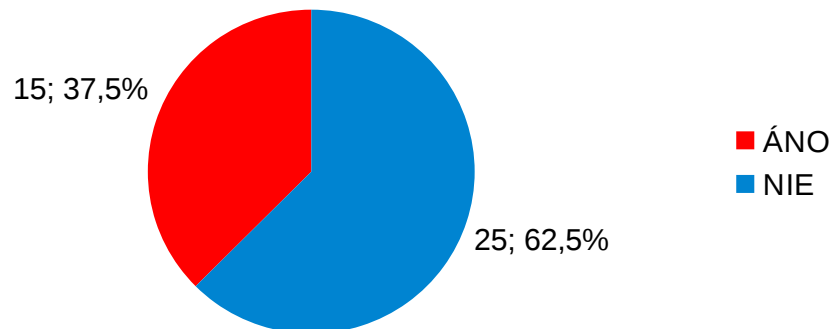
Z odpovedí na otázky, ktoré sa týkali USB kľúčov možno usúdiť, že väčší počet respondentov by nájdený USB kľúč skôr pripojilo k svojmu osobnému počítaču či notebooku, 50 % zamestnancov, než k pracovnému počítaču či notebooku, 40 % zamestnancov. Čo je ale potrebné zdôrazniť je, že počet respondentov, ktorí by na nájdenom USB kľúči prehliadalo a prezeralo dokumenty bez ohľadu na to či by išlo o osobný alebo pracovný počítač či notebooku je až 62,5 %, čo je skoro trištvrtina opýtaných.

Otázka č.4: V prípade, že nájdete na chodbe, na ulici, na parkovisku, atď. optické médium - CD/DVD so zaujímavým popisom, spustili by ste ho na Vašom vlastnom počítači alebo notebooku?



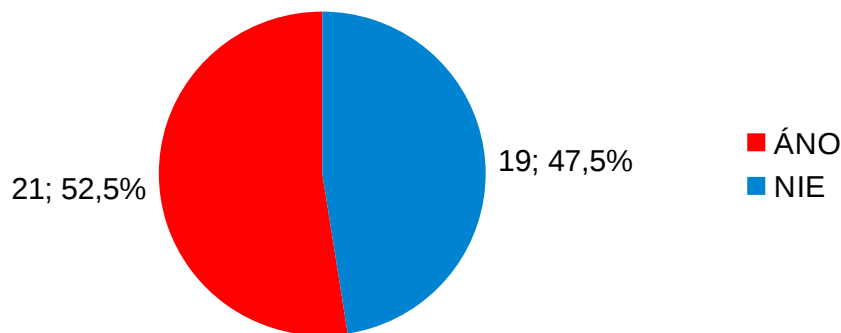
Obrázok 5.8: Vyhodnotenie otázky č. 4 z dotazníku scenára č. 3

Otázka č.5: V prípade, že nájdete na chodbe, na ulici, na parkovisku, atď. optické médium - CD/DVD so zaujímavým popisom, spustili by ste ho na pracovnom počítači alebo notebooku?



Obrázok 5.9: Vyhodnotenie otázky č. 5 z dotazníku scenára č. 3

Otázka č.6: Prehliadali, pozerali by ste obsah uložený na nájdenom CD/DVD médiu?



Obrázok 5.10: Vyhodnotenie otázky č. 6 z dotazníku scenára č. 3

Pri odpovediach s optickým médiom sú výsledky pozitívnejšie, nakoľko 42,5 % respondentov by nájdené optické médium spustilo na svojom osobnom počítači či notebooku, a 37,5 % respondentov by nájdené optické médium spustilo na svojom pracovnom počítači či notebooku. Tieto pozitívnejšie výsledky sa taktiež premietli do poslednej otázky a to tak, že obsah uložený na nájdenom optickom médiu, by prezeralo menší počet zamestnancov, konkrétne 52,5 %, než pri USB kľúčoch.

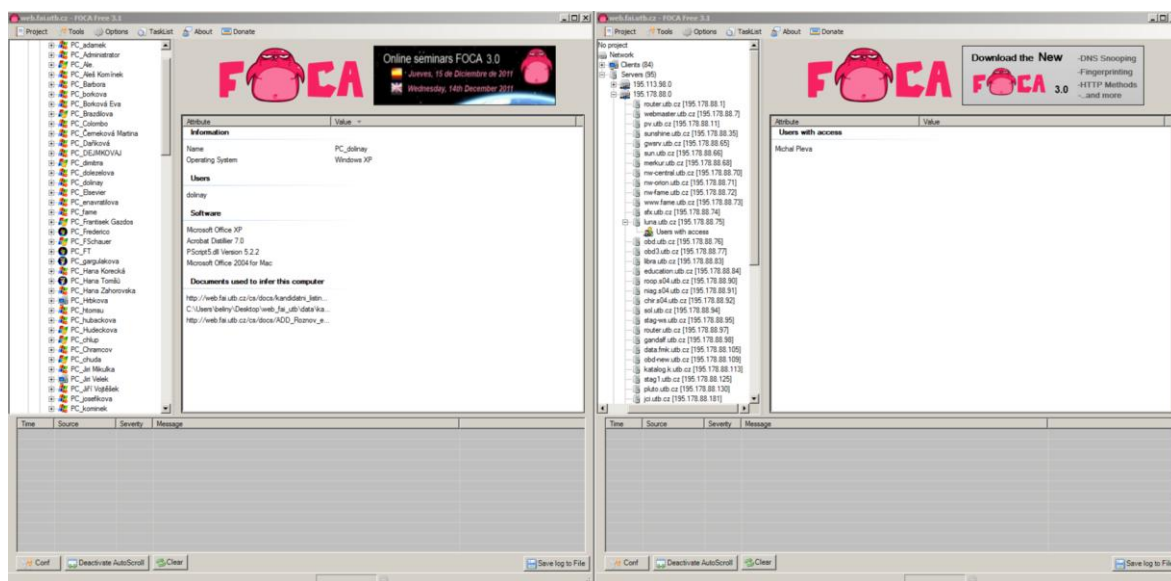
Pri porovnaní jednotlivých prenosných médií, USB kľúča a optického média, by boli respondenti pri nájdení optického média opatrnejší než pri nájdení USB kľúča. Je možné, že tento výsledok je spôsobený tým, že nález USB kľúča je pre obeť psychologicky atraktívnejší, nakoľko má možnosť toto zariadenie používať aj v budúcnosti, zatiaľ čo optické média postupom strácajú na svojej atraktivite a nemožno ich používať tak ako USB kľúče.

Z vyššie uvedených výsledkov možno usúdiť, že bežní zamestnanci a laici v oblasti informačnej bezpečnosti sú náchylní voči tomuto typu útoku, pričom dôsledky ich konania si veľmi neuvedomujú. Pri náleze akéhokoľvek presného média je potrebné vždy myslieť na to, že takéto zariadenie môže obsahovať rôzny malware, backdoor, prípadne infikované dokumenty alebo iný škodlivý kód, pomocou ktorého možno získať citlivé údaje, alebo dokonca kontrolu nad napadnutým počítačom.

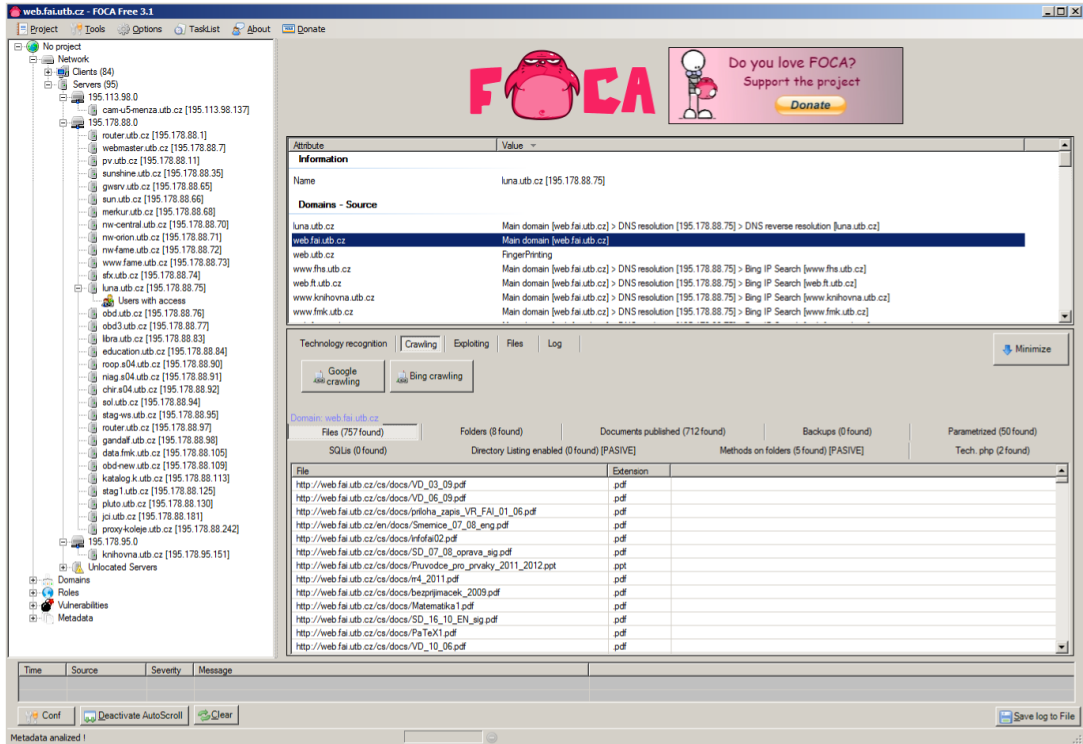
5.4 Scenár č. 4 – Preverenie zverejnených informácií

Štvrtý test sa týkal preverenia zverejnených informácií a zhodnotenia možnosti potenciálneho útoku vďaka týmto zverejneným a dostupným informáciám. Cieľová organizácia bola zvolená Fakulta aplikovanej informatiky (FAI) na UTB ve Zlíně, takže sa v rámci testu pracovalo napríklad s doménou <https://web.fai.utb.cz>, a kľúčovými slovami týkajúcich sa tejto fakulty. Pri testovaní boli hlavne použité nástroje FOCA, Maltego a taktiež dostupné informácie v rámci webovej stránky fakulty.

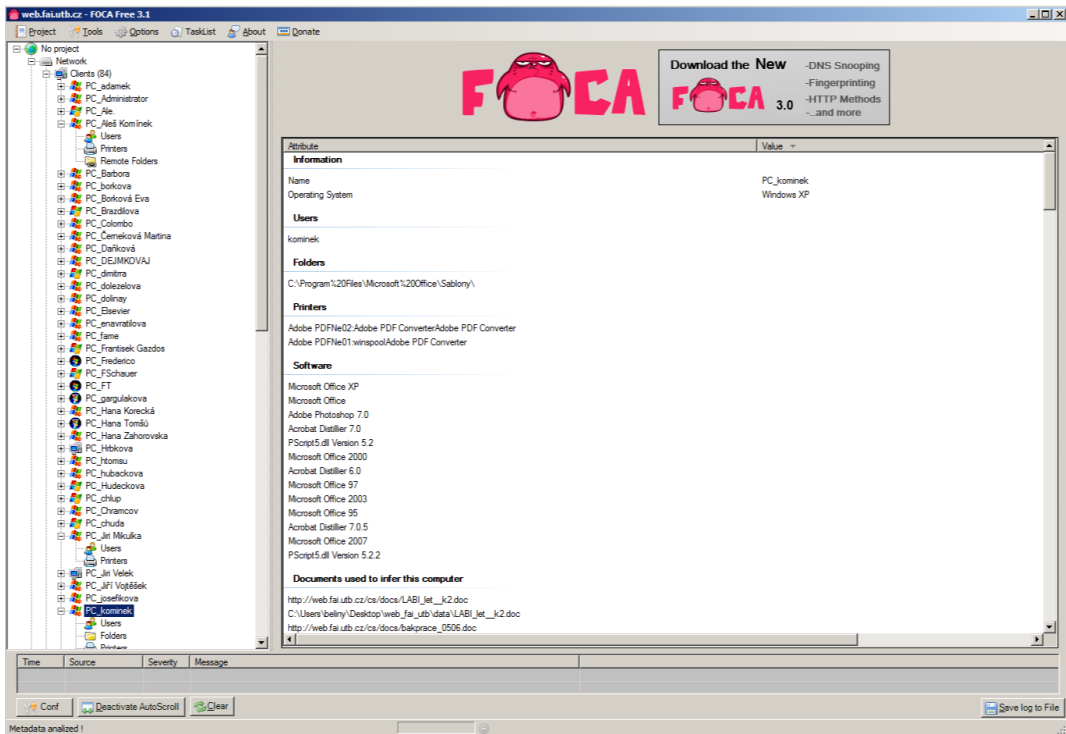
Nástrojom FOCA boli zistené údaje o sieťovej infraštruktúre – osobných počítačov, serverov či rozsahu IP adries. Ďalej pomocou tohto nástroja boli získané dokumenty, ktoré sú umiestnené na webovej stránke FAI a vďaka metadáтам bolo možné aj identifikovať rôzne ďalšie informácie, ktoré by bolo možné použiť pri prípadnom útoku sociálnym inžinierstvom. Použitie nástroje FOCA je ilustrované nižšie.



Obrázok 5.11: Použitie nástroja FOCA – údaje o sieťovej infraštruktúre 1



Obrázok 5.12: Použitie nástroja FOCA – údaje o sieťovej infraštruktúre 2



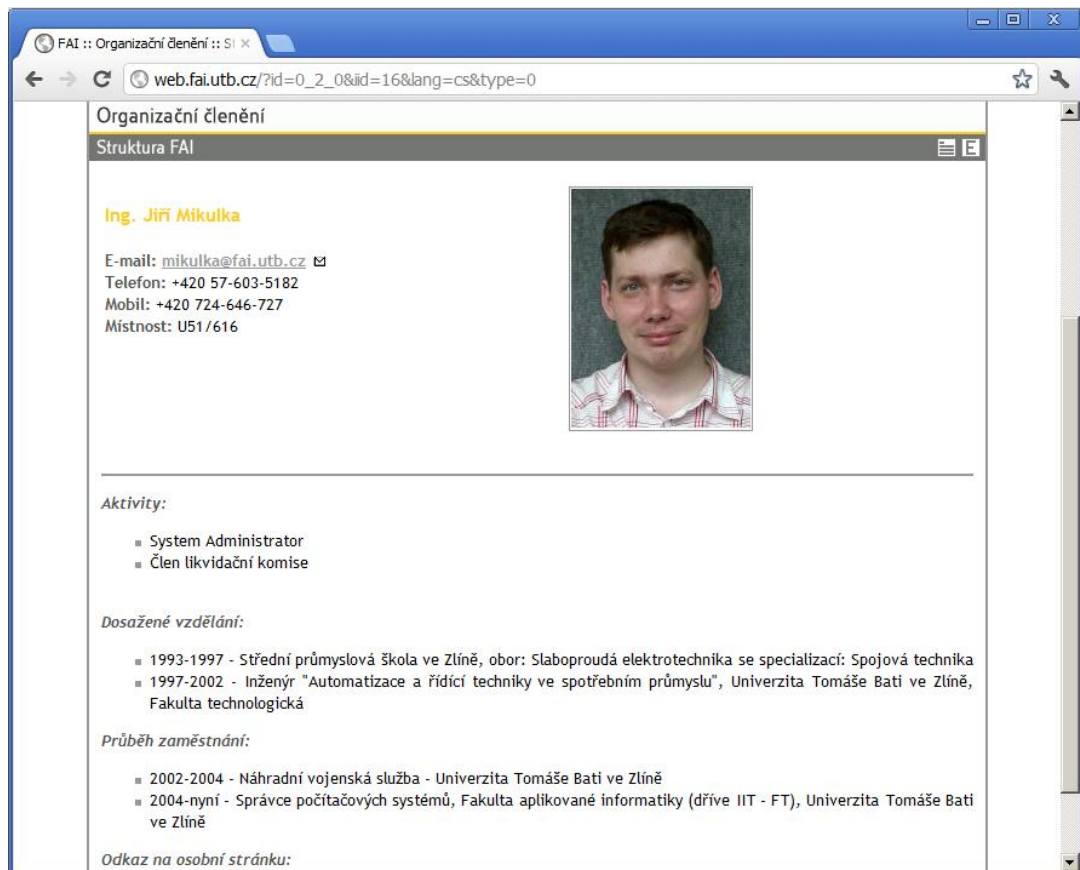
Obrázok 5.13: Použitie nástroja FOCA – údaje o sieťovej infraštruktúre 3

ID	Type	URL	Download	Download Date	Size	Analyzed	Modified Date
699	pdf	http://web.fai.utb.cz/cs/docs/IRT_Bc_10_modra.pdf	•	26. 4. 2012 12:32:54	183.71 KB	•	26. 4. 2012 13:26:29
690	pdf	http://web.fai.utb.cz/cs/docs/dekanske_vzhno_29_4_10.pdf	•	26. 4. 2012 12:32:49	249.59 KB	•	26. 4. 2012 13:26:28
664	pdf	http://web.fai.utb.cz/cs/docs/Oprav_IRT_cervena_2010.pdf	•	26. 4. 2012 12:32:21	183.52 KB	•	26. 4. 2012 13:26:26
666	pdf	http://web.fai.utb.cz/cs/docs/Oprav_BTSM_sluta_2011_komise.pdf	•	26. 4. 2012 12:32:22	183.57 KB	•	26. 4. 2012 13:26:26
667	pdf	http://web.fai.utb.cz/cs/docs/SD_07_ENGS_sig.pdf	•	26. 4. 2012 12:32:24	371.26 KB	•	26. 4. 2012 13:26:26
637	pdf	http://web.fai.utb.cz/cs/docs/IRT_Bc_10_sluta.pdf	•	26. 4. 2012 12:31:23	183.71 KB	•	26. 4. 2012 13:26:22
642	pdf	http://web.fai.utb.cz/cs/docs/PKS_ing_11_cervena.pdf	•	26. 4. 2012 12:31:27	183.55 KB	•	26. 4. 2012 13:26:22
644	pdf	http://web.fai.utb.cz/cs/docs/SD_06_11_sig.pdf	•	26. 4. 2012 12:32:18	7.76 MB	•	26. 4. 2012 13:26:22
606	pdf	http://web.fai.utb.cz/cs/docs/Metodika_hodnoceni_200816.pdf?PHPSESSID=63...	•	26. 4. 2012 12:31:02	432.16 KB	•	26. 4. 2012 13:26:19
608	pdf	http://web.fai.utb.cz/cs/docs/ObshovaNaphPrednasek.pdf?PHPSESSID=9448...	•	26. 4. 2012 12:31:02	58.99 KB	•	26. 4. 2012 13:26:19
570	pdf	http://web.fai.utb.cz/cs/docs/Oprav_BTSM_zelena_2011_komise.pdf	•	26. 4. 2012 12:30:19	183.54 KB	•	26. 4. 2012 13:26:15
574	pdf	http://web.fai.utb.cz/cs/docs/20110720084430321.pdf	•	26. 4. 2012 12:30:24	237.67 KB	•	26. 4. 2012 13:26:15
578	pdf	http://web.fai.utb.cz/cs/docs/FLKR_BTSM_bc_modra_11.pdf	•	26. 4. 2012 12:30:28	183.41 KB	•	26. 4. 2012 13:26:15
559	pdf	http://web.fai.utb.cz/cs/docs/PKS_ing_10_zelena.pdf	•	26. 4. 2012 12:30:11	183.53 KB	•	26. 4. 2012 13:26:14
566	pdf	http://web.fai.utb.cz/cs/docs/FLKR_BTSM_ing_modra_11_komise.pdf	•	26. 4. 2012 12:30:16	183.54 KB	•	26. 4. 2012 13:26:14
569	pdf	http://web.fai.utb.cz/cs/docs/FLKR_BTSM_ing_cervena_11.pdf	•	26. 4. 2012 12:30:18	183.57 KB	•	26. 4. 2012 13:26:14
552	pdf	http://web.fai.utb.cz/cs/docs/IRT_Bc_10_cervena.pdf	•	26. 4. 2012 12:30:07	183.72 KB	•	26. 4. 2012 13:26:13
494	pdf	http://web.fai.utb.cz/cs/docs/IRT_Bc_10_zelena.pdf	•	26. 4. 2012 12:29:31	184.68 KB	•	26. 4. 2012 13:26:09
496	pdf	http://web.fai.utb.cz/cs/docs/IT_ing_10_sluta.pdf	•	26. 4. 2012 12:29:32	184.95 KB	•	26. 4. 2012 13:26:09
502	pdf	http://web.fai.utb.cz/cs/docs/IRT_IT_ing_10_cervena.pdf	•	26. 4. 2012 12:29:36	184.59 KB	•	26. 4. 2012 13:26:09
504	pdf	http://web.fai.utb.cz/cs/docs/VD_11_11_sig.pdf	•	26. 4. 2012 12:29:39	392.98 KB	•	26. 4. 2012 13:26:09
466	pdf	http://web.fai.utb.cz/cs/docs/IRT_Bc_10_sluta.pdf	•	26. 4. 2012 12:29:14	184.66 KB	•	26. 4. 2012 13:26:07
430	pdf	http://web.fai.utb.cz/cs/docs/zadost_uznzeni_zapoctu_kousky_2011.pdf	•	26. 4. 2012 12:28:42	201.62 KB	•	26. 4. 2012 13:26:04
393	pdf	http://web.fai.utb.cz/cs/docs/VD_06_11_sig.pdf	•	26. 4. 2012 12:28:12	801.69 KB	•	26. 4. 2012 13:26:00
384	pdf	http://web.fai.utb.cz/cs/docs/SD_10_11_sig.pdf	•	26. 4. 2012 12:28:07	2.87 MB	•	26. 4. 2012 13:25:59
357	pdf	http://web.fai.utb.cz/cs/docs/SD_07_07_sig.pdf	•	26. 4. 2012 12:27:13	1.58 MB	•	26. 4. 2012 13:25:55
346	pdf	http://web.fai.utb.cz/cs/docs/VD_01_11_sig.pdf	•	26. 4. 2012 12:26:46	1.27 MB	•	26. 4. 2012 13:25:53
336	pdf	http://web.fai.utb.cz/cs/docs/VD_05_11_sig.pdf	•	26. 4. 2012 12:26:24	1.86 MB	•	26. 4. 2012 13:25:51
321	pdf	http://web.fai.utb.cz/cs/docs/moziny.pdf	•	26. 4. 2012 12:25:57	511.14 KB	•	26. 4. 2012 13:25:50
320	pdf	http://web.fai.utb.cz/cs/docs/SD_05_10_sig.pdf	•	26. 4. 2012 12:25:51	1.71 MB	•	26. 4. 2012 13:25:49
311	pdf	http://web.fai.utb.cz/cs/docs/Matematika1M1.pdf	•	26. 4. 2012 12:25:13	272.68 KB	•	26. 4. 2012 13:25:48
303	pdf	http://web.fai.utb.cz/cs/docs/IRT_Bc_11.pdf	•	26. 4. 2012 12:24:46	2.29 MB	•	26. 4. 2012 13:25:46
301	pdf	http://web.fai.utb.cz/cs/docs/EUROCORES.pdf	•	26. 4. 2012 12:24:29	992.78 KB	•	26. 4. 2012 13:25:45
294	pdf	http://web.fai.utb.cz/cs/docs/Smericka_dekana_pro_hodnoceni_ped_aktivni.pdf	•	26. 4. 2012 12:24:15	704.26 KB	•	26. 4. 2012 13:25:44
286	pdf	http://web.fai.utb.cz/cs/docs/VD_01_10_sig.pdf	•	26. 4. 2012 12:23:52	267.36 KB	•	26. 4. 2012 13:25:43
281	pdf	http://web.fai.utb.cz/cs/docs/SD_03_08_sig.pdf	•	26. 4. 2012 12:23:38	1.12 MB	•	26. 4. 2012 13:25:42

Obrázok 5.14: Použitie nástroja FOCA – údaje o sieťovej infraštruktúre 4

Ďalej bol taktiež použitý nástroj Maltego, pričom prvým záchytným bodom bolo vyhľadávanie v rámci domény web.fai.utb.cz a ďalej podľa potrieb s cieľom získať podobné informácie ako s nástrojom FOCA, ale v tomto prípade je možné vidieť aj samotné prepojenie medzi jednotlivými nájdenými údajmi, čo je ilustrované na obrázku 5.15. Boli zistené aj telefónne čísla či emailové kontakty a taktiež čiastočné odhalenie sieťovej infraštruktúry či použitých technológií.

Nakoľko je Fakulta aplikovanej informatiky verejný inštitúcia, je pochopiteľné, že sa na webových stránkach fakulty nachádza pomerne veľké množstvo zverejnených informácií, ale na základe preverenia možno toto zverejnenie hodnotiť ako uspokojivé.



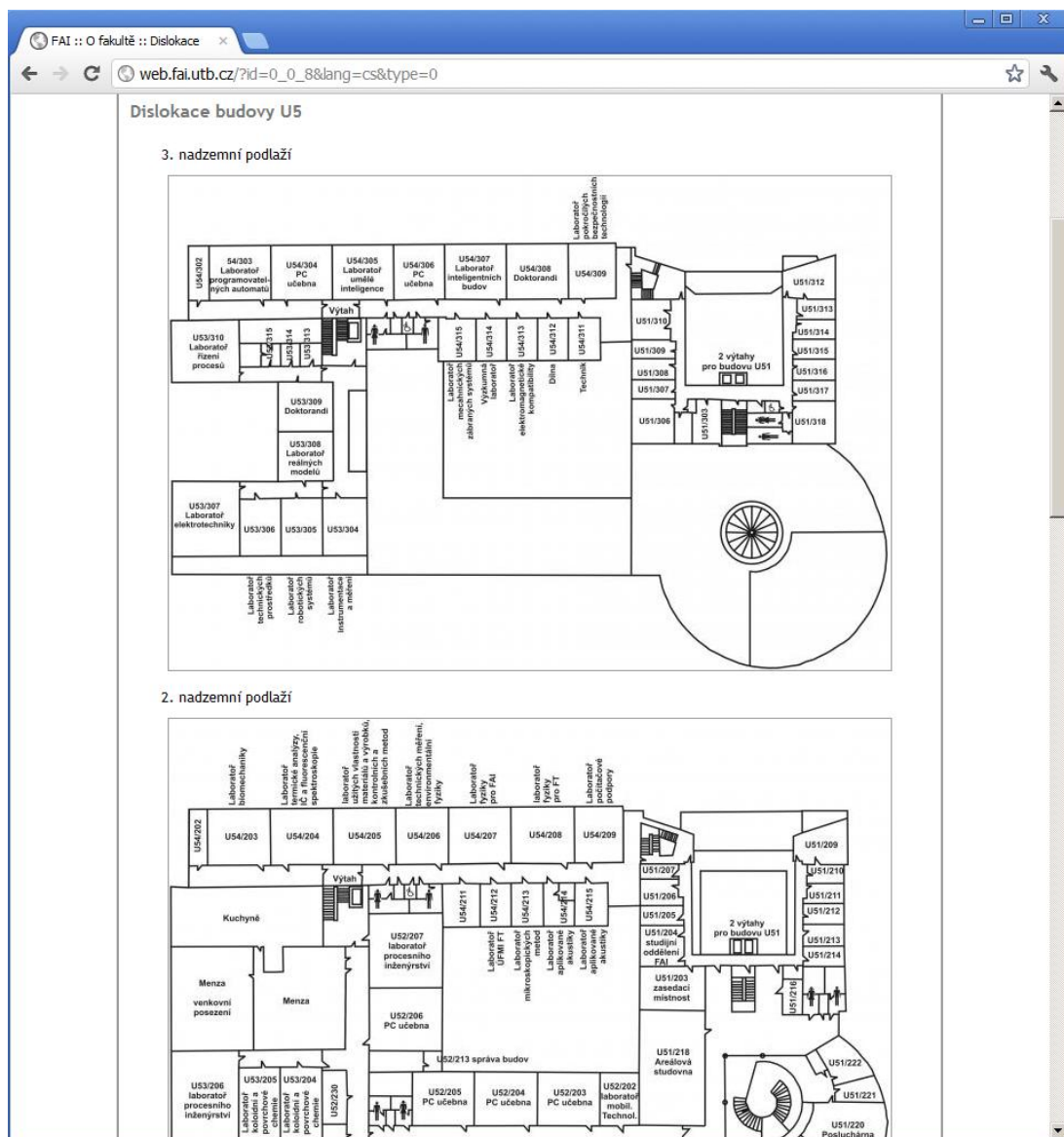
Obrázok 5.16: Informácie z webovej stránky `web.fai.utb.cz`

5.5 Scenár č. 5 – Test fyzického prieniku do organizácie

Posledný test bol zameraný na pokus o fyzický prienik do organizácie. Nakoľko v rámci testovania modelových situácií nebolo možné použiť výsledky z reálnych testov, obzvlášť pri fyzickom testovaní ide vždy o veľmi citlivé informácie, sú v tejto časti práce prezentované možnosti použitia sociálneho inžinierstva v rámci FAI. Je potrebné zdôrazniť, že cieľom nebolo realizovať samotný test, nakoľko na to nebolo vydané žiadne povolenie.

Tak ako je spomenuté v predchádzajúcej kapitole, že fakulta je verejná inštitúcia, tak pohyb osôb nie je v priestoroch fakulty nijak kontrolovaný či monitorovaný a vstup do priestorov fakulty je bezproblémový. Na základe týchto skutočností by potenciálnym cieľom

útočníka v rámci fakulty mohla napríklad byť priamo samotná miestnosť kde sú umiestnené servery. V predchádzajúcej kapitole sú uvedené informácie, ktoré si útočník môže zistiť napríklad z webových stránok a ďalej využiť pri prípadnej realizácii fyzickom útoku. Jednou z informácií, ktoré sú dostupné je aj plán s rozmiestnením miestností, obrázok 5.17.



Obrázok 5.17: Plán s rozmiestnením miestností z webovej stránky web.fai.utb.cz

Hlavne obrázky s popisom miestností môžu byť pre útočníka zaujímavé, nakoľko si dokáže aj bez predchádzajúceho pohybu v priestoroch FAI vytvoriť obraz a lepšiu predstavu o tom, kde hľadať miestnosť so servermi. Nakoľko sa útočník môže voľne pohybovať po budove, môže si overiť, či napr. miestnosť U51/204 je skutočne študijné oddelenie FAI.

Pomocou prehliadania webových stránok si útočník môže vyselektovať jednotlivé miestnosti, ktoré by potenciálne mohli byť práve tie, v ktorých sa nachádzajú servery, napr. miestnosti U51/205,206,207 či iné a odlíšiť ich od tých, ktoré slúžia ako kancelárie zamestnancov.

Na obrázku nižšie je možné si v pozadí všimnúť, že na Informáciách je uložené pomerne veľké množstvo kľúčov. Nakoľko nie sú známe bezpečnostné pravidlá v rámci fyzickej bezpečnosti konkrétnej miestnosti so servermi, teda či kľúče od tejto miestnosti má len zodpovedná osoba, alebo či sa na Informáciách nachádzajú kľúče aj od miestnosti so servermi, a taktiež nebolo naším cieľom to zisťovať, možno poukázať iba na to, že v prípade, že sa kľúče od serverovne nachádzajú na Informáciách a ich výdaj závisí iba od jedného človeka, možno konštatovať, že takáto situácia by mohla byť jednou z príležitostí, vďaka ktorým sa útočník môže dostať k svojmu cieľu. V prípade vyhodnotenia tejto situácie, by bolo potrebné realizovať reálny test, prípadne posúdiť existujúce bezpečnostné opatrenia, napríklad či je výdaj kľúčov registrovaný a pod kontrolou, alebo nie.



Obrázok 5.18: INFORMÁCIE na FAI UTB ve Zlíně

6 NÁVRH BEZPEČNOSTNEJ POLITIKY PRE IDENTIFIKÁCIU, PREVENCIU A OCHRANU PRED ÚTOKMI SOCIÁLNYM INŽINIERSTVOM

Väčšinu netechnických útokov sociálny inžinier realizuje fyzickým kontaktom so svojou obeťou a preto je všeobecne vhodné, aby práve pravidlá a opatrenia v rámci fyzickej bezpečnosti zabránili vstupu a pohybu útočníka v priestoroch organizácie obeti, prípadne bol tento vstup a pohyb neustále kontrolovaný a pod dohľadom. Je to prvá línia obrany a okrem vhodných technologických bezpečnostných systémov, je potrebné aby nielen perimenter fyzickej bezpečnosti bol na dostatočnej úrovni, ale aby sa hlavne minimalizovalo zlyhanie ľudského faktora, vo forme nedodržiavania pravidiel či ľahostajnému prístupu ľudí k bezpečnosti. V prípade technických útokov je najvhodnejším spôsobom ochrany dodržiavanie zavedených pravidiel, ktoré sú priamo orientované na to, aby predchádzali zlyhaniu ľudského faktora. Práve minimalizovanie zlyhania ľudského faktora je možné taktiež ovplyvniť pravidelným zvyšovaním bezpečnostného povedomia, a to formou bezpečnostných školení, ktoré sú zameraná na informačnú bezpečnosť či zvládnutie základov identifikácie útokov sociálnym inžinierstvom. V nasledovných kapitolách je poskytnutý návrh identifikácie útokov, prevencie a ťažiskových bodov bezpečnostnej politiky zameranej na ochranu pred útokmi sociálnym inžinierstvom, ktorý sa hlavne opiera o literatúru od najznámejšieho sociálneho inžiniera Kevina Mitnicka. [18]

6.1 Identifikácia útokov

Na to aby boli zamestnanci pripravení identifikovať a odhaliť útoky vedené sociálnym inžinierstvom, je potrebné aby boli oboznámení s informáciami, ktoré sa týkajú spôsobov realizácie všetkých útokov sociálnym inžinierstvom – netechnickým aj technickým spôsobom a akýmkoľvek komunikačným kanálom.

Jednotlivé fázy sociálneho inžinierstva môžu byť pre bežného zamestnanca pomerne ťažké identifikovateľné, ale je možné vyčleniť pár základných bodov, ktoré môžu vzbudiť v zamestnancoch podozrenie. Medzi tieto body patria:

- útočník má pomerne široké znalosti o štruktúre organizácie či zamestnaneckej hierarchie
- útočník spomína veľa mien, ktoré obeť pozná

- útočník žiada naliehavo o pomoc, prípadne tlačí na obeť vyhrážaním sa autoritou
- útočník žiada o podozrivo citlivé informácie a činnosti

Ďalej je potrebné aby zamestnanci poznali typické sociotechnické techniky, ktoré sú uvedené v kapitole 1.2.2, samozrejme medzi spomenutými technikami môžu byť aj také, ktoré nemusia vzbudzovať podozrenie, ale je potrebné aby boli zamestnanci obozretní, nakoľko je určite zvláštne, ak obchodný zástupca dodávateľa žiada informácie, ktoré nepotrebuje.

6.1.1 Varovné náznaky napadnutia

Ďalšími znakmi, ktoré dokážu zamestnancom či obetiam pomôcť identifikovať útok sú príznaky uvedené nižšie a všetky majú spoločné to, že sú opakom správania a konania korektnej a pravdivej osoby, ktorá nekoná so zlým úmyslom:

- odmietnutie podať telefónne či mobilné číslo na ktoré možno pre preverenie zavolať
- vyhováranie sa na nezapamätanie si svojho vlastného ID zamestnanca
- neustále sa oháňanie autoritou, trestami či vyhrážkami
- neochota volajúceho odpovedať na otázky
- podozrivé komplimenty pre obeť či flirtovanie od cudzej osoby

6.1.2 Typické ciele a obeť útokov

Medzi typické ciele a obeť útokov sociálnym inžinierstvom patria typy osôb, ktoré:

- nepoznajú hodnotu informácií, ktoré poznajú – personál na recepcii, asistenti, administratívni pracovníci, telefónny operátori
- majú privilegované a zvláštne práva – zamestnanci technickej podpory, správcovia počítačových sietí a serverov
- pracujú na zaujímavom oddelení plnom rôznych informácií – ekonomické oddelenie, personálne oddelenie

Netreba zabúdať na to, že nie len títo zamestnanci sú zamestnanci sú pre útočníka zaujímaví, ale každý jeden zamestnanec, ktorý disponuje nejakými zaujímavými, citlivými a dôvernými informáciami nesie v sebe potenciál stať sa obeťou sociálneho inžiniera.

6.2 Prevencia

Prevencia pred útokmi sociálnym inžinierstvom spočíva hlavne v pravidelnom zvyšovaní bezpečnostného povedomia a to formou školení, hlavne s ohľadom poučenia zamestnancov o hodnote informácií, ktorými disponujú, zaškolení, ako ich majú ochraňovať a v upovedomení ich o tom, ako sociálni inžinieri pracujú a realizujú svoje útoky. Informovanie zamestnancov o existencii sociálneho inžinierstva, by malo byť určite vykonávané nielen v pravidelných intervaloch ale aj individuálne pri nástupe nového zamestnanca do zamestnania.

Realizácia školení však niekedy nestačí a preto je nevyhnutné aby v rámci organizácie bol zavedený systém účinných opatrení, ktorý by znižoval zlyhanie ľudského faktora a tým pádom aj riziko bezpečnostného incidentu pri útoku sociálnym inžinierstvom. V rámci bezpečnostných pravidiel ide o správanie sa na pracovisku, napríklad v podobe vnútorných predpisov, na základe ktorých by zamestnanec vnímal tieto pravidlá ako záväzné a vďaka ktorým by bolo možné vyžadovať ich dodržiavanie alebo postihovať ich porušenie. Malo by byť v záujme samotnej organizácie aby takýto systém pravidiel na pracovisku existoval, a aby sa trvalo nie len na jeho dodržiavaní ale aj na jeho pravidelných kontrolách dodržiavania či aktuálnosti.

Samotný obsah školení by mal byť orientovaný na základný prvok sociálneho inžinierstva a tým je zmanipulovať obeť a podvodom dosiahnuť cieľ. Pri situácii, kedy si útočník vytvorí dôverný vzťah s obeťou a poskytne jej falošný pocit bezpečia, je obeť presvedčená o tejto nepravej dôvere natoľko, že je presvedčená, že útočník je kolega z práce alebo iná osoba, ktorá ma oprávnenie pristupovať k dôverným a citlivým informáciám a nemá problém mu ich aj poskytnúť. Takýto útok by mohol byť eliminovaný skoro vždy, ak by obeť dodržala dva bezpečnostné kroky:

- Overenie totožnosti osoby, ktorá o niečo žiada, či je naozaj tým za koho sa vydáva.
- Overenie, či je osoba oprávnená získať požadované informácie a či ich skutočne potrebuje.

Osnova školenia by mohla byť ďalej napríklad orientovaná nasledovnými bodmi:

- Popis, ako útočníci používajú metódy sociálneho inžinierstva, aby oklamali ľudí.
- Metódy, ktoré útočníci používajú, aby dosiahli požadovaný cieľ.

- Spôsoby rozpoznávania útoku sociálnym inžinierstvom.
- Ako postupovať v prípade podozrenia, že ide o útok sociálnym inžinierstvom.
- Informácie o tom, kde sa majú hlásiť pokusy alebo úspešné útoky.
- Upozornenie na nutnosť overovania každej osoby, ktorá prišla s podozrivou žiadosťou, nezávisle na jej postavení v hierarchii organizácie.
- Skutočnosť, že by sa nemalo veriť nijakej osobe bez zodpovedajúceho overenia.
- Úloha identifikácie osoby, ktorá žiada o informácie, alebo vykonanie nejakej činnosti.
- Procedúry ochrany citlivých informácií vrátane vedomostí existujúceho systému klasifikácie dát.
- Miesto, kde sú umiestnené bezpečnostné postupy a pravidlá, a ich úloha v procese ochrany informácií a informačných systémov.
- Zhrnutie bezpečnostnej politiky a vysvetlenie významu jednotlivých aspektov.
- Povinnosť prispôbiť sa pokynom bezpečnostnej politiky a dôsledky v prípade ich nedodržania.

V neposlednom rade je ďalšou formou prevencie pred útokmi sociálnym inžinierstvom realizácia bezpečnostných testov, pri ktorých sa skutočne preverí funkčnosť bezpečnostných pravidiel a ich dodržiavanie. V prípade nálezu zraniteľnosti možno túto zraniteľnosť zaradiť medzi príklady útokov prezentované na školení a vzniknutý incident zdôrazniť.

6.3 Bezpečnostná politika

Bezpečnostná politika sa skladá z jasne definovaných pravidiel, ktoré popisujú smernice týkajúce sa správania zamestnancov za účelom ochrany informácií, zníženia rizika zlyhania ľudského faktora a sú základným prvkom systému ochrany pred potenciálnymi hrozbami. Najdôležitejšou úlohou týchto pravidiel je pomoc pri identifikácii útokov založených na sociálnom inžinierstve a zabezpečení ochrany pred týmito útokmi. Treba však pamätať na to, že aj napriek všetkým odporúčaniam, dokonca aj keď sú dôsledne dodržiavané všetkými zamestnancami, nezaručujú stopercentnú ochranu pred všetkými útokmi sociálnym inžinierstvom.

Reálnym cieľom opatrení by malo byť zníženie rizika úspešnosti útoku a zvýšenie potenciálu odhalenia útoku samotným zamestnancom. V nasledujúcich kapitolách sú tiež

uvedené pravidlá popisujúce opatrenia, ktoré priamo nesúvisia so sociálnym inžinierstvom ale sú prepojené s technikami realizovanými v rámci útokov sociálnym inžinierstvom. Napríklad ide o pravidlá týkajúce sa tvorby bezpečných hesiel.

Pri návrh pravidiel v rámci organizácie je vhodné sa taktiež opierať o medzinárodnú normu ISO/IEC 27001, ktorej úlohou je zriadiť, implementovať, prevádzkovať, monitorovať, preskúmať, udržiavať a zlepšovať informačnú bezpečnosť.

Dôležitosť vytvorenia bezpečnostných pravidiel a opatrení reflektuje aj fakt, že z realizovaného dotazníku, ktorý je spomenutý v kapitole 4, vyplýva, že nie každej organizácii existujú bezpečnostné opatrenia pred útokmi sociálnym inžinierstvom, príloha A.2.

6.3.1 Klasifikácia dát

Politika klasifikácie údajov, informácií a dát predstavuje základ ochrany firemných informácií a určuje kategórie, ktoré určujú spôsob poskytovania dôverných informácií. Ide o hlavnú časť ochrany firemných dát a určuje zamestnancom jednotlivé stupne citlivosti každej informácie a aké overovanie je potrebné pri žiadosti o dané údaje, informácie a dáta.

Kategória: Verejné

Popis: Údaje, informácie a dáta verejne dostupné.

Overovanie: Nie je potrebné žiadne overovanie.

Kategória: Interné

Popis: Údaje, informácie a dáta určené pre vnútorné potreby organizácie s možnosťou zverejnenia tretím stranám – dodávateľom, obchodným partnerom. (organizačná štruktúra, vnútorné telefónne čísla, názvy vnútorných systémov, atď.)

Overovanie: Potreba overiť totožnosť žiadateľa, či ide o zamestnanca organizácie, v prípade tretích strán overiť totožnosť žiadateľa, platnosť zmluvy o mlčanlivosti a súhlas vedenia o poskytnutí.

Kategória: Privátne

Popis: Údaje, informácie a dáta určené výhradne pre vnútorné potreby organizácie. (osobné identifikačné údaje zamestnancov, história výplat, atď.)

Overovanie: Potreba overiť totožnosť žiadateľa, či ide o zamestnanca organizácie, pred poskytnutím musí byť súhlas osoby zodpovednej za dané aktívum.

Kategória: Tajné

Popis: Údaje, informácie a dáta, ktoré možno poskytnúť iba osobám v rámci organizácie s absolútnou potrebou ich znalostí. (obchodné tajomstvá, zdrojové kódy, know-how, marketingové a finančné plány, atď.)

Overovanie: Potreba overiť totožnosť žiadateľa, či ide o zamestnanca organizácie, pred poskytnutím musí byť písomný súhlas vlastníka aktíva alebo priameho nadriadeného, potreba overiť existenciu písomného záväzku mlčanlivosti. Poskytovať takéto informácie ľuďom, ktorý nie sú vo firme zamestnaný môže iba osoba z manažmentu s písomným súhlasom minimálne jedného ďalšieho člena manažmentu.

6.3.2 Pravidlá autentifikácie

Aby sa zaistila efektívna ochrana aktív, musí zamestnanec, ktorý je vyzvaný k vykonaniu nejakej činnosti alebo k poskytnutiu citlivých informácií zrealizovať identifikáciu osoby, ktorá takúto žiadosť realizuje a overiť si, či má takáto osoba na toto konanie oprávnenie. Doporučené postupy by mali pomôcť zamestnancovi, ktorý dostáva žiadosť akýmkoľvek komunikačným kanálom pri realizovanej kontrole a overovaní.

Kategória: Autentifikácia dôveryhodnej osoby

Overovanie: Kontrola, či je osoba v súčasnosti zamestnancom alebo má nejaké väzby, ktoré by ju oprávňovali k prístupu k údajom, o ktoré žiada. Preverenie, či daná osoba túto informáciu naozaj potrebuje a či je oprávnená k nej pristupovať.

Kategória: Autentifikácia neoverenej osoby

Overovanie: Identifikácia a overenie osoby, či je skutočne tým, za koho sa vydáva. Kontrola, či je pýtajúci vo firme v súčasnosti zamestnaný alebo k nej má nejaký vzťah, ktorý by vysvetľoval potrebu získať informáciu. Zistenie, či má daná osoba oprávnenia, aby danú informáciu dostala, alebo aby pre ňu bola vykonaná určitá činnosť.

Ďalej sú uvedené spôsoby, pomocou ktorých možno realizovať vyššie uvedené overovanie a pri každej je taktiež uvedená zraniteľnosť a spôsob, akým ju sociálny inžinier môže zneužiť.

Overenie totožnosti a identity:

- Identifikácia volajúceho: uistiť sa na displej telefónu, ak je to možné, či je telefonát z vnútorného okruhu organizácie, alebo zvonku a či číslo zodpovedá menu, ktoré volajúci uviedol. Zraniteľnosť: možnosť použiť Caller-ID alebo SMS spoofing.
- Spätné volanie: preverenie si volajúceho v telefónnom zozname a vykonanie spätného telefonátu, pre overenie, či ide o zamestnanca organizácie. Zraniteľnosť: útočník s príslušnými znalosťami môže presmerovať hovor z danej vnútornej linky. Potom volania na vnútornú linku spôsobí presmerovanie hovoru na vonkajšie číslo útočníka.
- Spoločné tajomstvo: použitie vnútorného spoločného tajomstva v rámci organizácie, napríklad heslá alebo denného kódu. Zraniteľnosť: ak spoločné tajomstvo pozná veľa ľudí, môže byť jeho zistenia pre útočníka veľmi ľahké.
- Vedúci či nadriadený volajúceho: overenie si volajúceho u nadriadeného či vedúceho zamestnanca. Zraniteľnosť: ak volajúci číslo svojho nadriadeného uviedol sám, potom osoba, ktorej sa obeť dovoľá, nemusí byť v skutočnosti jeho šéfom, ale spoločník útočníka.
- Overovací email: vyžiadať si emailovú správu, prostredníctvom ktorej sa potvrdí identita zamestnanca podpisom GPG kľúča. Zraniteľnosť: útočník môže s príslušnými znalosťami poslať email so sfaľšovanou hlavičkou emailu.
- Identifikácia hlasu: osoba, ku ktorej je smerovaná žiadosť, a mala možnosť sa stretnúť s volajúcou osobou, by mala rozpoznať jej hlas v telefóne. Zraniteľnosť: je to dosť bezpečná metóda, ktorá sa nedá ľahko obísť. Nemožno ju však použiť v situácii, keď sa človek prijímajúci telefón nikdy s volajúcim nestretol a ani s ním nikdy nehovoril.

- Dynamické heslá: žiadateľ sa identifikuje pomocou technológie dynamického hesla. Zraniteľnosť: aby útočník toto zabezpečenie obišiel, musí sa dostať k jednému z identifikačných zariadení a k jemu priradenému PIN kódu vlastníka alebo zmanipulovať zamestnanca tak, aby mu prečítal PIN kód zo svojho zariadenia a oznámil svoje PIN ako prvý.
- Osoba s identifikátorom: osoba, ktorá k nám vznáša žiadosť, sa objavuje osobne a preukazuje sa identifikátorom zamestnanca alebo kartičkou s fotografiou. Zraniteľnosť: útočník je schopný ukradnúť identifikátor zamestnancovi alebo si vytvoriť falošný identifikátor, ktorý vyzerá dôveryhodne a presvedčivo.

Overenie oprávnenia prístupu k aktívam:

- Pri overovaní je taktiež potrebné realizovať overenie, či osoba, ktorá požaduje prístup k informáciám má oprávnenie pristupovať k týmto informáciám, alebo oprávnenie k vykonávaniu činností o ktoré žiada. Takúto kontrolu možno vykonať pomocou nasledovných krokov:
- vytvorenie zoznamu, ktorý popisuje oprávnenia jednotlivých zamestnancov voči aktívam organizácie a následné sprístupnenie vo vnútri organizácie, je ale dobré pamätať na to, že práve získanie takéhoto dokumentu môže byť pre sociálneho inžiniera veľmi zaujímavé
- získanie oprávnenia od nadriadené prostredníctvom žiadosti a následné preukázanie sa podpísaným potvrdením o oprávnení
- získanie a preukázanie oprávnenia od vlastníka aktíva či zodpovednej osoby, taktiež prostredníctvom písomného potvrdenia

Na záver je potrebné upozorniť, že osobné identifikačné údaje ako sú napríklad zamestnanecké identifikačné číslo, číslo občianskeho preukazu, rodné číslo, dátum a miesto narodenia a iné by nikdy nemali slúžiť ako prostriedky overovania totožnosti, nakoľko tieto údaje je možné získať mnohými rôznymi spôsobmi.

6.3.3 Manažment

Nasledujúce pravidlá sa týkajú vedúcich pracovníkov a vrcholového manažmentu v organizácii a spočíva v zodpovednom prístupe k nasledujúcim bodom:

- navrhnúť a zaviesť bezpečnostnú politiku - pravidlá do života organizácie

- stanovenie rolí a zodpovednosti za informačnú bezpečnosť, vytvorenie skupiny alebo určenie osoby, ktorej budú zamestnanci môcť nahlásiť podozrenie či zistený bezpečnostný incident
- vytvoriť nezávislé podmienky a prostredie pre zaistenie pravidelnej realizácie bezpečnostných testov zameraných na všetkých zamestnancov – od najnižších pracovných pozícií až po vrcholové, následné vyhodnotenie testov a okamžité prijatie navrhovaných opatrení
- oboznámenie všetkých zamestnancov organizácie o dôležitosti dodržiavania politiky informačnej bezpečnosti
- oboznámenie všetkých zamestnancov so zoznamom, ktorý popisuje oprávnenia jednotlivých zamestnancov voči aktívam
- udržiavať a zvyšovať bezpečnostné povedomie všetkých zamestnancov organizácie prostredníctvom pravidelných bezpečnostných školení
- zavedenie klasifikácie dát do praxe s pravidelným intervalom kontroly dodržiavania
- definovať bezpečnostné pravidlá pre jednotlivé oddelenia v rámci organizácie, s ohľadom na potreby a prácu ktorá sa vykonáva v rámci oddelenia

6.3.4 Ľudské zdroje

Personálne oddelenie a riadenie ľudských zdrojov má osobitnú úlohu v oblasti informačnej bezpečnosti, nakoľko je jej povinnosťou chrániť pracovníkov pred osobami, ktoré sa pokúšajú získať osobné údaje zamestnancov a taktiež zodpovednosťou za ochranu organizácie pred pred napríklad nespokojnými bývalými zamestnancami, či nástupom zamestnancov, ktorí by chceli poškodiť organizáciu. Bezpečnosť ľudských zdrojov možno definovať dvomi bodmi, uvedené nižšie, v rámci ktorých sú uvedené jednotlivé návrhy opatrení.

Bezpečnosť ľudských zdrojov pred nástupom do a počas zamestnania:

- pri prijímaní nového zamestnanca si overiť pravosť jeho životopisu a hlavne uvádzaných referencií
- zmluvne presne definovaná pracovná náplň, podmienok a zodpovednosti za zverené aktíva a taktiež oboznámenie o postihoch vyplývajúcich z nedodržania zodpovednosti, ochrany aktív či napríklad mlčanlivosti

- existencia disciplinárnych opatrení pri spôsobení narušenia bezpečnosti organizácie
- zabezpečenie vstupného preškolenia so zameraním na informačnú bezpečnosť a zavedené vnútorné pravidlá
- pridelenie potrebných oprávnení novému zamestnancovi a zaradenie do zoznamu, ktorý popisuje oprávnenia jednotlivých zamestnancov voči aktívam
- všetci zamestnanci vrátane manažmentu sú povinní nosiť nosiť identifikátory na viditeľnom mieste

Bezpečnosť ľudských zdrojov pri ukončení alebo zmeny pracovného pomeru:

- personálne oddelenie je zodpovedné za odstránenie zamestnanca zo zoznamu zamestnancov, rovnako aj z telefónneho zoznamu
- je potrebné upovedomiť oddelenie informačných technológií o potrebe deaktivácii všetkých možných prístupov do siete a systémov organizácie – prístup do sieťových zariadení, databáz, elektronickej pošty
- zabezpečenie odovzdania všetkých aktív v takom stave ako boli zamestnancovi zverené
- informovať personál na vrátnic o zmene stavu zamestnanca a informovať o tejto udalosti aj celé oddelenie
- pri zmene pracovného pomeru, všetky vyššie body aplikovať s ohľadom zmeny, to znamená, že ak sa zmenou pracovného pomeru zmenia oprávnenia k aktívam, je napríklad potrebné o tom informovať ostatných zamestnancov

6.3.5 Informačné a komunikačné technológie

Oddelenie zodpovedné za informačné a komunikačné technológie či technickú podporu musí mať definované pravidlá takým spôsobom, aby svojou činnosťou pomáhalo pri ochrane informačných aktív organizácie. Návrh opatrení, ktoré sú orientované na informačné a komunikačné technológie sú taktiež opatrenia týkajúce sa používania informačných zariadení všetkými zamestnancami, nakoľko je potrebné, aby sa samotný používatelia správali bezpečne. Jednotlivé návrhy opatrení sú rozčlenené užšie oblasti, ktorých sa týkajú.

6.3.5.1 Pravidlá pre oddelenie informačných technológií

- kontaktné údaje – telefónne čísla či emailové adresy, by nemali byť poskytované žiadnej osobe, ktorá nemá konkrétny dôvod na to, aby ich poznala
- všetky požiadavky o technickú pomoc musia byť delegované na oddelenie určené pre technickú podporu
- nie je povolené deaktivovať alebo aktivovať sieťové zásuvky na základe žiadosti od neoverenej osoby, na vykonanie takejto činnosti je potrebné písomný príkaz nadriadeného zamestnanca alebo vlastníka aktíva
- zamestnanci, ktorí majú privilegované účty nesmú zadávať žiadne príklady a spúšťať programy na žiadosť neoverených osôb a taktiež osôb, ktoré osobne nepoznajú

6.3.5.2 Pravidlá pre oddelenie technickej podpory

- zamestnanci technickej podpory nesmú poskytovať informácie o spôsobe a možnostiach vzdialeného pripojenia sa do vnútornej siete, alebo spôsoboch pripojenia k vnútornej bezdrôtovej sieti pokiaľ osoba požadujúca tieto informácie nebola overená ako oprávnená a dôveryhodná osoba
- zmena hesla môže byť vykonaná iba pri žiadosti konkrétneho zamestnanca, ktorý bol overený prostredníctvom spätného telefonátu na telefónne číslo, uvedené v zozname organizácie
- zmena prístupových práv, vytvorenie nového konta alebo blokovanie konta môže byť vykonaná iba vtedy, ak existuje písomne schválená žiadosť vedúcim či nadriadeným zamestnancom alebo vlastníkom aktíva
- pridelenie nového hesla je potrebné považovať za tajnú informáciu a jeho doručenie musí byť zabezpečené iba bezpečnou cestou – osobne alebo v zapečatenej obálke
- zamestnanci, ktorí majú privilegované účty nesmú zadávať žiadne príklady a spúšťať programy na žiadosť neoverených osôb a taktiež osôb, ktoré osobne nepoznajú

6.3.5.3 *Správa systémov a sietí*

- vytvorenie vzdialeného prístupu pre zamestnanca možno zriadiť iba pri písomnej žiadosti nadriadeného zamestnanca a v súlade s overovacími pravidlami, v prípade prístupu pre externého technika je nutné overiť identitu osoby, ktorá žiada o vstup do systému a po ukončení práce je okamžite nutné na danom účte zmeniť heslo
- zmena hesiel privilegovaných účtov môže byť zrealizovaná iba po schválení konkrétnym vlastníkom aktíva
- všetky prístupové miesta k internej sieti musia byť chránené účinnými overovacími mechanizmami
- je potrebné sledovať vydanie aktualizácií používaných operačných systémov a softvérového vybavenia a aktualizácie vždy pri vydaní ihneď nainštalovať
- internetová stránka určená pre verejnosť by nemala obsahovať žiadne podrobnosti týkajúce sa štruktúry firmy, náčrty plánikov rozmiestnenia kancelárií a ani uvádzať mená svojich zamestnancov
- všetky údaje, ktoré sa nachádzajú mimo organizáciu by mali byť zašifrované
- sieťové zásuvky by sa mali používať v takom množstve aké je potrebné pre pripojenie zaradení na danom pracovisku, napríklad pre počítač a sieťovú tlačiareň sú potrebné iba dve sieťové zásuvky
- každý operačný musí mať nainštalovaný a aktualizovaný antivírusový program
- každý operačný systém musí mať zapnutý firewall
- v prípade dodržiavania vysokých požiadavkov na bezpečnosť je potrebné aby hraničný sieťový firewall filtroval všetky prílohy v prichádzajúcich emailoch
- je nutné pre všetky operačné systémy alebo hardvérové zariadenia, ktoré majú implicitné heslo, okamžite zmeniť heslo podľa politiky hesiel
- v prípade výskytu neúspešných pokusov o prístup na akýkoľvek účet mal by sa tento účet po určitom počte pokusov pozastaviť
- všetky počítačové systémy musia byť nakonfigurované tak, aby pri štarte vyžadovali bootovacie heslo

- všetci používatelia bezdrôtového pripojenia by mali pri prístupe do siete používať technológiu VPN
- je nutné vytvoriť samostatnú bezdrôtovú sieť určenú pre návštevníkov, ktorí k prihláseniu do tejto siete obdržia prihlasovacie údaje, ktoré budú obmedzené časovým vyexpirovaním

6.3.5.4 Politika hesiel

- v rámci organizácie sa musí dodržiavať politika hesiel
- prideľovanie hesiel realizuje vedúci zamestnanec informačných technológií
- heslo musí mať minimálne 10 znakov, heslo musí obsahovať aspoň jedno veľké písmeno a jednu číslicu, v prípade hesiel pre privilegované účty musí byť heslo minimálne 12 znakové
- expiračná doba nesmie byť dlhšia ako 12 mesiacov a heslo nesmie byť opakovane použité 3 x po sebe, teda jedno heslo možno použiť až po 3 expiračných cykloch
- heslá privilegovaných účtov by sa mali meniť minimálne každých 30 dní
- heslo nesmie obsahovať takú kombináciu znakov, ktorú by bolo možné priradiť k jeho osobe, akými sú napríklad meno používateľa a jeho rodinných príslušníkov napísané spredu či odzadu, telefónne číslo domov alebo na pracovisko a podobne, príklad správneho hesla je „u1cLt4Re0x“
- prvé heslo pre zamestnancov by malo byť nastavené ako expirované, aby si každý zamestnanec pri prvom prihlásení zmenil heslo
- je zakázané používať rovnaké heslo do viacerých počítačových systémov alebo emailových schránok
- zamestnanci nesmú nikdy prezradiť svoje heslo, či heslá ktoré im boli zverené bez predchádzajúceho súhlasu nadriadeného vedúceho zamestnanca z oddelenia informačných technológií
- je zakázané zapisovať si heslá na voľne viditeľné miesta v rámci svojho pracovného priestoru, heslá možno zaznamenávať iba vtedy, ak sú bezpečne uschované mimo blízkosti počítača

- je zakázané heslá ukladať do textových editorov v počítači, v prípade nutnosti je možné heslá ukladať prostredníctvom šifrovaného nástroj schváleného vedúcim zamestnancom informačných technológií

6.3.5.5 Používanie osobných počítačov a notebookov

- každý zamestnanec nesmie zadávať príkazy a spúšťať programy na svojom počítači na žiadosť cudzích osôb, aj keď sa zdá, že žiadosť je opodstatnená, túto činnosť možno vykonať len so súhlasom nadriadeného
- používatelia nesmú poskytovať žiadne informácie o systémoch alebo zariadeniach, ktoré sa v organizácii používajú, bez toho aby si overili identitu osoby, ktorá takéto informácie požaduje
- všetky elektronické médiá, ktoré obsahujú citlivé, dôverné či tajné informácie musia byť fyzicky zabezpečené na bezpečnom mieste
- všetky záložné kópie musia byť uložené v trezore organizácie
- zamestnanci organizácie nesmú sťahovať a inštalovať softvér na žiadosť cudzích osôb, ak nie sú identifikovaní ako zamestnanci informačných technológií
- je zakázané používať v pracovnej dobe sociálne siete a kedykoľvek na nich zverejňovať akékoľvek interné informácie alebo informácie týkajúce sa organizácie
- všetci zamestnanci musia mať nastavené pri šetriči obrazovky heslo a nastavenú aktiváciu šetriču po určitej dobe
- je zakázané vkladať do počítača alebo notebooku nájdené či neznáme optické médiá a pripájať USB kľúče, ktorých identitu nepoznáme a je potrebné takéto prenosné médiá odovzdať na oddelení informačných technológií
- odporúča sa zakázať na všetkých počítačoch používanie USB portov a povoliť ich používanie iba v prípade potreby v rámci daného oddelenia

6.3.5.6 Používanie elektronickej pošty

- každé oddelenie musí mať vytvorenú emailovú adresu, ktorá bude slúžiť na komunikáciu so svetom

- kontaktné údaje pri vlastníkovi domén by mali byť vo obecnej forme napríklad *admin@organizacia.com*
- algoritmus tvorenia používateľských mien je potrebné považovať za citlivú informáciu a ja zakázané tento algoritmus poskytovať cudzím osobám bez predchádzajúceho overenia identity
- prílohy v emailových správach sa nesmú otvárať, pokiaľ nie sú očakávané a nepochádzajú od známych a dôveryhodných osôb
- preposialanie emailov na základe požiadaviek cudzích osôb je zakázané
- emailovú správu, ktorá sa zdá byť dôveryhodná, ale obsahuje žiadosť o poskytnutie dôverných informácií alebo vykonanie rôznych činností na počítači, je potrebné preveriť a identifikovať osobu od ktorej pochádza

6.3.5.7 Používanie telefónov, hlasových schránok, faxu a mobilných zariadení

- zamestnanci nesmú odpovedať na otázky v rámci telefonických prieskumov alebo otázky osôb mimo organizácie, všetky takéto žiadosti je potrebné smerovať na oddelenie PR
- je zakázané poskytovať telefónne čísla zamestnancov neovereným osobám, pri identifikácii osoby a poskytnutí dôkazu, že je to skutočne nutné, možno poskytnúť telefónne číslo
- zanechávanie hesiel v hlasových schránkach je zakázané
- bez overenia totožnosti je prijímanie a posielanie faxov neznámym osobám zakázané
- pred vykonaním akýchkoľvek činností obdržaných vo faxe musí byť odosielateľ identifikovaný ako zamestnanec organizácie
- je zakázané posielat' heslá prostredníctvom faxov
- pri nahrávaní úvodných odkazov v hlasovej schránke sa neodporúča udávať informácie o spojené s pracovnou cestou či rozvrhom dňa
- je zakázané odovzdávať tajné a dôverné informácie prostredníctvom hlasovej schránky
- je zakázané sa pripájať s mobilnými zariadeniami, ktoré boli zamestnancovi pridelené na verejne dostupných bezdrôtových sieťach

- zakazuje sa vstup osôb s mobilnými zariadeniami do priestorov, kde sú umiestnené servery, vstup s mobilnými zariadeniami je možný iba s písomným povolením vedúceho zamestnanca oddelenia informačných technológií
- je zakázané vykonávať akékoľvek činnosti obdržané v SMS správach, pokiaľ nie sú očakávané, činnosti možno vykonávať až po realizácii spätného telefonátu

6.3.6 Fyzická bezpečnosť

V prípade opatrení pred fyzickým útokom na organizáciu je vhodné prijať nasledujúce navrhnuté opatrenia:

- V prípade opatrení pred fyzickým útokom na organizáciu je vhodné prijať nasledujúce navrhnuté opatrenia:
- identifikáciu osôb nezamestnaných v organizácii realizovať takým spôsobom, že sa zabezpečí pravidelná kontrola cudzích osôb, v prípade dodávateľov či iných osôb, ktorí v organizácii nie sú zamestnaní potrebujú pravidelne vstupovať do areálu či objektu organizácie je potrebné vyhotoviť špeciálne identifikátory, určené iba pre tieto osoby, aby sa odlišili od zamestnancov
- identifikácia návštevníkov musí prebiehať tak, že sa bude viesť evidencia osôb, ktorým bolo pridelené dočasné povolenie pre vstup do vnútra organizácie a toto povolenie bude mať pri sebe, napríklad formou identifikátora, ktoré bude na ich tele viditeľne umiestnené, zároveň sa nesmie návšteva nechať v rámci objektu bez dozoru
- pri čakaní návštevy na recepcii, je potrebné aby taktiež návštevník neostával bez dozoru, ale personál zodpovedný za recepciu bol vždy prítomný na recepcii a mal pod dohľadom svoje pracovisko
- rozčlenenie objektu organizácia na bezpečnostné zóny, pričom do týchto zón budú môcť vstupovať iba zamestnanci, ktorý budú mať na to oprávnenie, takáto identifikácia môže prebiehať napríklad prostredníctvom čipových kariet
- rozčlenenie areálu organizácie na väčšie zóny, kde sa definujú verejné priestory, priestory určené na expedíciu a prijímanie, priestory určené na prestávky zamestnancov a v každom vchode v rámci priestoru umožňujúci vstup do objektu bude monitorovaný a zabezpečený

- zamestnanci nesmú dovoliť aby za nimi do objektu vstúpila neznáma osoba, kým k otváraní vstupu používajú bezpečnostný identifikátor
- zavedenie pravidla, že každý zamestnanec je zodpovedný za fyzickú bezpečnosť svojho pracoviska a zverených mu pracovných prostriedkov, pri odchode z pracoviska je povinný uzamknúť pracovisko, uzavrieť okná a prekontrolovať zariadenia či nemôžu spôsobiť požiar alebo inú haváriu, ak zamestnanec nemôže túto povinnosť splniť oznámi to ihneď svojmu nadriadenému
- je potrebné viesť evidenciu, ktorej obsahom je zoznam zamestnancov, s presným popisom, aké kľúče a z akej časti organizácie majú zamestnanci pridelené, zároveň v prípade funkcie centrálného výdaju kľúčov je potrebné dodržiavať výdaj iba zamestnancom, ktorí majú na to povolenie, prípadne sa preukážu a overia prideleným povolením, ktoré je podpísané buď vedúcim zamestnancom alebo vlastníkom aktíva
- odpadkové koše musia byť po celú dobu iba v areály alebo objekte organizácie a nemali by byť voľne prístupné

6.3.7 Hlásenie bezpečnostných incidentov

Snahou každej organizácie by malo byť vytvorenie a zabezpečenie centrálnej skupiny, ktorej úlohou je slúžiť zamestnancom, v takých prípadoch akými sú prípadné odhalenia nejakej formy ohrozenia bezpečnosti organizácie, či zistenia vzniku bezpečnostného incidentu.

Každý zamestnanec by mal byť informovaný a vybavený kontaktnými údajmi o tom, kde je potrebné alebo komu je nutné oznámiť akékoľvek podozrenie či odhalenie ohrozenia, alebo vznik bezpečnostného incidentu narušujúceho bezpečnosť organizácie.

Ďalšou súčasťou pravidiel o hlásení bezpečnostných incidentoch sú pokyny pre skupinu alebo osobu, ktoré tieto informácie prijíma. V prípade, že sú oznámené podozrenia či zistenia o bezpečnostnom incidente je potrebné neodkladne varovať všetkých zamestnancov, ktorí patria do okruhu ohrozených a prijať všetky bezpečnostné opatrenia, ktoré zabránia rozšíreniu tohto incidentu. Taktiež sa odporúča zaznamenať údaje o incidente, pričom takýto záznam by mal napríklad obsahovať nasledovné body:

- dátum a čas zaznamenania a skončenia bezpečnostného incidentu
- opis spôsobu zistenia incidentu
- meno zamestnanca, ktorý incident ohlásil

- dátum a čas začiatku a ukončenia záchranného režimu
- chronologický opis priebehu incidentu a zistených udalostí
- zoznam dotknutých aktív s predpokladanou dobou obnovy
- zoznam opatrení a nariadení, ktoré boli porušené a mohli spôsobiť incident
- návrh na prijatie opatrení pre zamedzenie recidívy
- opis prijatých opatrení s dátum a podpisom, že skutočne došlo k prijatiu opatrení

ZÁVER

V oblasti informačnej bezpečnosti je sociálne inžinierstvo charakterizované ako netechnická forma prelomenia bezpečnostných postupov, a na základe tohto tvrdenia je možné, aby prostredníctvom útokov sociálnym inžinierstvom dokázal hocikto ohroziť bezpečnosť akejkolvek veľkej organizácie, ktorá používa aj najmodernejšie špičkové bezpečnostné technológie.

V práci sú zdokumentované metódy a techniky útokov sociálnym inžinierstvom a nástroje, ktoré možno pri útokoch sociálnym inžinierstvom použiť a zároveň je poskytnutý návrh opatrení voči týmto útokom. Na základe realizovaného dotazníka možno konštatovať, že z netechnických útokov má najväčší potenciál ohrozenia metóda Piggybacking a z technických útokov sú to metódy Caller-ID a SMS spoofing, Phishing, Pharming a Road apples. Z tohto dôvodu je pri využití sociálneho inžinierstva ako nástroja na testovanie informačnej bezpečnosti poskytnutý návrh na realizáciu konkrétnych testov, ktorými sú: phishingový test, telefonický test, test s prenosnými médiami, fyzický prienik do priestoru organizácie, prehľadávanie odpadkov a preverenie zverejnených informácií. Realizácia testov je založená na prezentovanej metodike, ktorá je postavená na identifikácii cieľov, preskúmaní, tvorbe predstieraných scenárov a vykonaní samotného útoku. Ďalšou časťou metodiky je spracovanie výsledkov vykonaných testov, pričom vďaka realizácii a výsledkom testov možno identifikovať potenciálne slabiny a zraniteľnosti v zabezpečení.

Na základe návrhov testov boli následne realizované testy modelových situácií. Prvým testom bol phishingový test, kde bola dosiahnutá 5 % úspešnosť. Podľa môjho názoru je aj 5 % veľa, nakoľko stačí len jediné kliknutie na podvrhnutý odkaz, prostredníctvom ktorého možno získať prístup do internej siete organizácie. Druhým testom bol telefonický test, kde až 80 % zamestnancov bez akýchkoľvek známk overenie bolo ochotných poskytnúť citlivé údaje, čo je veľmi vysoké číslo. Tretí test bol orientovaný na bezpečnostné správanie sa zamestnancov pri nájdení prenosného média, bol realizovaný formou dotazníka, pričom 62,5 % respondentov by prehliadalo dokumenty na nájdenom USB kľúči bez ohľadu na to, či by ho pripojili k vlastnému alebo pracovnému počítaču. Aj toto číslo je veľmi vysoké a znamená slabé bezpečnostné povedomie. Štvrtý test, ktorý bol realizovaný bol zameraný na preverenie zverejnených informácií, pričom výsledky, ktoré boli dosiahnuté možno hodnotiť ako uspokojivé. Posledný realizovaný test modelovej situácie sa týkal fyzického prieniku do organizácie, v rámci testu boli iba zhodnotené možnosti realizácie fyzického prieniku.

Posledná časť práce poskytuje návrhy pre identifikáciu útokov, prevenciu a tvorbu bezpečnostnej politiky zameranej na ochranu pred útokmi sociálnym inžinierstvom, pričom všetky tieto opatrenia by mali prispieť k zníženiu zlyhania ľudského faktora a zvýšeniu ochrany pred útokmi sociálnym inžinierstvom.

Na základe skúmania problematiky sociálneho inžinierstva, útokov a obrany pred nimi, možno konštatovať, že najlepším a najúčinnjším spôsobom ochrany pred útokmi sociálnym inžinierstvom je okrem realizácie testov sociálnym inžinierstvom aj dodržiavanie základných pravidiel, ktoré sa týkajú overenia totožnosti osôb a oprávnenia pristupovať k aktívam organizácie.

ZÁVER V ANGLIČTINE

In the information security field is social engineering characterized as a non-technical form to breaking security procedures. On the base of these arguments is possible, that through social engineering attacks could anybody jeopardized the security of any large organization, which uses the latest high-security technology.

In the master thesis are presented social engineering attacks methods and techniques and tools, which can be used and at the same time is provided proposal of procedures against social engineering attacks. On based survey can allege, that Piggybacking attack has the most potential of threat from non-technical attacks and from technical attacks it is Caller-ID and SMS spoofing, Phishing, Pharming and Road apples. Therefore, for using social engineering as a tool for testing information security are provided instructions for realization penetration tests, such as: phishing test, phone test, test with removable media, physical penetration into the organization, dumpster diving, searching garbage and verification of published information. Realization penetration test is based on the presented methodology, which is based on target identification, reconnaissance, creating scenarios and execution of the attack. Another part of the methodology is processing the results of penetration tests, through the test results can be identify potential weaknesses and vulnerabilities in security.

On the base penetration tests was realized the tests of models situations. First test was phishing test, when was obtain 5 % success. For my opinion, it is a lot, because only one click to false link can cause get access to internal network. Second test was phone test, when 80 % employees without any try to authentication were willing to provide confidential informations. Third test was focused on security behavior in the case that employees found a removable media, test was realized by the survey and 62,5 % respondents will browse documents on removable media, whether they would join it to own or work computer. This number is a very big, and means that security behavior is weak. Fourth test, which was focused on verification of published information and results are satisfactory. The last realized test was about physical penetration into organization and there was reviewed only possibilities for realization of this attack.

Last part of thesis provide proposals for identifying attacks, preventing and the creation the security policy to protect against social engineering attacks, all of these measures should help reduce failure of human factor and increase protection against social engineering attacks.

On the base of research about social engineering attacks and defense against it, can be said, that the best and the most effective way to defense against social engineering attacks is, also like realization penetration tests, follow to basic guidelines, such as authentication identity humans and authorization to access the assets of the organization.

ZOZNAM POUŽITEJ LITERATÚRY

- [1] BALCOVÁ, B. SOCIÁLNE INŽINIERSTVOAKOACHILLOVA PÄTA BEZPEČNOSTNÝCH SYSTÉMOV. In: [online]. Žilina, 2007 [cit. 2012-05-10]. Dostupné z: <http://www.securityrevue.com/download/sociotechnika.pdf>
- [2] BARCELÓ, Marta a Pete HERZOG. ISECOM. *The Open Source Security Testing Methodology Manual* [online]. 3. vydanie. 2010, 211 s. [cit. 2012-01-18]. Dostupné z: <http://www.isecom.org/mirror/OSSTMM.3.pdf>
- [3] BASKIN, Brian, Kent NABORS a Jayson E. STREET. *Dissecting the Hack: The F0rb1dd3n Network*. Boston: Syngress Publishing, 2010, 360 s. ISBN 978-1-59749-478-6.
- [4] BASU, Rintu. *Zakázané přesvědčovací techniky*. 1. české vyd. Praha: Grada, 2011, 154 s. ISBN 978-80-247-3722-5.
- [5] Computer Based Social Engineering Tools Social_Engineer_Toolkit_(SET). [online]. [cit. 2012-05-10]. Dostupné z: [http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_\(SET\)](http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_(SET))
- [6] CONHEADY, S. The Future of Social Engineering. In: [online]. [cit. 2012-05-10]. Dostupné z: <http://milano.securitysummit.it/upload/file/atti%20milano%202010/18%20marzo/16.%20CONHEADY.pdf>
- [7] CONHEADY, S. Social Engineering for Penetration Testers. In: [online]. 2009 [cit. 2012-05-10]. Dostupné z: http://malbytes.schleppingsquid.net/Files/BruCon09/Brucon_SE_Presentation.pdf
- [8] FOCA. [online]. [cit. 2012-05-10]. Dostupné z: <http://www.informatica64.com/foca.aspx>
- [9] HADNAGY, Christopher. *Social engineering: The art of human hacking*. Indianapolis: Wiley Publishing, 2011, 408 s. ISBN 978-0-470-63953-5.
- [10] ISO/IEC 27001:2005. *Information Security Management System*. Geneva: International Organization for Standardization, 2005. Dostupné z: http://www.iso.org/iso/catalogue_detail?csnumber=42103

- [11] KUMMER, R. a R. RAK. Informační hrozby v letech 2007-2017. *Magazín Security*. 2007, č. 1, s. 2-5.
- [12] Kurz sociálneho inžinierstva. *Kurz sociálneho inžinierstva* [online]. [cit. 2012-05-10]. Dostupné z: <http://www.isaca.sk/events/seminare/kurz-socialneho-inzinerstva-pre-it-bezpecnostnych-profesionalov-2011/>
- [13] LONG, Johnny, Kevin D. MITNICK, Scott PINZON a Jack WILES. *No Tech Hacking: A guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Burlington: Syngress Publishing, 2008, 384 s. ISBN 978-1-59749-215-7.
- [14] NETOLICKÁ, B. Sociálne inžinierstvo v organizácii. In: IT NEWS [online]. 2012 [cit. 2012-05-10]. Dostupné z: <http://www.itnews.sk/2012-02-29/c146997-socialne-inzinerstvo-v-organizacii>
- [15] Maltego. [online]. [cit. 2012-05-10]. Dostupné z: <http://www.paterva.com/web5/>
- [16] Mapview with results. Dostupné z: http://ilektrojohngithub.github.com/creepy/creepy_mapview.png
- [17] MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. *Hacking bez záhad*. 5. akt. vyd. Praha: Grada, 2007, 520 s. ISBN 978-80-247-1502-5.
- [18] MITNICK, Kevin D. a William L. SIMON. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley Publishing, 2003, 368 s. ISBN 0-7645-4280-X.
- [19] *PDCA-Cycle*. Dostupné z: <http://commons.wikimedia.org/wiki/File:PDCA-Cycle.png>
- [20] *Security World: Čtvrtletník o informační bezpečnosti*. Praha: IDG Czech, 2007-, roč. 2010, č. 3. ISSN 1214-794X.
- [21] SHODAN. [online]. [cit. 2012-05-10]. Dostupné z: <http://www.shodanhq.com/>
- [22] Social engineering. [online]. [cit. 2012-05-10]. Dostupné z: <http://searchsecurity.techtarget.com/definition/social-engineering>
- [23] Social Engineering: A Means To Violate A Computer System. In: [online]. 2006 [cit. 2012-05-10]. Dostupné z: http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-means-violate-computer-system_529

- [24] Social engineering: An attack vector most intricate to tackle!. In: THAPAR, A. *Social engineering* [online]. [cit. 2012-05-10]. Dostupné z: http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf
- [25] USB Rubber Ducky. [online]. [cit. 2012-05-10]. Dostupné z: <https://github.com/hak5darren/USB-Rubber-Ducky/wiki>
- [26] WINKLER, S. I. Case study of industrial espionage through socioal engineering. In: *Case study of industrial espionage through socioal engineering* [online]. [cit. 2012-05-10]. Dostupné z: <http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper040/WINKLER.PDF>

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

FAI	Fakulta aplikovanej informatiky
IKT	Informačná a komunikačná technika
NLP	Neurolingvistické programovanie
PR	Public relations
SMS	Short message service

ZOZNAM OBRÁZKOV

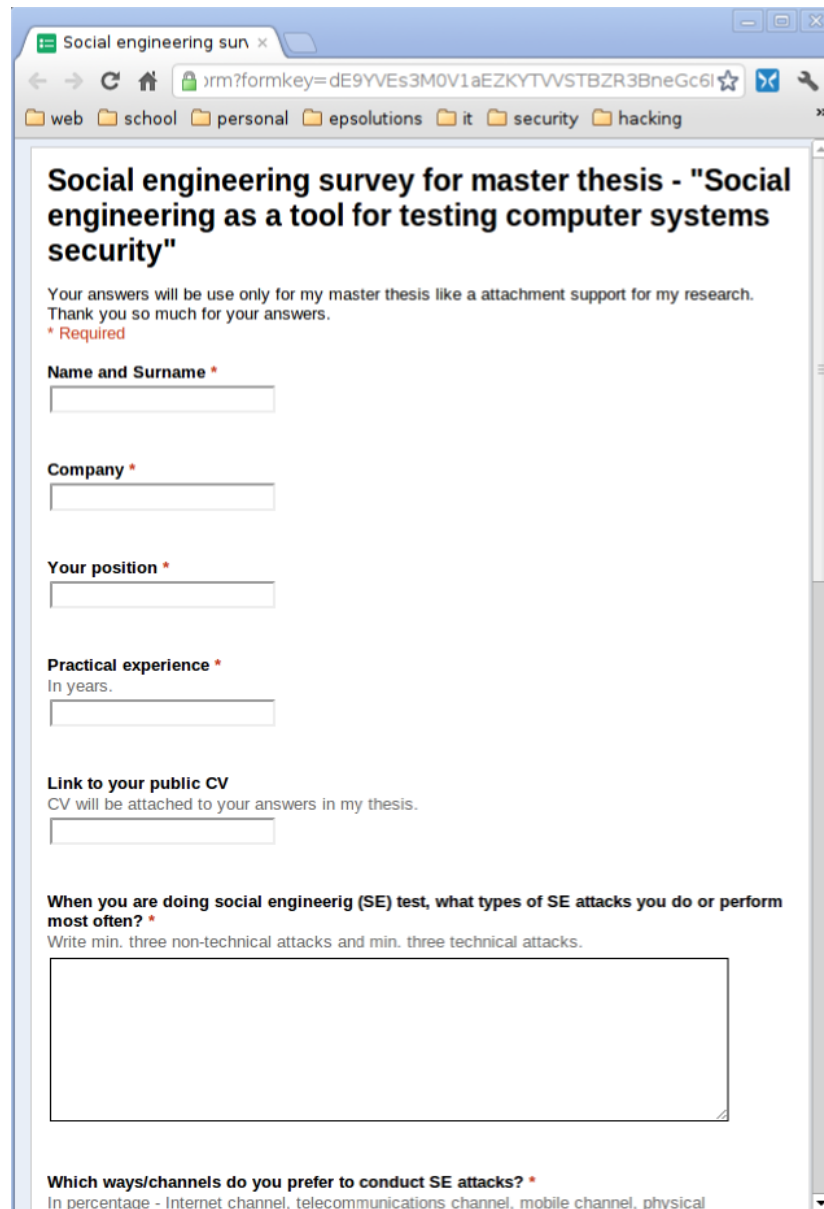
Obrázok 1.1: Fázy sociálneho inžinierstva	16
Obrázok 2.1: Príklad formy phishingu z osvetovej webovej stránky http://ismycreditcardstolen.com, ktorý stavia na ľudskej dôverčivosti	21
Obrázok 2.2: Ukážka úpravy súboru hosts a presmerovanie na falošnú IP adresu	22
Obrázok 2.3: Nástroj Creepy [16]	25
Obrázok 2.4: Nástroj FOCA	26
Obrázok 2.5: Nástroj Maltego	27
Obrázok 2.6: Nástroj SET	27
Obrázok 2.7: Mini kamera v tvare diaľkového ovládača od auta	29
Obrázok 3.1: PDCA cyklus [19]	31
Obrázok 5.1: Vyhodnotenie prvej časti phishingových emailov	48
Obrázok 5.2: Vyhodnotenie druhej časti phishingových emailov	48
Obrázok 5.3: Vyhodnotenie poslednej časti phishingových emailov	49
Obrázok 5.4: Prezentované výsledky zo scenára č. 2	51
Obrázok 5.5: Vyhodnotenie otázky č. 1 z dotazníku scenára č. 3	52
Obrázok 5.6: Vyhodnotenie otázky č. 2 z dotazníku scenára č. 3	53
Obrázok 5.7: Vyhodnotenie otázky č. 3 z dotazníku scenára č. 3	53
Obrázok 5.8: Vyhodnotenie otázky č. 4 z dotazníku scenára č. 3	54
Obrázok 5.9: Vyhodnotenie otázky č. 5 z dotazníku scenára č. 3	54
Obrázok 5.10: Vyhodnotenie otázky č. 6 z dotazníku scenára č. 3	55
Obrázok 5.11: Použitie nástroja FOCA – údaje o sieťovej infraštruktúre 1	56
Obrázok 5.12: Použitie nástroja FOCA – údaje o sieťovej infraštruktúre 2	57
Obrázok 5.13: Použitie nástroja FOCA – údaje o sieťovej infraštruktúre 3	57
Obrázok 5.14: Použitie nástroja FOCA – údaje o sieťovej infraštruktúre 4	58
Obrázok 5.15: Použitie nástroja Maltego	59
Obrázok 5.16: Informácie z webovej stránky web.fai.utb.cz	60
Obrázok 5.17: Plán s rozmiestnením miestností z webovej stránky web.fai.utb.cz	61
Obrázok 5.18: INFORMÁCIE na FAI UTB ve Zlíně	62
Obrázok P.1: Dotazník vo webovom prehliadači 1	92
Obrázok P.2: Dotazník vo webovom prehliadači 2	93
Obrázok P.3: Dotazník vo webovom prehliadači 3	94
Obrázok P.4: Detailné odpovede všetkých respondentov 1	95

Obrázok P.5: Detailné odpovede všetkých respondentov 2	95
Obrázok P.6: Detailné odpovede všetkých respondentov 3	96
Obrázok P.7: Dotazník vo webovom prehliadači pre scenár č. 3	98
Obrázok P.8: Počet respondentov a vekové rozloženie v dotazníku pre scenár č. 3.....	99

ZOZNAM PRÍLOH

Príloha A.1: Elektronický dotazník	92
Príloha A.2: detailné odpovede všetkých respondentov	95
Príloha B.1: Zdrojový kód skriptu na posielanie phishingových emailov	97
Príloha C.1: Dotazník – podklady pre diplomovú prácu – Sociálne inžierstvo ako nástroj na testovanie bezpečnosti PC systémov	98
Príloha C.2: Počet respondentov a vekové rozdelenie	99
Príloha D.1: Elektronická príloha	100

PRÍLOHA A.1: ELEKTRONICKÝ DOTAZNÍK
SOCIAL ENGINEERING SURVEY FOR MASTER THESIS –
„SOCIAL ENGINEERING AS A TOOL FOR TESTING COMPUTER
SYSTEMS SECURITY“



The image shows a web browser window with a single tab titled "Social engineering sun". The address bar contains a URL with a formkey parameter. The browser's bookmark bar shows folders for "web", "school", "personal", "epsolutions", "it", "security", and "hacking". The main content area displays a survey form with the following sections:

- Title:** Social engineering survey for master thesis - "Social engineering as a tool for testing computer systems security"
- Introduction:** Your answers will be use only for my master thesis like a attachment support for my research. Thank you so much for your answers.
- Required:** * Required
- Name and Surname *** (text input field)
- Company *** (text input field)
- Your position *** (text input field)
- Practical experience *** (text input field)
In years.
- Link to your public CV** (text input field)
CV will be attached to your answers in my thesis.
- When you are doing social engineerig (SE) test, what types of SE attacks you do or perform most often? ***
Write min. three non-technical attacks and min. three technical attacks.
(Large text area for response)
- Which ways/channels do you prefer to conduct SE attacks? ***
In percentage - Internet channel, telecommunications channel, mobile channel, physical

Obrázok P.1: Dotazník vo webovom prehliadači 1

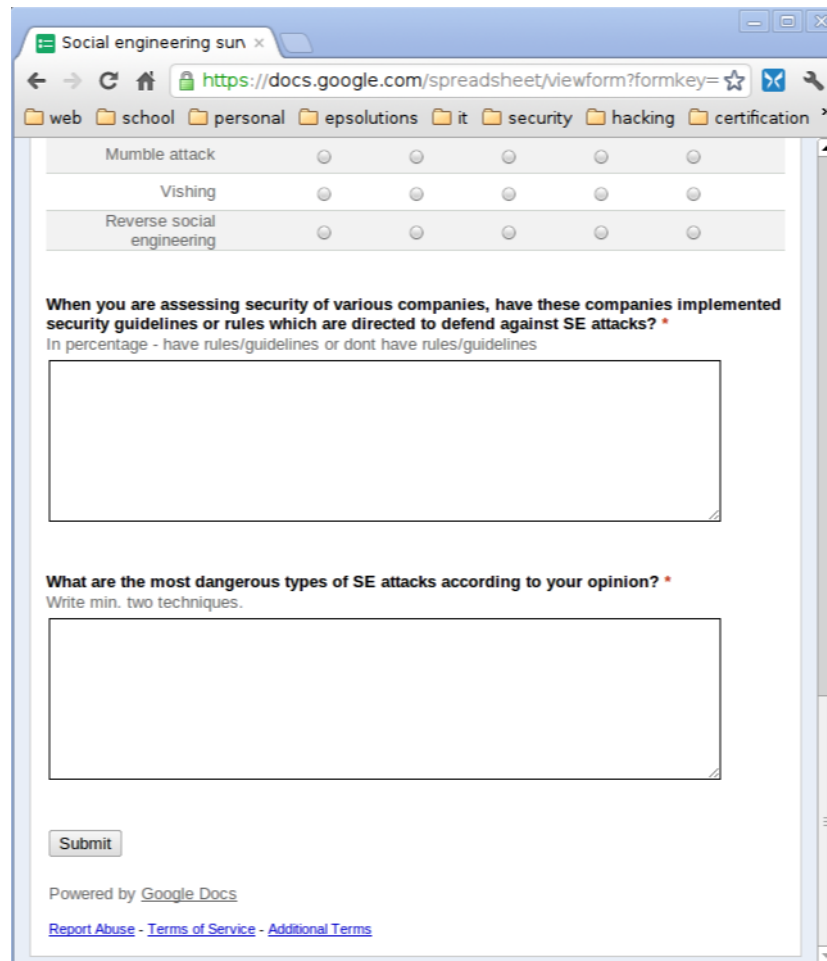
Which ways/channels do you prefer to conduct SE attacks? *
 In percentage - Internet channel, telecommunications channel, mobile channel, physical access/contact.

For each type of attack, mark the level of potential threat to security of a company. *
 1 - minimum potential threat, 5 - maximum potential threat

	1	2	3	4	5
Trashing/Dumpster diving	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Spying/Shoulder surfing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Techie Talk	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ten attack	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Piggybacking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Phishing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Pharming	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Caller-ID and SMS spoofing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Road apples	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Whaling attack	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mumble attack	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vishing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reverse social engineering	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

When you are assessing security of various companies, have these companies implemented security guidelines or rules which are directed to defend against SE attacks? *
 In percentage - have rules/guidelines or dont have rules/guidelines

Obrázok P.2: Dotazník vo webovom prehliadači 2



The image shows a web browser window with a single tab titled "Social engineering sun". The address bar displays the URL "https://docs.google.com/spreadsheet/viewform?formkey=". The browser's bookmark bar contains folders for "web", "school", "personal", "epsolutions", "it", "security", "hacking", and "certification".

The form content includes a table with the following items:

Mumble attack	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vishing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reverse social engineering	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

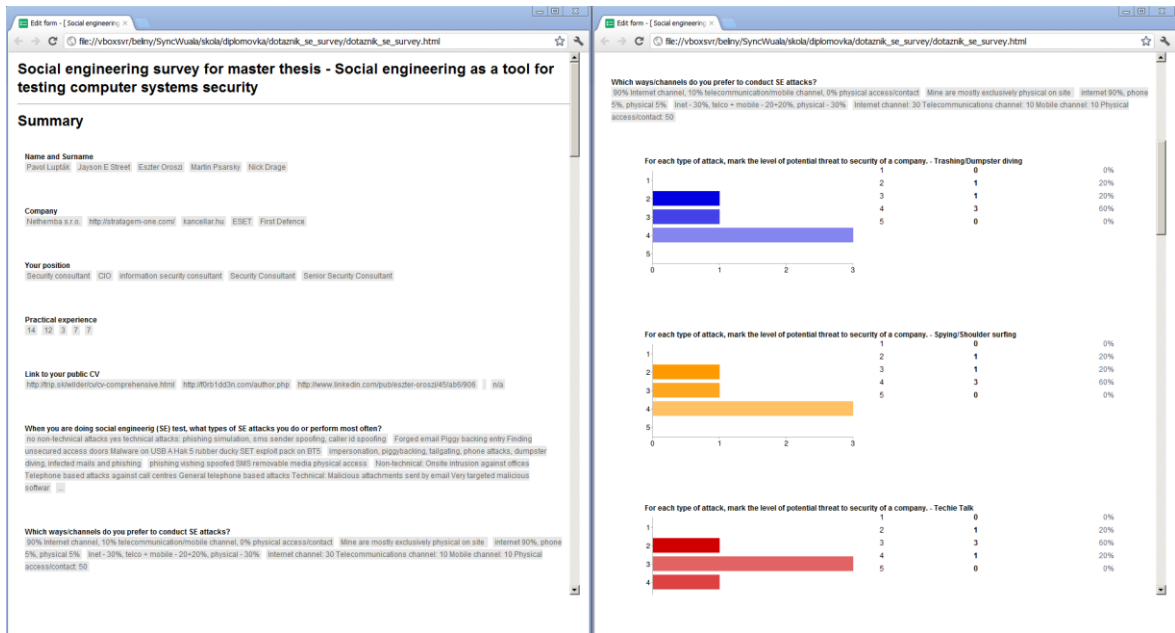
Below the table, the form asks: "When you are assessing security of various companies, have these companies implemented security guidelines or rules which are directed to defend against SE attacks? *". A sub-question reads: "In percentage - have rules/guidelines or dont have rules/guidelines". This is followed by a large empty text input box.

The next question is: "What are the most dangerous types of SE attacks according to your opinion? *". A sub-question reads: "Write min. two techniques." This is followed by another large empty text input box.

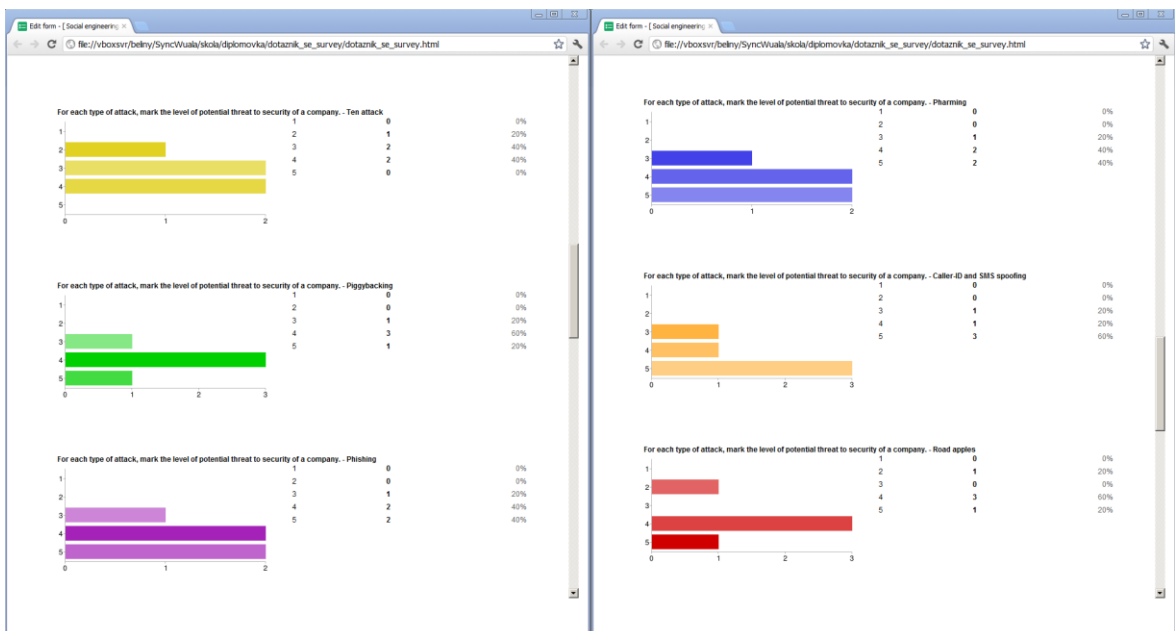
At the bottom of the form is a "Submit" button. Below the button, it says "Powered by Google Docs" and provides links for "Report Abuse", "Terms of Service", and "Additional Terms".

Obrázok P.3: Dotazník vo webovom prehliadači 3

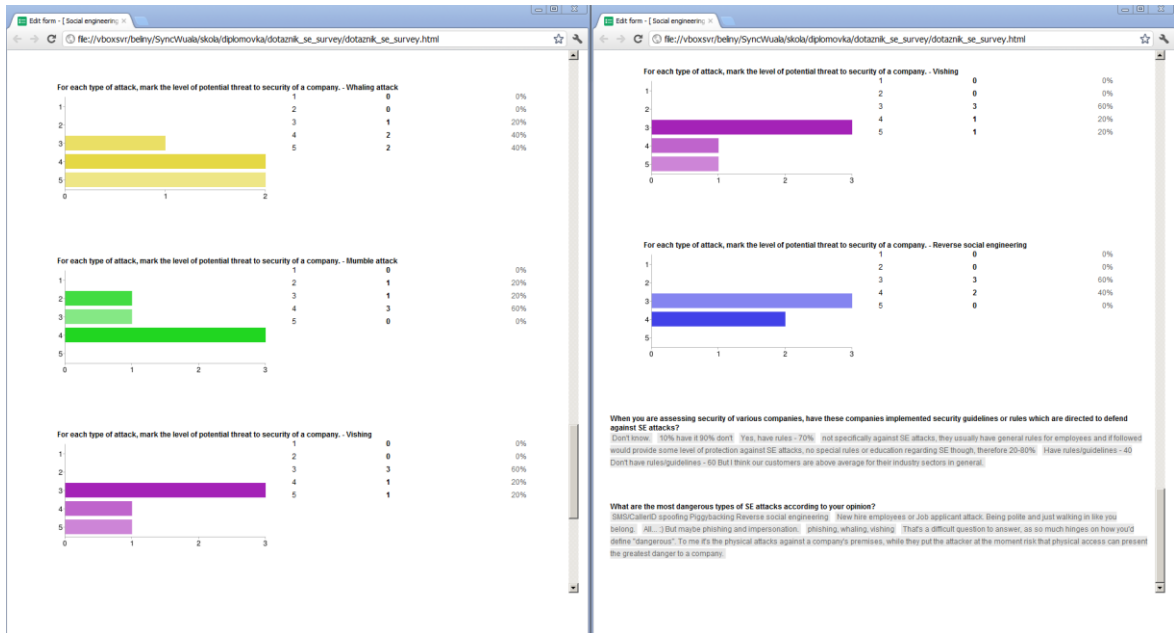
PRÍLOHA A.2: DETAILNÉ ODPOVEDE VŠETKÝCH RESPONDENTOV



Obrázok P.4: Detailné odpovede všetkých respondentov 1



Obrázok P.5: Detailné odpovede všetkých respondentov 2



Obrázok P.6: Detailné odpovede všetkých respondentov 3

PRÍLOHA B.1: ZDROJOVÝ KÓD SKRIPTU NA POSIELANIE PHISHINGOVÝCH EMAILOV

```
#!/usr/bin/perl

use strict;
use warnings;

use constant RECIPIENTS => qw/
    adresa.obete@institucia.com
    /;

use constant FROM => 'podvrhnutá.adresa@institucia.com';
use constant REPLY_TO => 'adresa.utocnika@domena.com';
use constant RETURN_PATH => ' adresa.utocnika@domena.com ';
use constant SUBJECT => 'SUBJEKT EMAILU';
use constant MESSAGE => 'TELO EMAILU';

sub send_mail
{
    my ($from, $recipient, $reply_to, $return_path, $subject, $message) = @_ ;
    open (MAIL,"|/usr/sbin/sendmail -oi -t -f $return_path ") or die "Can't open sendmail";
    print MAIL "To: $recipient\n";
    print MAIL "From: $from\n";
    print MAIL "Reply-to: $reply_to\n";
    print MAIL "Subject: $subject\n";
    print MAIL "\n";
    print MAIL "$message\n";
    close MAIL;
};

foreach my $to ( RECIPIENTS)
{
    send_mail( FROM, $to, REPLY_TO, RETURN_PATH, SUBJECT, MESSAGE);
};
```

PRÍLOHA C.1: DOTAZNÍK – PODKLADY PRE DIPLOMOVÚ PRÁCU – SOCIÁLNE INŽINIERSTVO AKO NÁSTROJ NA TESTOVANIE BEZPEČNOSTI PC SYSTÉMOV

Dotazník - podklady pre diplomovú prácu - Sociálne inžierstvo ako nástroj na testovanie bezpečnosti PC systémov

Dobrý deň, som študentom magisterského štúdia na Univerzite Tomáše Bati ve Zlíne, Fakulta aplikovanej informatiky a chcem Vás poprosiť o vyplnenie nasledovného dotazníka. Cieľom dotazníka je získať informáciu a obraz o reakciách bežného používateľa počítača. V práci budú Vaše odpovede prezentované vo forme grafu. Výsledky budú úplne anonymné, a preto prosím odpovedajte na otázky úprimne a pravdivo.

Ďakujem, s pozdravom Bc. Peter Bublányi.
* Pozor!

Pohlavie *

Muž
 Žena

Vek

20 - 29 rokov 30 - 39 rokov 40 - 49 rokov 50 - 59 rokov

Vek

V prípade, že nájdete na chodbe, na ulici, na parkovisku, atď. USB kľúč, pripojili by ste ho k Vášmu vlastnému počítaču alebo notebooku? *

Áno
 Nie

V prípade, že nájdete na chodbe, na ulici, na parkovisku, atď. USB kľúč, pripojili by ste ho k pracovnému počítaču alebo notebooku? *

Áno
 Nie

Prehliadali, pozerali by ste obsah uložený na nájdenom USB kľúči? *

subory, office dokumenty, fotografie a iné

Áno
 Nie

V prípade, že nájdete na chodbe, na ulici, na parkovisku, atď. optické médium - CD/DVD so zaujímavým popisom, spustili by ste ho na Vašom vlastnom počítači alebo notebooku? *

Áno
 Nie

Prehliadali, pozerali by ste obsah uložený na nájdenom USB kľúči? *

subory, office dokumenty, fotografie a iné

Áno
 Nie

V prípade, že nájdete na chodbe, na ulici, na parkovisku, atď. USB kľúč, pripojili by ste ho k Vášmu vlastnému počítaču alebo notebooku? *

Áno
 Nie

V prípade, že nájdete na chodbe, na ulici, na parkovisku, atď. USB kľúč, pripojili by ste ho k pracovnému počítaču alebo notebooku? *

Áno
 Nie

Prehliadali, pozerali by ste obsah uložený na nájdenom USB kľúči? *

subory, office dokumenty, fotografie a iné

Áno
 Nie

V prípade, že nájdete na chodbe, na ulici, na parkovisku, atď. optické médium - CD/DVD so zaujímavým popisom, spustili by ste ho na Vašom vlastnom počítači alebo notebooku? *

Áno
 Nie

Prehliadali, pozerali by ste obsah uložený na nájdenom CD/DVD médiu? *

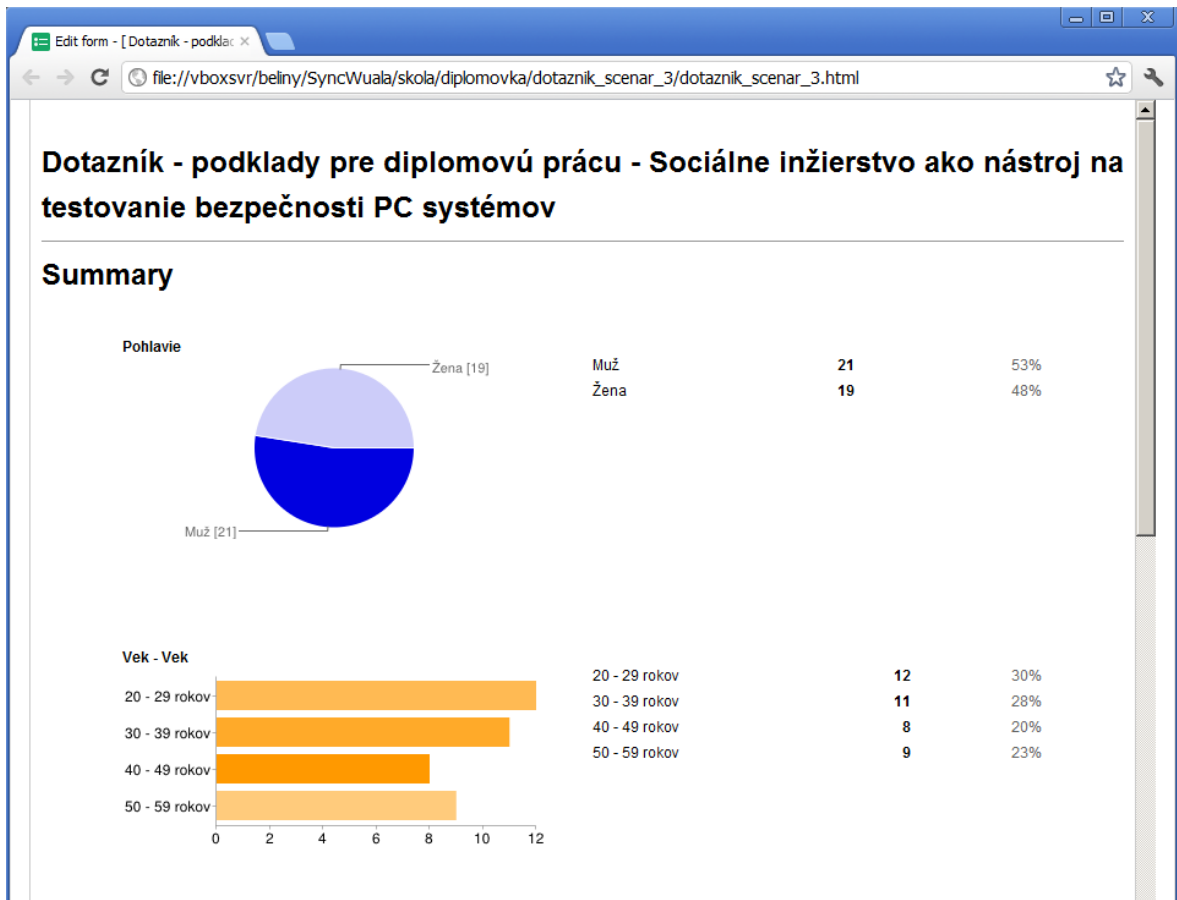
subory, office dokumenty, fotografie a iné

Áno
 Nie

Použite technológiu Dokumenty Google

[Chráňte svoje údaje](#) - [Podmienky poskytovania služieb](#) - [Dodatočné podmienky](#)

Obrázok P.7: Dotazník vo webovom prehliadači pre scenár č. 3

PRÍLOHA C.2: POČET RESPONDETOV A VEKOVÉ ROZDELENIE

Obrázok P.8: Počet respondentov a vekové rozloženie v dotazníku pre scenár č. 3

PRÍLOHA D.1: ELEKTRONICKÁ PRÍLOHA

Optické médium, ktoré obsahuje:

- diplomová práca *master_thesis_bubeliny* vo formáte .pdf
- Výsledky dotazníka – Social engineering survey for master thesis – „Social engineering as a tool for testing computer systems security“ v HTML kóde
- Výsledky dotazníka – podklady pre diplomovú prácu – Sociálne inžinierstvo ako nástroj na testovanie bezpečnosti PC systémov v HTML kóde
- Údaje získané pri realizácii scenáru č. 4 pomocou nástrojov FOCA a Maltego.