ŽILINSKÁ UNIVERZITA V ŽILINE

FAKULTA ŠPECIÁLNEHO INŽINIERSTVA

SOCIÁLNE INŽINIERSTVO AKO SÚČASNÁ HROZBA INFORMAČNÝCH SYSTÉMOV

BARBORA BALCOVÁ

2008

SOCIÁLNE INŽINIERSTVO AKO SÚČASNÁ HROZBA INFORMAČNÝCH SYSTÉMOV

BAKALÁRSKA PRÁCA

BARBORA BALCOVÁ

ŽILINSKÁ UNIVERZITA V ŽILINE
FAKULTA ŠPECIÁLNEHO INŽINIERSTVA

KATEDRA BEZPEČNOSTNÉHO MANAŽMENTU

Študijný odbor: Ochrana osôb a majetku

Vedúci bakalárskej práce: Ing. Tomáš Loveček, PhD.

Stupeň kvalifikácie: Bakalár (Bc.)
Dátum odovzdania práce: 6. 6. 2008

ŽILINA 2008

ABSTRAKT

BALCOVÁ, Barbora: Sociálne inžinierstvo ako súčasná hrozba informačných systémov. [Bakalárska práca]. Žilinská univerzita v Žiline. Fakulta špeciálneho inžinierstva; Katedra bezpečnostného manažmentu. Vedúci: Ing. Tomáš Loveček, PhD. Stupeň odbornej kvalifikácie: Bakalár v odbore Ochrana osôb a majetku. Žilina: FŠI ŽU, 2008. 65 s.

Cieľom práce je predstaviť sociálne inžinierstvo ako málo poznanú a pritom najúčinnejšiu hrozbu pre informačné systémy v súčasnosti. Zaoberá sa popísaním metód, ktoré sociálni inžinieri aplikujú na dosiahnutie stanoveného cieľa, najmä zmanipulovaním obete a zneužitím vybudovanej dôvery voči nim. V poslednej časti práce sú navrhnuté možné ochranné opatrenia proti tejto hrozbe a overenie hypotéz, na základe zmapovania súčasného stavu informovanosti o nej.

Kľúčové slová: sociálne inžinierstvo, sociotechnika, sociálny inžinier, sociotechnik, útok, hrozba, informácie, bezpečnosť

ABSTRACT

BALCOVÁ, Barbora: *Social engineering as a current treath of information systems*.. [Bachelor Thesis]. University of Zilina. Faculty of Special Engineering; Department of Security Management. Advisor: Ing. Tomáš Loveček, PhD. Qualification degree: Bachelor of Protection of Persons and Property. Žilina: FŠI ŽU, 2008. 65p.

The goal of the thesis is to present the social engineering as a hardly known and at the same time the most effective threat for information system this days. The thesis is trying to describe methods, which social engineers aplicate to reach the allocated goal, especially manipulating the victim and abuseing builted arrangements against them. In the last chapter are devised possible protective measures against this threat and approval of the hypothesis, based on research of the current condition of awareness of sociotechnology.

Key words: social engineering, sociotechnology, social engineer, sociotehcnician, attack, threat, information, security

PREDHOVOR

Tému bakalárskej práce „Sociálne inžinierstvo ako súčasná hrozba informačných systémov“ som si zvolila preto, že je podľa môjho názoru aktuálna, vzhľadom na neodmysliteľnosť pomoci počítačov v živote a pri práci. Ale len málo kto vie, ako si uchrániť citlivé informácie pred útokmi sociotechnikov, pretože nedisponuje dostatočným množstvom informácií o danej hrozbe a nepoužíva vhodné preventívne opatrenia proti nej.

Očakávam, že bakalárska práca bude informatívnym prínosom pre jej čitateľov, ale bude mať i praktické využitie, ktoré vyplýva z popísaných preventívnych opatrení na a elimináciu realizácie sociotechnických útokov a tým minimalizovať ich nežiaduce následky na spoločnosti.

Pri spracovaní bakalárskej práce som získala informácie z knižných, internetových a periodických zdrojov, ale i z vedomostí získaných štúdiom.

Chcela by som poďakovať vedúcemu bakalárskej práce Ing. Tomášovi Lovečkovi, PhD. za pomoc pri kompletizácii informácií, za poskytnutý čas, neoceniteľné rady a konzultácie, ale aj ostatným, ktorí mi pomohli pri spracovaní bakalárskej práce.

Zároveň čestne prehlasujem, že som bakalársku prácu vypracovala samostatne s využitím teoretických vedomostí a s použitím uvedenej literatúry.

.....

BARBORA BALCOVÁ

ZOZNAM GRAFOV, OBRÁZKOV A TABULIEK

***GRAFY*:**

OBRÁZKY:

TABUĽKY:

OBSAH

ÚVOD

Tretie tisícročie je nazývané aj informačným vekom. V tejto dobe môžeme stále počuť, či sa dokonca sami presvedčiť, že úspešný je ten, kto ovláda schopnosť získavať, hľadať a správne vyhodnocovať informácie. Lenže ľudia si ešte stále nevedia uvedomiť ich hodnotu. Málokto vie, že informácie je tiež nutné zodpovedajúcim spôsobom chrániť.

Narušenie bezpečnosti počítačových systémov, nie je čisto technická záležitosť vznikajúca následkom dier v systéme, ktoré je útočník schopný využiť, lebo najslabším článkom týchto systémov je človek.

Ľudia, ktorí prostredníctvom manipulácie, presviedčania a zmeny svojej totožnosti nadobudnú informácie potrebné na realizáciu vytýčeného cieľa, sa volajú sociálni inžinieri alebo sociotechnici a sú najväčšou súčasnou hrozbou informačných systémov.

Najnebezpečnejším rysom sociotechniky je to, že pri dobre vedenom útoku si obeť väčšinou vôbec neuvedomí, že niečo vyzradila nepovolanej osobe, čiže že sa stala obeťou sociálneho inžiniera.

Vzhľadom na malú informovanosť ľudí o sociotechnike, je cieľom práce oboznámiť ich o jej význame a existencii, metódach, ktoré sociotechnici využívajú, preventívnych opatreniach a zmapovanie informovanosti právnických osôb o tejto hrozbe.

Útočníci, na dosiahnutie cieľa postupujú podľa cyklu, ktorý sa skladá zo štyroch fáz: zhromažďovanie informácií, budovanie vzťahov a dôvery, využitie dôvery a realizácia a zneužitie.

Sociálne inžinierstvo môže byť realizované formou priameho a nepriameho kontaktu sociotechnika s obeťou. K priamemu kontaktu dochádza pri osobnom požiadaní o informácie alebo činnosti a pri inverznej sociotechnike. Nepriamy kontakt je uskutočňovaný prostredníctvom využitia technológií ako je telefón, fax, internet, pošta a odpadky.

Preventívne opatrenia zamerané proti sociotechnike, majú byť súčasťou bezpečnostnej politiky firiem a ich zamestnanci by si ich mali osvojiť prostredníctvom bezpečnostných školení a aj realizovať v praxi.

1 VYMEDZENIE POJMU SOCIÁLNE INŽINIERSTVO A SOCIOTECHNICKÝ CYKLUS

1.1 ACHILLOVA PÄTA BEZPEČNOSTNÝCH SYSTÉMOV

V dnešnej uponáhľanej a modernej dobe, si my, ľudia, nevieme predstaviť život bez mobilov, počítačov a internetu, ktoré nám nahradili knihy, posielanie listov a čiastočne aj chodenie do obchodov a inštitúcií. Každý jeden človek či organizácia si chráni svoje súkromie a dôverné informácie ako sú heslá a prístupové kódy, ktoré umožňujú využívanie elektronickej pošty a platby.

Ale ako úspešne chrániť tieto informácie utajeného styku pred ich odhalením a hackermi?

Firma si môže zariadiť tie najlepšie a najdrahšie bezpečnostné technológie, vyškoliť personál tak, aby bola každá dôverná informácia pod zámkom, najať si najlepšiu firmu na ochranu objektov, a predsa bude tá organizácia ešte stále zraniteľná.

Súkromné osoby sa môžu držať všetkých najlepších zásad doporučených odborníkmi, môžu otrocky nainštalovať všetky najnovšie produkty vylepšujúce zabezpečenie a zodpovedajúcim spôsobom pozorne skonfigurovať systém, môžu použiť všetky jeho vylepšenia či opravy, a predsa sú tieto osoby stále nechránené [10, s.19].

Túžba po pocite absolútnej bezpečnosti je prirodzená, ale vedie ľudí k falošnému pocitu chýbajúceho ohrozenia. Vezmime za príklad zodpovedného milujúceho muža, ktorý si zaobstaral do vstupných dverí cylindrický zámok známy tým, že sa nedá otvoriť pakľúčom, aby ochránil svoju ženu, deti a domov. Po namontovaní tohto zámku sa cíti lepšie, pretože jeho rodina je teraz vo väčšom bezpečí. Ale čo sa stane ak žena otvorí dvere, lebo prišli skontrolovať plyn? Nezávisle na drahých zámkoch nie sú stále obyvatelia v bezpečí.

Prečo? Pretože achillovou pätou zabezpečenia je *ľ u d s k ý f a k t o r.*

Bezpečnosť je až príliš často podceňovaná. Pokiaľ k tomu ešte pridáme ľahkovážnosť, stereotyp v práci, naivitu, ignoráciu a hlavne ochotu pomôcť, situácia sa ďalej zhoršuje. Najuznávanejší vedec 20. storočia ***Albert Einstein*** vraj povedal*: „Iba dve veci sú nekonečné: vesmír a ľudská hlúposť. Avšak tým prvým si nie som istý.“* Vo výsledku sa

útok sociotechnika často podarí, pretože ľudia bývajú hlúpi, naivní, nepozorní, nápomocní a ľahostajní. Častejšie sú ale takéto útoky účinné preto, že ľudia nerozumejú overeným zásadám bezpečnosti [10, s.20].

1.1.1 ČO JE TO SOCIÁLNE INŽINIERSTVO?

Existuje veľmi veľa definícií *sociálneho inžinierstva* tiež nazývaného aj *sociotechnika*. Niektoré z nich sú:

- „Bývalý najväčší hacker na svete a terajší najvyhľadávanejší expert na zabezpečenie počítačových systémov Kevin Mitnick [10, s. 4] definoval sociotechniku ako ovplyvňovanie a presviedčanie 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.“

- „Sociálne inžinierstvo sú systematicky používané vedomosti ľudského chovania a umenia presviedčať, aby užívateľ 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“ [13].

- „Sociálne inžinierstvo je metóda získavania dôverných informácií pomocou manipulácie oprávnených užívateľov. Sociotechnik väčšinou používa telefón alebo internet na oklamanie (podvedenie) ľudí, aby odhalil tajné informácie. Sociálni inžinieri využívajú prirodzenú tendenciu jednotlivca veriť im, pred využívaním dier v počítačových systémoch. Spravidla to súhlasí s názorom, že „užívatelia sú najslabším článkom“ v zabezpečení a toto je podstata toho, prečo je sociálne inžinierstvo uskutočniteľné.

Sociotechnik je hacker, ktorý využíva inteligenciu namiesto počítačovej sily. Hackeri volajú do informačných centier (výpočtových stredísk) a predstierajú, že sú zákazníci, ktorí zabudli heslo alebo sú odhalení a jednoducho počkajú na niekoho, kto im uverí

a prezradí potrené informácie. Iné druhy sociálneho inžinierstva nie sú až také očividné. Hackeri vedia vytvoriť falošné webové stránky alebo dotazníky, v ktorých požiadajú užívateľov o prezradenie hesla alebo dôverných informácií“ [2].

- „V počítačovej bezpečnosti je sociálne inžinierstvo pojem, ktorý charakterizuje netechnickú formu obťažovania, ktorá je založená na schopnosti ovplyvňovania a klamania ľudí, na prelomenie bezpečnostných postupov. Sociotechnik používa „neférovú hru“, aby nadobudol dôveru oprávnenej osoby k získaniu potrebných informácií, na prekonanie bezpečnostného systému a následného preniknutia do siete. Sociálni inžinieri sa spoliehajú na prirodzenú ústretovosť ľudí, ako aj na ich bezmocnosť. Dovolávanie sa právomoci a využívanie staromódneho odpočúvania sú typické techniky sociálneho inžinierstva.

Ďalší trend sociotechniky spočíva v tom, že sociotechnik verí v ľudskú neschopnosť držať krok s dobou, pričom sa veľmi spoliehajú sa na informačné technológie. Sociálne inžinierstvo je založené na skutočnosti, že ľudia si nie sú vedomí závažnosti informácií, ktoré vlastnia a preto si neuvedomujú, aká dôležitá je ich ochrana a nevyzradenie. Preto často sociálni inžinieri prehľadávajú odpadky, učia sa naspamäť prístupové kódy, keď ich letmo zbadajú ponad niečie plece, alebo využijú prirodzenú ľudskú tendenciu zvoliť si heslá, ktoré sú pre nich ľahko zapamätateľné a zmysluplné, ale práve také sú najľahšie uhádnuteľné. Bezpečnostní experti sa domnievajú, že čím viac sa stáva naše vzdelanie, rozvíjanie a kultúra závislé na informáciách, tým bude sociotechnika predstavovať čoraz väčšiu hrozbu pre akékoľvek bezpečnostné systémy“ [15].

Po zhrnutí rôznych definícií dostávame vysvetlenie, že sociálne inžinierstvo, alebo tiež sociotechnika je útok narušiteľa z vonkajšieho prostredia, ktorý využíva psychologické triky, city, vyhrážky, na oprávnených užívateľov informačných systémov, aby vyhoveli prianiam útočníka.

Sociálni inžinieri sú prevažne osoby bystré, čulé, výrečné s vlohami manipulácie s ľuďmi. Vyznačujú sa aj schopnosťou rozptyľovať myšlienky ľudí, s ktorými hovoria, čo vedie k rýchlemu navádzaniu spolupráce s obeťou útoku. Myslieť si, že nie každá osoba podľahne takejto manipulácii, je podceňovanie schopností a inštinktov

sociotechnika. Na druhej strane si dobrý sociotechnik nikdy nedovolí podceňovať svojho protivníka.

Dobrý sociotechnik si často vyberá za obeť osobu s nízkym postavením vo firme. Takýmito ľuďmi je ľahké manipulovať a vyťahovať z nich zdanlivo nedôležité údaje, ktoré krok za krokom približujú útočníka k dôverným informáciám.

Útočník sa zameriava na osoby na nízkych pozíciách, pretože tie si plne neuvedomujú význam niektorých informácií a dôsledky niektorých činností. Okrem toho sú proti sociotechnickým metódam menej odolné – volajúci má autoritu, zdá sa milý a priateľský, robí dojem, že pozná rôznych ľudí vo firme, vec, o ktorú žiada, je veľmi naliehavá a obeť predpokladá, že si získa niečie uznanie či vďačnosť.

Metódy klamu

Aby prekonal zabezpečenie, musí útočník, votrelec alebo sociotechnik nájsť metódu na oklamanie dôveryhodného pracovníka tak, aby prezradil nejakú informáciu, trik alebo zdanlivo nedôležitú nápovedu, ktorá by mu umožnila dostať sa do systému. Pokiaľ sa dajú pracovníci oklamať, alebo sa dá s mini manipulovať, aby prezradili dôverné informácie, alebo keď ich činnosť spôsobuje vznik dier v zabezpečení, ktoré umožnia útočníkovi prístup do systému, potom neexistuje žiadna technológia, ktorá by mohla firmu ochrániť.

Motivácia

Sociálny inžinier je motivovaný rôznymi podnetmi, ktoré ho nabádajú k tomu, aby vykonával sociotechnické útoky. Existuje veľa takýchto podnetov, medzi ktoré patria:

Finančný zisk: z rôznych dôvodov sa stáva „hypnotizovaný“ peňažnými ziskami. Napríklad môže byť presvedčený, že si zaslúži viac peňazí ako zarába, alebo má potrebu uspokojiť neovládateľný zlozvyk – gamblerstvo.

Sebeckosť: chce získať prístup a/alebo možnosť upravovať informácie, ktoré sa týkajú členov rodiny, priateľov alebo dokonca susedov.

Pomsta: z dôvodov, ktoré pozná len on sám, môže hľadať cieľ v priateľovi, kolegovi, organizácii alebo dokonca v úplnom cudzincovi, aby uspokojil emocionálnu túžbu po odplate.

Vonkajší tlak: môže byť pod tlakom priateľov, rodiny alebo organizovaných kriminálnych skupín, z dôvodov ako sú finančný zisk, sebeckosť a/alebo pomsta [17].

1.1.2 PSYCHOLOGICKÉ FAKTORY POUŽÍVANÉ V SOCIOTECHNIKE

Odvtedy, ako sa sociálne inžinierstvo stalo spoločenskou a psychologickou aktivitou, pokúšajú sa odborníci pochopiť psychológiu používanú v ňom, pred vyhľadávaním zlepšenia obrany proti nemu. Je to v poriadku, pretože je nevyhnutné rozumieť psychologickým spúšťačom, ktoré sú zodpovedné za efektívnosť sociotechnických útokov. Faktory sú psychologické princípy, ktoré sa prejavujú nejakým druhom ovplyvňujúcej sily alebo presviedčaním ľudí. Poznatky o psychologických faktoroch v sociotechnike, by mali pomôcť stanoviť efektívnu obranu proti nemu.

Silný afekt

Silný afekt je faktor, ktorý využíva najväčšie emocionálne rozpoloženie, ktoré umožňuje sociotechnikovi získať viac informácií, ako predpokladal. Ak obeť cíti silný pocit prekvapenia, predzvesti alebo hnevu, potom s menšou pravdepodobnosťou bude schopná rozmýšľať o argumentoch, ktoré sú prezentované. Silný afekt je využívaný, keď sociotechnik povie nejaký výrok na začiatku interakcie, ktorý je spúšťačom prudkých emócií. Silný hnev zahŕňa rozrušenie alebo paniku, ale nie je to obmedzené strachom. Nápor silných emócií pôsobí ako rozptýlenie a narušenie schopnosti obete odhadovať, myslieť logicky alebo klásť protiargumenty.

Kontrafaktuálne myslenie (premýšľanie o neuskutočnených alternatívach riešenia problémov) je fenomén spojený so silným afektom. Toto myslenie nastáva vtedy, keď dochádza k očakávaniu možností, ako je výhra veľkej ceny, pričom vznikajú skraty ľudského racionálneho myslenia. Človek ignoruje fakt, že pravdepodobnosť výhry je v skutočnosti veľmi vzdialená, navádza ľudí aby riskovali skutočný a cenný tovar (informácie alebo prístupy) pre možnosť výhry. Je to tak, ako keby bola osoba začarovaná, čo prináša množstvo rušivých emócií.

Hackeri webových stránok dávajú dôraz na použitie prekvapenia. Prekvapenie môže byť uskutočňované prostredníctvom telefonovania zavčasu ráno alebo prísť s veľmi nezvyčajnými okolnosťami alebo argumentmi. Prekvapenie, môže byť tiež dosiahnuté aj použitím citovo zafarbených slov alebo obrazov.

Preťaženie

Mylné predpoklady vedú k nespochybňovaniu, keď sú vypočuté narýchlo a zamiešané medzi presvedčivé banality. Je to psychologický faktor preťaženia alebo zahltenia. Rýchlo riešiť veľké množstvo informácií naraz, ovplyvňuje logickú činnosť a môže spôsobiť „zmyslové preťaženie“. Keď majú ľudia spracovať príliš veľké množstvo informácií stávajú sa „mentálne pasívny – radšej informácie absorbujú ako ich vyhodnocujú“.

Argumentovanie z nečakanej perspektívy môže tiež viesť k preťaženiu. Na vytvorenie nového stanoviska, potrebuje obeť čas, ktorý ale nemá k dispozícii. Obeť má veľa informácií a nedostatok času na ich premyslenie, čo znižuje jej schopnosť spracovať ich alebo preskúmať. Vtedy je ochotnejšia akceptovať argumenty, ktoré by mali byť odmietnuté.

Opätovanie

Dobre známe pravidlo pri sociálnych interakciách je, ak niekto dá niekomu niečo alebo mu niečo sľúbi, mal by mu to oplatiť láskavosťou. Inklinuje to k pravde, i keď pôvodný dar nebol vyžiadaný a dokonca, vrátená vec by mala byť hodnotnejšia ako bola pôvodná darovaná. Táto skutočnosť je známa ako opätovanie alebo reciprocita.

Tento psychologický faktor je pokladaný za dobre dohodnutú obyčaj. V korporačnom prostredí nevedia ľudia dôkladne vyhodnotiť požiadavky, pretože podliehajú duševným skratom. Príčina je tá, že ak niekto zatelefonuje a požiada o pomoc s problémom, volajúci mu ochotne pomôže.

Inverzné sociálne inžinierstvo využíva podobné faktory. Sociotechnik sa javí ako hrdina pripravený a ochotný vyriešiť problémy. Predtým, ako je problém vyriešený, sa mu obeť cíti byť zaviazaná. Toto je samozrejme ideálna situácia pre sociálneho inžiniera.

Iný spôsob, ako môže byť reciprocita využitá, je prostredníctvom behavioristických experimentov. Tieto pokusy ukazujú, že keď majú dvaja ľudia rozdielne názory, ak sa jeden vzdá jednej požiadavky, ten druhý sa bude cítiť donútení vzdať sa jej tiež.. Pre hackera to je úplne jednoduché. Potrebuje iba vytvoriť viac ako jednu požiadavku, pri dohode sa jednej vzdá a potom bude obeť cítiť tlak, aby sa aj ona vzdala jednej požiadavky.

Reciprocita je neustále videná v korporačnom prostredí. Zamestnanec pomáha ostatným, s očakávaním, že nakoniec, mu túto láskavosť vrátia. Je to nepísaný výmenný systém, ktorý je považovaný za neoceniteľnú pomoc, ak chce byť niekto úspešný. Avšak, sociálny inžinier využíva tento systém, pretože jeho motívy sú nečestné a vyhľadáva (dožaduje sa) niečoho, čo by nemalo byť poskytnuté za žiadnu cenu.

Klamlivé vzťahy

Ďalší psychologický faktor je budovanie vzťahov so zámerom zneužívania ľudí. Jedným zo spôsobov je prerozdelenie informácií a diskutovanie o nepriateľoch. Obľúbeným podfukom sociotechnika je, keď obalamutí zamestnanca, ktorý je voči nemu nedôverčivý v rôznych súvislostiach. V tomto čase si s ním vybudujú vzťah cez emaily, prostredníctvom zdieľania informácií a technológií, bez akejkoľvek žiadosti zadosťučinenia. Okrem toho pomáha dávať dokopy vzťahy pomocou negatívneho rozprávania o sebe samom, čo zamestnanci nepochopia, že on je autorom emailov. Po vybudovaní vzťahu, je schopný získať všetky druhy informácií o cieľovom systéme.

Keď je vzťah vybudovaný, je množstvo spôsobov, ktorými môže byť zneužívaný. Ak sú si príliš podobní (útočník a obeť), môže sociotechnik vytvoriť rýchly vzťah prostredníctvom odhalenie cieľa. Ideou je, aby sa obeť cítila ako on a telefonujúca osoba myslela rovnako, mala rovnaké záujmy alebo očakávala rovnaké veci od života. Uveriť, že niekto má totožné alebo podobné vlastnosti ako on sám, poskytuje silný podnet, jednať s touto osobou kladne, dokonca dôverovať jej bez opodstatnenej pohnútky.

Zväčšenie zodpovednosti a mravnej povinnosti

Rozšírenie zodpovednosti nastáva vtedy, keď obeť má pocit, že nebude zodpovedná iba za svoje konanie. Paradoxne, tento faktor môže veľmi dobre spolupracovať s využitím

morálnej povinnosti, ako podnetu pre presviedčanie. Morálne povinnosti vstupujú do hry, keď obeť cíti, ako útočník robí niečo, pre záchranu zamestnanca, vypomáha spoločnosti, alebo dokonca sa chce vyhnúť pocitu viny.

Obeť má pocit, že robí rozhodnutia, v ktorých ide o rozdiel medzi úspechom a zlyhaním spoločnosti alebo „zamestnanec“, ktorý volá, naznačuje, že volajúci môže prísť o prácu na základe jeho rozhodnutia. Pre veľa ľudí je to veľmi zložité urobiť rozhodnutie a zamestnanec sa jednoduchšie poddá (prispôsobí), ak si myslí, že nie je zodpovedný za dané konanie.

Autorita

Ľudia sú určení reagovať na vedenie. Znamená to, že urobia veľa pre niekoho, o kom si myslia, že je nadriadený. Treba uvažovať s prípadom útoku, že zamestnanec bude vystupovať ako falošný riaditeľ, alebo viceprezident. Tento faktor je o to silnejší, o čo viac je útok príbuznejší realite s chýbajúcou výzvou na overenie identity autority. Nedostatok perspektívy zanecháva tento faktor široko otvorený na zneužívanie pre niekoho, kto si želá vystupovať ako daná autorita.

Bezúhonnosť a dôslednosť

Ľudia majú sklon pokračovať s povinnosťami na pracovisku, aj keď táto oddanosť možno nie je veľmi rozumná a na prvom mieste. Pre niekoho to je záležitosť bezúhonnosti „urobiť to, čo mi povedia, že mám urobiť “ dokonca aj keď má niekto podozrenie, že táto požiadavka nie je oprávnená. Ak sa hacker zmocní „zoznamu dovoleniek“, zamestnancova neprítomnosť môže byť zneužitá. Ďalšou stránkou tohto faktoru je, že ľudia majú tendenciu veriť ostatným, keď sa rozprávajú o svojich skutočných názoroch, že sú to ich rozhodnutia. Táto tendencia veriť ostatným je primárne založená na ich vlastnej čestnosti o vyjadrovaní pocitov [5].

Zneužitie dôvery

Vo väčšine prípadov majú sociotechnici veľké schopnosti pôsobiť na ľudí. Vedia byť okúzľujúci, zdvorilí. Je ľahké si ich obľúbiť – to sú vlastnosti potrebné k tomu, aby si získali porozumenie a dôveru iných. Skúsený sociotechnik, ktorý používa stratégiu a taktiku patriacu k jeho remeslu, je schopný získať prístup prakticky ku každej informácii.

Dômyselní technológovia vypracovali do „posledného detailu“ systémy ochrany informácií, aby zminimalizovali riziko spojené s používaním počítačov; zabudli ale na to najdôležitejšie – na ľudský faktor. Cez naše intelektuálne schopnosti zostávame my, ľudia, najväčším nebezpečenstvom pre svoju vlastnú bezpečnosť. [10]

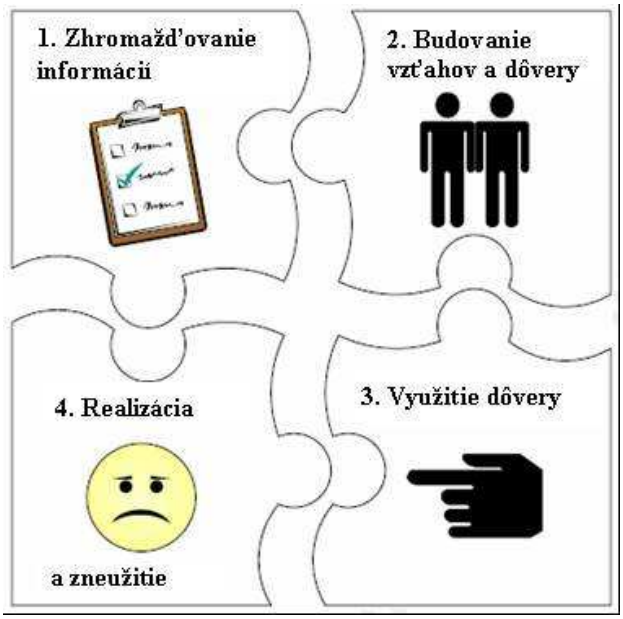
1.2 SOCIOTECHNICKÝ CYKLUS

Tak ako každý trestný čin má všeobecný vzor, tak aj všetky útoky sociálneho inžinierstva sú všeobecne uskutočňované podľa vzorovej schémy tiež nazvanej cyklus.

Každý útok sociálneho inžinierstva je jedinečný, pretože môže zahŕňať viacnásobné fázy/cykly a/alebo môže dokonca obsahovať iné techniky využívané pri útokoch, na dosiahnutie požadovaného koncového výsledku.

Sociotechnický cyklus sa skladá zo štyroch fáz, ktoré sú znázornené v nasledujúcom obrázku a sú to:

- **1.** *zhromažďovanie informácií*
- **2.** *budovanie vzťahov a dôvery*
- **3.** *využitie dôvery*
- **4.** *realizácia a zneužitie*



Obrázok č. 1 Sociotechnický cyklus

Zdroj: http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper040/WINKLER.PDF

1.2.1 ZHROMAŽĎOVANIE INFORMÁCIÍ

Rôznorodé techniky môžu byť použité útočníkom na zhromaždenie informácií o cieli. Keď nazhromaždí dostatočné množstvo informácií, môže ich použiť na budovanie medziľudských vzťahov buď s cieľovou osobou alebo niekým významným, kto mu pomôže dopracovať sa k úspešnému útoku.

Informácie, ktoré bývajú zhromažďované môžu, ale aj zároveň nemusia byť len tieto:

- telefónny zoznam
- dátum narodenia
- usporiadanie organizačnej štruktúry
- žargón

Do tejto fázy cyklu patrí aj prieskum, ktorý môže začať od analýzy voľne prístupných informácií ako sú finančné výsledky, katalógy, patentové prihlášky, články v odbornej tlači, obsah internetových stránok a tiež obsah smetných košov [17].

1.2.2 BUDOVANIE VZŤAHOV A DÔVERY

Sociotechnik môže bez obmedzenia využívať dôverčivosť napadnutého za účelom vytvorenie si vzťahu s ním. Pokiaľ prebieha rozvíjanie vzťahu, útočník si vybuduje dôvernú pozíciu, ktorú bude môcť potom využiť. Veľká dôvera ľudí môže spôsobovať nemalé problémy.

Na vytvorenie si čoraz väčšej dôvery, používajú najmä tieto typické sociotechnické techniky:

- Vydávanie sa za pracovníka tej istej firmy.
- Vydávanie sa za zástupcu dodávateľa, partnerskej firmy alebo štátneho úradu.
- Vydávanie sa za niekoho, kto má moc (napr. nadriadený).
- Vydávanie sa za nového pracovníka, ktorý prosí o pomoc.
- Vydávanie sa za predstaviteľa, či dodávateľa operačného systému s odporučením jeho neodkladnej aktualizácie.
- Ponúknutie pomoci v prípade nejakého problému, vyvolanie tohto problému a zmanipulovanie obeti, aby sama zatelefonovala s prosbou o pomoc.
- Zaslanie bezplatnej aktualizácie programu k inštalácii.
- Zaslanie vírusu alebo trójskeho koňa v prílohe elektronickej pošty.

- Použitie falošného dialógového okna, zobrazujúceho žiadosť o opakované prihlásenie alebo o zadanie hesla.
- Zaznamenávanie stlačených kláves pomocou špeciálneho programu.
- Podstrčenie diskiet alebo CD-ROM s nebezpečnými programami (*malware*) v okolí pracoviska obeti.
- Používanie vnútropodnikovej terminológie a žargónu s úmyslom vybudovať si dôveru.
- Ponúkanie 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 recepčnú, 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 [10, s. 334].

1.2.3 VYUŽITIE DÔVERY

Obeť býva zmanipulovaná sociálnym inžinierom, ktorému verí tak, aby prezradila informácie (napr. heslá) alebo vykonala opatrenia (napr. vytvorenie konta), ktoré by za normálnych okolností neurobila. Toto konanie môže byť koniec útoku, ale zároveň aj začiatok nasledujúcej etapy.
V tej to fáze môže sociotechnik žiadať o informácie alebo činnosť, ktorá je adresovaná obeti, alebo zmanipuluje obeť tak, aby sama poprosila o pomoc [17].

1.2.4 REALIZÁCIA A ZNEUŽITIE

Sociotechnik dokončí prácu požiadaním obete, aby mu prezradila dôležité informácie, alebo aby urobila nim zadané veci a dosiahnutím požadovaného cieľa sa sociotechnický cyklus končí.

Ale pokiaľ je získaná informácia alebo vykonaná činnosť iba ďalším krokom približujúcim útočníka k cieľu, vracia sa k predchádzajúcim bodom cyklu tak dlho, pokiaľ nedosiahne svoj cieľ.

2 METÓDY ÚTOKOV SOCIÁLNEHO INŽINIERSTVA

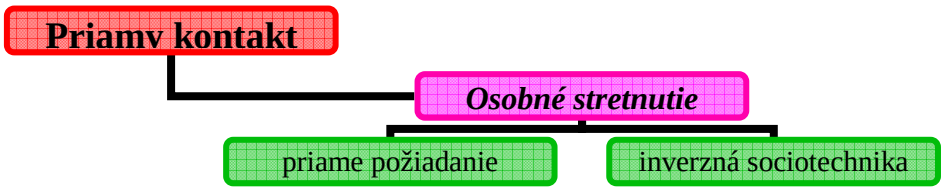
Metódy útokov sociálneho inžinierstva pri získavaní tajných informácií sa dajú vo všeobecnosti rozčleniť podľa viacerých kritérií.

Jedným z delení môže byť delenie na ***tvrdé*** a ***mäkké*** spôsoby útoku.

- ***Mäkké*** metódy vychádzajú z ľudskej dôverčivosti a ochoty pomôcť. Ide najmä o zneužitie nič netušiaceho pracovníka a to formou mailu, telefónu, listu alebo aj osobne
- ***Tvrdé*** využívajú ľudskú slabosť ako je úplatnosť, citové lability, vydierateľnosť, frustrácia z práce, pomstychtivosť, škodoradosť alebo závisť. V tejto skupine sociotechnik využíva vydieranie, poskytnutie sa ako nástroj pomsty alebo nadviazanie intímneho vzťahu s užívateľom.

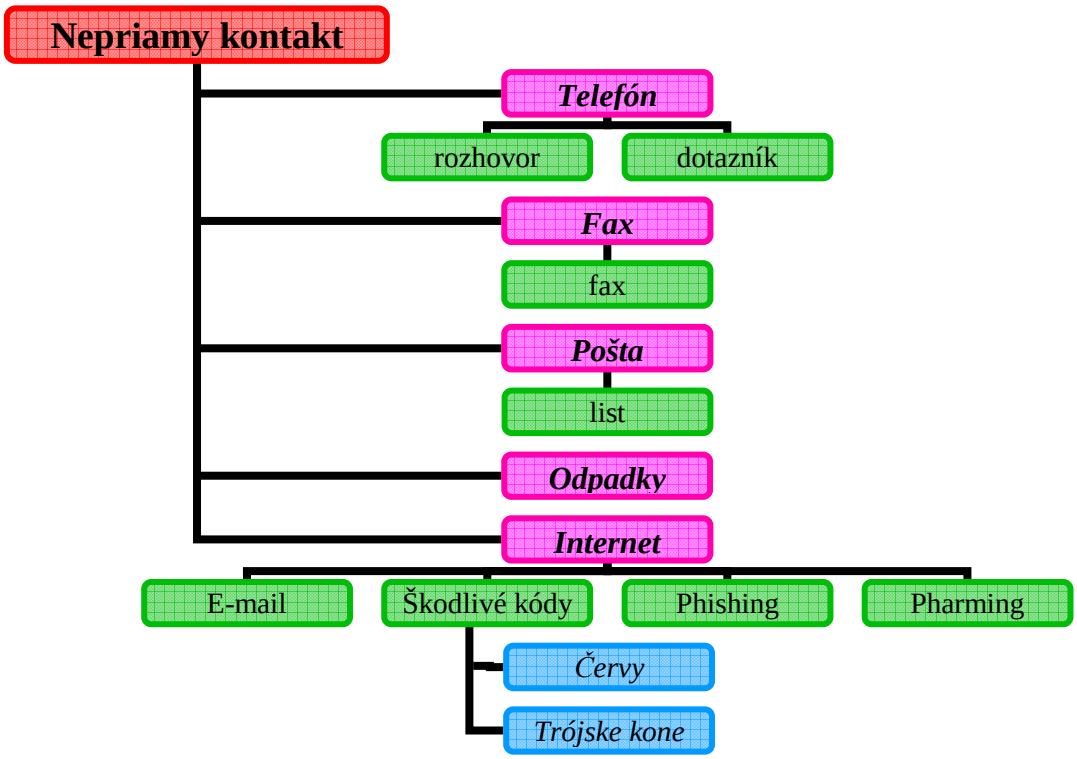
Ďalší spôsob delenia môže byť delenie podľa spôsobu kontaktu útočníka s obeťou na útoky s ***priamym*** a ***nepriamym kontaktom.***

- ***Priamy kontakt*** je využívaný pri *osobnom stretnutí* sociotechnika s obeťou či už pri jeho priamom požiadaní o potrebné informácie, alebo pri *inverznom*, tiež pomenovanom aj *obrátenom sociálnom inžinierstve*, kedy sociotechnik umelo vyvolá problém a čaká, pokiaľ ho poverená osoba/obeť požiada, aby eliminoval tento nežiaduci jav.



Obrázok č. 2 Schéma delenia priamych kontaktov
Zdroj: vlastný

- ***Nepriamy kontakt*** sa aplikuje pri využívaní technológií ako sú telefón, fax, pošta a internet. Nasledujúca schéma znázorňuje prostriedky, ktoré môže využiť sociálny inžinier pri jednotlivých technológiách.



Obrázok č. 3 Schéma delenia nepriamych kontaktov

Zdroj: vlastný

2.1 PRIAMY KONTAKT

Pri priamom kontakte dochádza k osobnému styku zamestnanca s útočníkom, ktorý sa snaží získať informácie o firme. Do tejto metódy patrí aj tzv. prevrátené alebo inverzné sociálne inžinierstvo.

2.1.1 PRIAME POŽIADANIE

Aj nasledujúci príbeh z praxe ukazuje o tom, akí sú sociotechnici šikovní a vedia sa dostať k napojeniu na firemnú sieť a získať významné dáta.

Útočník sa obliekol a upravil tak, aby vyzeral ako niekto z manažmentu, kto dobre zarába. Prišiel do firmy a povedal recepčnej, že sa má stretnúť s majiteľom. Popri čakaní na neho, si všimol neobyčajného výkonu recepčnej. Zaoberala sa niekoľkými vecami naraz, čo vnímal ako vlastnosť osoby, ktorá je zainteresovaná kariérou a rozvojom. keď potom povedal, že je z marketingu, pozoroval jej reakcie, či nezbadá nejaké znamenie bližšieho kontaktu medzi nimi. Dievča mu prezradilo, že jej snom je pracovať v marketingu. Tak si získal osobu, ktorú mohol zmanipulovať sľubom pomoci dostať sa k lepšej práci. Po dlhšom čakaní, sa jej opýtal, či by sa pre neho nenašla

nejaká voľná rokovacia miestnosť, kde by si mohol sadnúť a skontrolovať si poštu. Našiel svoju miestnosť, usadil sa, pripojil svoj notebook do zásuvky s firemnou sieťou a tak mohol stiahnuť všetky potrebné informácie. Votrelec použil dve techniky psychologickej diverzie – prvá bola plánovaná a druhá spočívala v improvizácii na okamžitú situáciu [10].

Ponaučenie: Šaty nerobia človeka. To, že je niekto dobre oblečený a má dobré vystupovanie ešte neznamená, že je dôveryhodný. Riziko narušenia bezpečnosti zvyšuje aj povolenie vstupu cudzích osôb do miest, kde je možnosť pripojiť sa do firemnej siete.

2.1.2 INVERZNÁ SOCIOTECHNIKA

Jedným z najúčinnejších sociotechnických trikov je obrátenie situácie. Sociotechnik vytvára problém a následne ho zázračne „lieči“, pričom vyláka od obete informácie o prístupe k najviac stráženým firemným informáciám.

Všetci pociťujeme vďaku, keď nám niekto, kto niečo vie, rozumie sa a je skúsený ponúkne pomoc pri riešení našeho problému. Sociotechnik si to uvedomuje a vie, ako túto skutočnosť využiť.

Tiež sa vyzná v tom, ako vyvolať problém a následne získať vďačnosť obete za jeho vyriešenie. Potom môže s obeťou manipulovať tak, aby sa dostal k informáciám alebo aby poprosil o drobnú službičku, v dôsledku ktorej ponesie obeť alebo firma straty. Nie je ale vylúčené, že si obeť nebude uvedomovať, že o niečo cenné prišla.

Existuje mnoho spôsobov, ako získať i tie najlepšie strážené firemné dáta. Jano, ktorého klient požiadal o získanie informácií si nakoniec vybral metódu vyžadujúcu taký úskok, ktorý mal obzvlášť rád: zmanipulovanie obete tak, aby sa sama na neho obrátila s prosbou o pomoc.

Jano si kúpil mobil a s totožnosťou firemného technika zavolal vybratej obeti a pripravil si situáciu tak, aby mu neskôr zavolala sama a požiadala ho o pomoc. Potom počkal 2 dni, aby to vyzeralo prirodzenejšie a zavolal na správu siete firmy. Prehlásil, že odstraňuje Tomášovi nejaký problém a poprosil o odpojenie jeho zásuvky. Tým bol Tomáš odrezaný od vnútornej siete firmy, bol zbavený možnosti sťahovať si súbory zo serveru, výmeny súborov s kolegami, čítanie pošty a dokonca aj tlače dokumentov. V dnešnom svete to znamená skoro návrat do jaskyne.

Po Tomášovej prosbe o pomoc, bol Jano samozrejme ochotný pomôcť kolegovi, ktorý bol odstrihnutý od sveta. Zavolal na správu siete a požiadal o opätovnú aktiváciu zásuvky svojej obete. Nakoniec, Tomáš ešte raz zvážil Janov návrh a súhlasil so skopírovaním programu na svoj počítač.

Samozrejme si neuvedomil, s čím vlastne súhlasil. Program, ktorý mal predchádzať výpadkom spojenia, bol v skutočnosti *trójsky kôň*. Tomáš po spustení programu nevidel, že by sa niečo dialo. Táto aplikácia navonok nič neukazovala, ani vtedy, keď inštalovala skrytý program umožňujúci špehovi skrytý prístup k počítaču[10]

Poučenie: Útočník obkľučuje obeť, presviedča ju, že má problém, ktorý vlastne neexistuje alebo, ako v tomto prípade, informuje o probléme, ktorý ešte nenastal, ale vyskytne sa v najbližšej budúcnosti (o to sa už útočník sám postará). Útočník sa potom predstaví ako človek, ktorý môže tento problém vyriešiť. Z prípadu vyplýva, že netreba prijať pomoc od každého, kto ju ponúkne.

2.2 NEPRIAMY KONTAKT

2.2.1 TELEFONÁT

Väčšina ľudí si myslí, že všetky sociotechnické útoky musia byť dôkladne premyslenou intrigou, tak zložitou, že je prakticky neodhaliteľná. Niektoré útoky sú prekvapivo úprimné, jednoduché. Niekedy sa proste stačí iba spýtať, o čom nasvedčuje aj príbeh.

„Je pondelok, pol jednej. Ideálny čas na obed“, hovorí si pán M., malý podnikateľ a živiteľ štvorčlennej rodiny. Nestihne sa však ani postaviť od stola, keď mu zazvoní telefón. Zo slúchadla naňho prehovorí príjemný ženský hlas, predstavujúc sa ako pracovníčka nemenovanej banky.
Ž.H.: „Pán M., potrebovala by som, pre zvýšenie spokojnosti a bezpečnosti pri vedení Vášho účtu overiť niekoľko údajov. Mali by ste na mňa, prosím, dve minútky?“
Pán M. trošku namrzene zašomre. Ponorí sa ešte hlbšie do kresla, je mu jasné, že telefonát bude dlhší, ako sľúbené dve minútky. V záujme bezpečnosti jeho dlhodobo hromadených úspor s rozhovorom nakoniec súhlasí.
Ž.H.: „Vy si nechávate potvrdzovať odchádzajúce a prichádzajúce platby prostredníctvom SMS správy, ak sa nemýlim...“

p.M.: „Nie, túto vašu službu zatiaľ nevyužívam.“

Ž.H.: „Ach, pardon, áno, už tu vidím poznámočku kolegynky. Takže svoje, platby cez Internet banking potvrdzujete iba prostredníctvom GRID karty?“

p.M.: „Áno, veď aj minule som vám na pobočke hovoril, že mi to stačí.“

Ž.H.: „Samozrejme, pán M., ale viete, bezpečnosť pri Internet bankingu je naozaj dôležitá, považujeme za svoju povinnosť informovať klienta o ponuke a predstaviť mu efektívnejšie prostriedky. K tým by sme sa ešte počas dnešného rozhovoru dostali. Rada by som Vás poprosila, keby sme mohli prejsť k spomínanej kontrole údajov. Vedeli by ste mi prosím povedať číslo z Vašej GRID karty pri pozícii D4?“

p.M.: „8417, bude tento rozhovor trvať ešte dlho?!“

Ž.H.: „Nie, sľubujem, že už iba dve minútky...iba si podľa jednotlivých pozícii overíme, či sedí vaše sériové číslo GRID karty, aby Vaše platby prebiehali absolútne bez komplikácii.... Na pozícii B6 by ste tým pádom mali mať uvedené číslo.....moment.... hneď to zistím..... ešte chvíľočku.....“

p.M.: „4943 a sériové číslo karty je 0007497205“

Ž.H.: „Ach, áno, práve to tu vidím, ďakujem. S rozhovorom sme takmer pri konci, skontrolujeme si iba, či sa viete bez problémov prihlásiť..... Vaše identifikačné číslo pri prihlasovaní je 0104456313?"

p.M.: „Ženská, máte vy vôbec otvorené moje záznamy?! Prihlasujem sa pod číslom 14628975.“

Ž.H.: „Prepáčte, hapruje nám tu systém, to viete – tie počítače. Už naozaj len posledná pripomienka – naša banka v rámci prevencii krádeží cez internet zaviedla povinnú zmenu hesla po dvoch mesiacoch. Vidím, že vy ste si heslo menili už veľmi dávno.“

p.M.: „To je pravda.“

Ž.H.: „Aké by ste chceli vaše nové heslo? Prosím, vyhláskujte mi ho.“

p.M.: „Počkajte... Dobre, už mám. Hláskujem: H ako Hana, A ako Andrej, B ako Beáta, E ako Eleonóra, S ako Samuel.“

Ž.H.: „HABES. V poriadku, ďakujem. Teraz už len overíme vaše staré heslo, aby sme si boli naozaj istí, že hovoríme s majiteľom účtu. Nadiktujte mi prosím vaše staré heslo, opätovne ho hláskujte.“

p.M.: „BALADA. B ako Beáta, A ako Andrej, L ako Laco, A ako Andrej, D ako Daniel, A ako Andrej.“

Ž.H.: „pán M., ďakujem veľmi pekne. Nemám ďalšie otázky, kontrolou sme zistili, že všetky Vaše údaje sú v absolútnom poriadku. Heslo vám bolo zmenené. Ďakujem Vám za trpezlivosť a čas, veľmi ste mi pomohli. Príjemný zvyšok dňa želám.....“ [12].

Ponaučenie: I keď volajúci pozná meno obete a predstaví sa ako pracovník dôveryhodnej inštitúcie, neznamená to, že je naozaj tým, za koho sa vydáva. Rozhodne tým nezískava oprávnenie k získaniu súkromných citlivých informácií a k manipulácii s nimi.

2.2.2 FAX

Nasledujúci príklad poukazuje na to, ako sa dá aj fax použiť na získanie dôležitých informácií, ktoré vlastní polícia.

Adam, ktorý cez internet zdarma distribuuje filmy, uspokojil svoj hlad po informáciách nasledovne. Najprv našiel číslo najbližšej pošty, zavolal tam a poprosil o číslo faxu. Potom zatelefonoval na oblastnú prokuratúru a požiadal ich o spojenie s archívom. Tu sa predstavil ako vyšetrovateľ a povedal, že by chcel hovoriť s osobou, ktorá má na starosti aktuálne povolenie k domovej prehliadke a prehlásenie. Poprosil ju o vytvorenie kópií a pre nedostatok času vyzdvihnúť si ich, ju požiadal, aby mu ich poslala faxom. Bol s tým malý problém, lebo fax sa nachádzal len v kancelárii zapisovateľov. Úradníčka od zapisovateľov povedala, že to s radosťou urobí, ale musí vedieť, kto to zaplatí. Potrebovala účtovný kód. Zavolal na sekretariát oblastnej prokuratúry, predstavil sa ako policajný dôstojník a opýtal sa priamo recepčnej, aký je účtovný kód kancelárie oblastnej prokuratúry. Bez váhania mu ho dala [10].

Poučenie: Nedať sa ľahko rozptýliť komplikovanými situáciami, nedostatkom času, emocionálnym stavom alebo vyčerpaním. Lebo v takýchto situáciách používame myšlienkové skraty, kedy sa rozhodujeme bez dôkladnej a úplnej analýzy informácií a reagujeme automaticky.

2.2.3 POŠTA

Útočník z predchádzajúceho príbehu mohol požiadať o odoslanie potrebných kópií pomocou listu, keby nemal tak naponáhlo, preto nebudem uvádzať príklad na zneužite poštových služieb sociálnym inžinierstvom.

Pri využití listov ako prostriedku na uskutočnenie sociotechniky sa veľmi často využíva zmena ich hlavičiek a podpisov, lebo nesú identitu niekoho z firmy, za koho sa sociotechnik skrýva.

2.2.4 ODPADKY

Udivujúce je množstvo informácií, ktoré sa dajú získať prehľadávaním odpadkov vyvážaných z firmy.

Veľa ľudí si neuvedomuje, čo vlastne vyhadzujú. Či sú to účty za telefón, výpisy z bankového účtu, obaly z liekov, materiály spojené s prácou, alebo mnoho iných vecí. Pracovníci vo firmách si musia uvedomovať, že existujú ľudia, ktorí hľadajú v odpadkoch využiteľné informácie.

Sociotechnik môže nájsť v odpadkovom koši veľa zaujímavých vecí. Môže tam získať informácie postačujúce k zahájeniu útoku na firmu, napríklad koncepty, harmonogramy, listy a podobné dokumenty, kde sa objavujú mená, oddelenia, pracovné postavenia, telefónne čísla i názvy realizovaných projektov. Smeti mu môžu dodať informácie o štruktúre firmy, plánoch výjazdov atď. Tieto detaily sa väčšinou zdajú ľuďom z danej organizácie nedôležité, ale pre útočníka sú veľmi cenné.

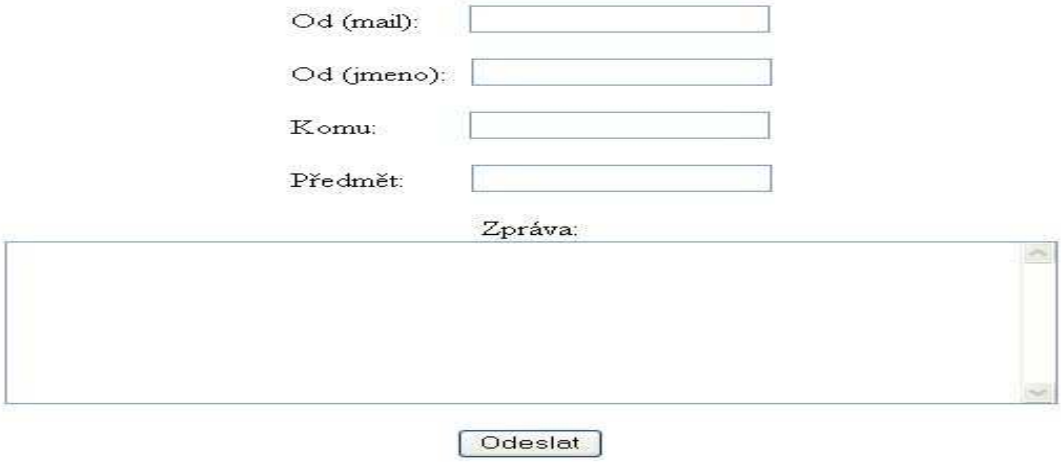
Preto by si mali, či už jednotlivci alebo firmy dávať väčší pozor na vyhadzované citlivé informácie nachádzajúce sa na papieroch, disketách, CD nosičoch, ... a zamerať sa na ich dôkladnejšiu likvidáciu, či už pomocou skartovacích zariadení, ktoré dokážu skartovať okrem papiera aj sponky, diskety, CD nosiče a kreditné karty, alebo ich fyzickým zničením. Ich likvidácia by mala byť taká kvalitná, aby z vyhodených nosičov informácií sociotechnik nebol schopný vyčítať informácie, ktoré by mu umožnili vykonať útok.

2.2.5 INTERNET

Veľa sociotechnických útokov prebieha práve cez internet, kde si útočník môže vybrať s viacerých variant ako čo najpresvedčivejšie nalákať obeť aby mu „padla rovno do pasce“. Môže využiť email, škodlivé kódy, či dokonca phishing alebo pharming.

E-MAIL

Veľmi často využívaný na sociotechniku je práve e-mail, v ktorom dokáže sociotechnik zmeniť jeho hlavičku či podpis, čím vyzerá dôveryhodne a nikoho by ani nenapadlo, že nie je od dolu podpísanej osoby. Na internetovej stránke s adresou *http://www.mozektevidi.euweb.cz/fakemail.php* existuje možnosť posielať e-maily so zmenenou identitou odosielateľa.



Obrázok č. 4 Ukážka možnosti odoslania e-mailu so zmenenou identitou odosielateľa

Ďalším zneužitím mailu bývajú jeho prílohy, ktoré môžu obsahovať toľko obávané vírusy. Aj keď si užívateľ dáva veľký pozor, neotvára a nepozerá si prílohy v elektronickej pošte, ktorých odosielateľov nepozná, používa antivírusové programy, aj tak sa môže stať obeťou vírusu. Čo ak dostane e-mail od priateľa alebo spolupracovníka, ktorý obsahuje prílohu s vírusom?

Táto technika je účinná, pretože sa ňou „dajú zabiť dve muchy jednou ranou“: možnosť šírenia vírusu nič netušiacej obeti a identifikáciu odosielateľa, ktorá vyvoláva zdanie, že správa je od dôveryhodnej osoby.

E-mail môže obsahovať reklamy, odkazy na iné internetové stránky alebo aj ponuky niečoho zadarmo, čo ani nechceme, a ani nepotrebujeme. Sťahovanie programov, o ktorých sme sa dozvedeli z reklamného e-mailu, klikanie na odkaz, ktorý nás prenesie na stránku, o ktorej sme nikdy predtým nepočuli, alebo otváranie príloh od niekoho, koho nepoznáme – to je všetko spôsob, akým sa dá na počítač zaslať nebezpečný program, ktorý je len jeden z prvkov útoku.

ŠKODLIVÉ KÓDY

Škodlivý kód je škodlivý softvér, ktorý má znepríjemňovať život užívateľovi alebo má prevziať čiastočnú resp. úplnú kontrolu nad jeho počítačom [9].

Medzi škodlivé kódy patria aj červy a trójske kone.

Červy

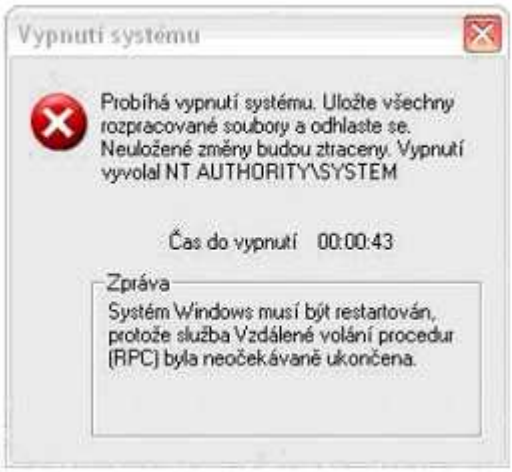
Červ je samostatný program, ktorý rozširuje svoje kópie pomocou internetu, alebo lokálnej siete. Klasický vírus je pasívny a na rozšírenie potrebuje kopírovanie nakazeného súboru, nepotrebuje na svoje šírenie hostiteľský program. Červ sa rozširuje aktívne, rozosielaním kópií po lokálnej sieti alebo internete využívajúc e-mailovú komunikáciu, prípadne na nižšej úrovni bezpečnostné diery operačného systému. Červ môže so sebou niesť aj ďalší škodlivý program, ktorý môže vykonať rozličné činnosti ako napr. inštalovať tzv. backdoor, ktorý umožní autorovi vzdialený prístup na počítač a nainštaluje sa bez vedomia klienta. Aj bez takéhoto "nákladu" môže červ spôsobiť veľké škody vplyvom zahltenia komunikačných kanálov. Dôsledkom rozšírenosti internetu je červ schopný rozdistribuovať sa po celom svete v priebehu niekoľkých hodín. Vedľajším efektom môže byť kompletné zahltenie siete, nevnímajúc podnikové LAN [9].

U červov spočíva sociotechnika v tom, že pri otvorení správy s určitým zaujímavým cieľom, ako napr. pornografia, alebo pri nahliadnutí na atraktívne internetové stránky sa bez vedomia užívateľa nainštaluje do počítača cez bezpečnostné chyby alebo diery internetového prehliadača.

Jedným z kritérií na rozlišovanie typov počítačových červov je podľa povahy šírenia a typu útoku:

- **e-mailový červ**, ktorý sa šíri na základe zoznamu adries v užívateľskom programe. Na svoje šírenie používa e-mailovú komunikáciu, pričom zneužíva chyby v programe. Napriek tomu však potrebuje aj ľudský prvok na to, aby sa mohol úspešne šíriť. Príklady e-mailových červov: Melissa, Klez, BugBear, W32/Kedebe-F, Zotob…

- **sieťový červ** sa po sieti šíri využívajúc chyby v serverových častiach programov, pričom sám aktívne vyhľadáva ďalšie servery vhodné na napadnutie. Vďaka tomu, že nepotrebuje k svojej činnosti ľudský prvok, je nebezpečnejší a ťažko ovládateľný. Príklady sieťových červov: CodeRed, Slapper, Sdbot.ABI, Randex.AJA [9].



Obrázok č. 5 Ukážka napadnutia MS Windows XP červom Lovsan
Zdroj: http://www.ikaros.cz/node/4048

Trójske kone

Trójsky kôň (trójan) je škodlivý program, ktorý na rozdiel od vírusov alebo červov nemá schopnosť samostatne sa kopírovať a infikovať súbory. Najčastejšie sa vyskytuje vo forme spustiteľného súboru s príponou „.exe“, alebo „.com“. Súbor neobsahuje v zásade nič iné okrem samotného škodlivého kódu. Najúčinnejšia metodika jeho odstránenia je jednoduchá - zmazanie. Trójsky kôň sa môže tiež vydávať za užitočný program. Tento typ infiltrácie má rozličné funkcie, od zasielania stlačených kláves (keylogger) až po mazanie súborov (napr. sformátovaním disku). Trojský kôň sa nazýva preto, lebo ide o súbor, ktorý sa chová ako neškodný program (napr. antivírus, komprimačný program).

Medzi základné trójske kone možno zaradiť:

- **Password – stealing trojan** (PSW) resp. Key Logger – skupina trójskych koní, ktorá obvykle sleduje jednotlivé stisky na klávesnici, ktoré ukladá a následne

odosiela na dané e-mailové adresy. Tento typ infiltrácie možno klasifikovať ako spyware.

- **Deštruktívne trójany** – klasická forma, pod ktorou je pojem trójsky kôň všeobecne chápaný. Pokiaľ je taký kôň spustený, likviduje dáta na disku alebo ho rovno kompletne sformátuje.
- **Backdoor** – ide o typ aplikácii, ktoré sú podobné programom pre vzdialenú správu počítača **RAT** (*Remote Access Tool*), akurát s tým rozdielom, že táto správa je vykonávaná bez vedomia samotného užívateľa.
- **Dropper** – škodlivý program najčastejšie typu .exe, ktorý nesie v sebe ďalšie škodlivé kódy,
- **Downloader** (*Trojan Downloader*) – jeho význam je podobný ako je to v prípade droppera, až na rozdiel toho, že downloader sa snaží stiahnuť škodlivý kód z pevne definovaných internetových adries.
- **Proxy trójan** – tieto trójske kone sa postarajú o to, že infikovaný počítač môže byť zneužitý pre rozosielanie spamu [9].

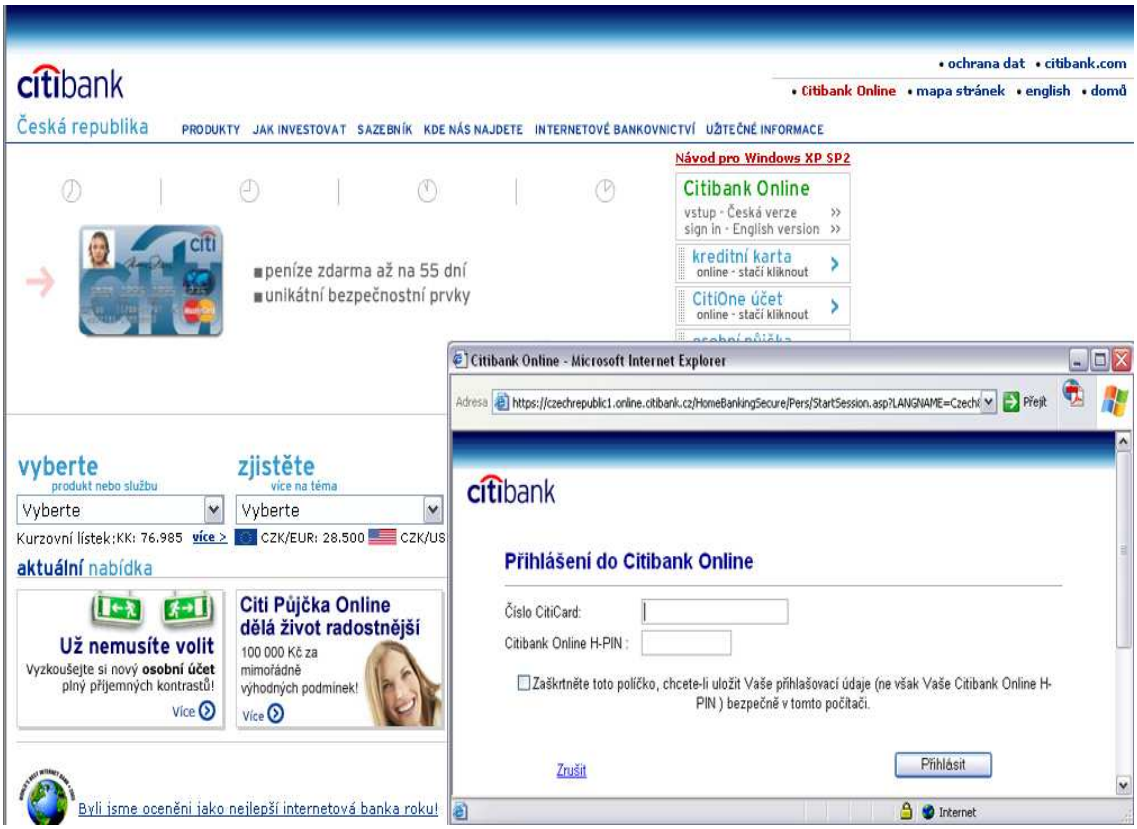
PHISHING

Phishing je formou nežiaducej aktivity, ktorá využíva prvky sociálneho inžinierstva. Týmto slovom sa označujú podvodné e-maily alebo web stránky. Ide o špeciálnu kategóriu nevyžiadanej pošty. Slovo phishing je odvodené z anglického slova *fishing* (rybárčenie) Na veľké množstvo adries sa rozošlú podvodné e-maily, ktoré na prvý pohľad vyzerajú ako informácie z dôveryhodnej inštitúcie (napr. banky). Príjemca je informovaný o údajnej nutnosti vyplniť údaje v pripravenom formulári, inak mu môže byť zablokovaný účet, prípadne môže byť iným spôsobom znevýhodnený. V e-maili býva uvedený odkaz na pripravené stránky s formulárom, ktoré akoby odkazovali na server dôveryhodnej inštitúcie. V skutočnosti je užívateľ presmerovaný na cudzí server, ale vytvorený v rovnakom dizajne, ako sú stránky „pravej“ inštitúcie. Obeť nemusí poznať rozdiel a môže vyplniť predvolené políčka, v ktorých sú od neho vyžadované dôverné informácie (napr. čísla účtov, kódy k internetovému bankovníctvu, PIN pre platbu). Takto získané údaje môžu podvodníci veľmi ľahko zneužiť [9].

Phishing je možné rozpoznať na základe dvoch znakov:

- podozrivé URL v paneli s adresou,

- neprítomnosť ikony zámku, ktorá reprezentuje bezpečné HTTPS spojenie.

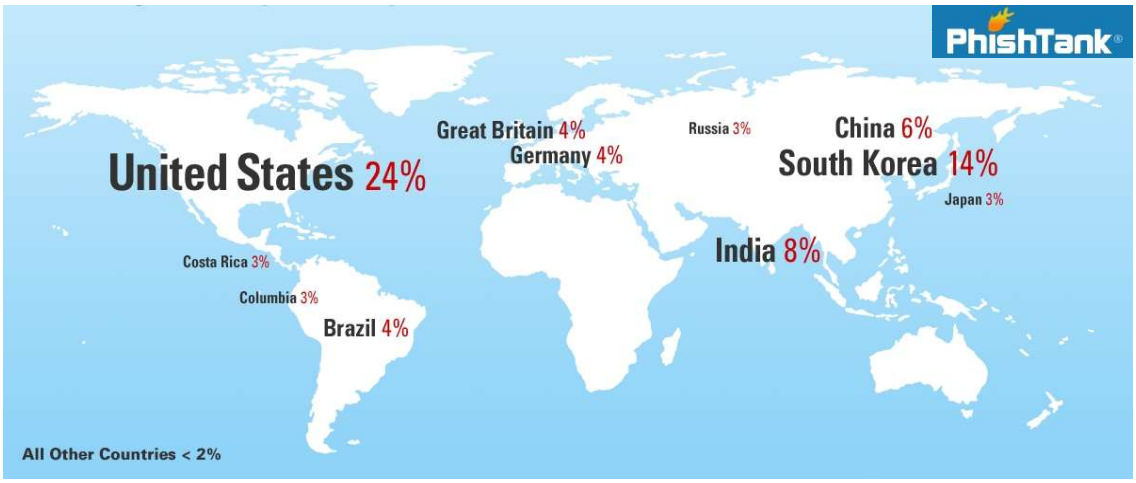


Obrázok č. 6 Phishing e-mailu a webovej stránky
Zdroj: http://www.ikaros.cz/node/4048

Najviac phishingových útokov prichádzalo podľa servera PhishTank sledujúceho trendy v e-mailových podvodoch z počítačov umiestnených v USA a v Južnej Kórey.

Databáza, ktorú prevádzkuje OpenDNS - výrobca anti-phishingového riešenia zaznamenala prostredníctvom informácií od dobrovoľníkov počas októbra 2006 3678 platných phishingových útokov, z ktorých 24% posielalo obete na servery umiestnené v USA. Ďalších 14% smerovalo na servery z Južnej Kórey. Tri štvrtiny všetkých phishingových útokov smerovalo obete do jedenástich krajín, vrátane napríklad Indie, Číny a Brazílie (Obrázok 7).

Komunita PhishTank dokáže rozoznať pravosť phishingového e-mailu v priemere za niečo viac než 18 minút. Najviac zneužívanými značkami pri phishingu sú EBay a jeho partner PayPal. Orientovalo sa na ne až 73% všetkých útokov. 80% e-mailov používalo v linku doménové meno (napríklad lugers.biz, web.com a podobne...), zvyšných 20% používalo IP adresu [16].



Obrázok č. 7 Výskyt phishingu vo svete v októbri 2006
Zdroj: http://www.phishtank.com/images/phish_world_map.gif

PHARMING

Najzákernejší spôsob, ktorým hacker môže pripraviť obeť o jej úspory, je *Pharming* (farmárčenie). Táto metóda spočíva v presmerovaní názvu www stránky na inú adresu. Každej mennej adrese napríklad ib.vub.sk prislúcha číselná adresa napríklad 215.5.214.144. Presmerovanie takejto adresy môže hacker uskutočniť napadnutím servera DNS, ktorý ukladá prístup k informácii o názve stroja a poskytuje mechanizmus získania jeho IP adresy priamo vo vašom počítači. Pomerne jednoduchým spôsobom sa dá toto nastavenie zmeniť. Ak zadá obeť mennú adresu do Vášho prehliadača, miesto stránky banky sa zobrazí jej dokonalá napodobenina. Teda ani nezbadá, že je na inej stránke. Po zadaní údajov, ich získa neoprávnená osoba, ktorá takúto falošnú stránku vytvorila. Proti takejto hrozbe sa môžete brániť rôznym spôsobom. Najjednoduchším spôsob je zistiť si číselný kód stránky internet bankingu. Stačí otvoriť príkazový riadok a zadať príkaz ping *adresa* (napr. ping ib.vub.sk). Potom miesto mennej adresy do prehliadača zadať číselnú adresu (napríklad https:// 215.5.214.144). Ďalšou možnosťou je overovanie platnosti certifikátu a upozornenie pri prechode zo zabezpečenej stránky na nezabezpečenú. Tieto funkcie sa dajú nastaviť v internetovom prehliadači. Niektoré banky sa proti takémuto spôsobu elektronického podvodu bránia tak, že ihneď po prihlásení do systému pošlú SMS s kódom, ktorý musí klient zadať alebo ho aspoň upozornia, že sa niekto prihlásil k jeho účtu [11].

Po zhrnutím všetkých sociotechnických útokov vyplýva, že majú jeden spoločný prvok: *podvod*. Obeť je väčšinou presvedčená, že útočník je kolega z práce alebo iná osoba oprávnená k prístupu k dôverným informáciám, prípadne niekým poverená vydávať

príkazy, ktoré sa viažu s vykonávaním činností na počítači, či podobnom zariadení. Čiže je to osoba, ktorá zmenou svojej identity získava potrebné informácie na dosiahnutie požadovaného cieľa.

Je veľmi málo, alebo takmer vôbec nie sú štatistiky týkajúce sa tohto problému, pretože osoby alebo firmy, na ktoré sociotechnik použil svoje schopnosti a zručnosti, si len málokedy uvedomujú, že sa stali jeho obeťou. A zároveň, ktorá firma by sa pochválila, že podľahla útoku, a tak si pokazila svoju reputáciu na verejnosti?

Štúdia na internetovej stránke www.pcrevue.sk z 22. 1. 2007 sa zaoberá množstvom peňazí, o ktoré prišli nižšie uvedené krajiny v dôsledku zámeny identity. Podľa americkej Federálnej komisie pre obchod (Federal Trade Commission) len ročná hodnota škôd z krádeže identity pre jednotlivca a podniky v USA dosahuje vyše 50 miliárd dolárov. Britské ministerstvo vnútra vypočítalo, že britská ekonomika zaplatila za krádeže identity v uplynulých troch rokoch cenu okolo 3,2 mld. dolárov. Odhady austrálskeho Centra pre politický výskum (Centre for Policing Research) vyčísľujú každoročné škody spôsobené krádežou identity na sumu 3 miliárd dolárov [1].

Uvedené sumy nie sú zanedbateľné finančné čiastky, a aj preto by sa mali firmy viac zaoberať ich bezpečnostnou politikou. Veľmi dôležitá je informovanosť zamestnancov o tejto zákernej hrozbe, ktorá môže striehnuť na každý podnik a možnosti jej predchádzania, s ktorými by sa mali pracovníci oboznámiť na školeniach.

3 OCHRANNÉ OPATRENIA PROTI SOCIÁLNEMU INŽINIERSTVU

V dnešnom stále meniacom sa svete, je dôležité byť dobre oboznámený s technikami sociálneho inžinierstva a protiopatreniami schopnými zredukovať pravdepodobnosť jeho úspechu. S týmito vedomosťami každý môže zaistiť vhodné (preventívne, detektívne a nápravné) opatrenia, ktoré sú používané na ochranu personálu a aktív organizácie.

Útoky sociálnych inžinierov sa netýkajú len právnických osôb ale aj fyzických osôb. Preto by sa ochranným opatrenia zameraným proti sociálnemu inžinierstvu mali zaoberať nie len podniky ale aj ľudia v domácnostiach, ktorí by si mali rozšíriť obzor pôsobenia sociotechniky ak nechcú, aby ich osobné údaje boli používané niekým iným, napríklad na prístup k ich účtu, čím by mohli prísť o úspory.

K faktorom uľahčujúcich útok sociálneho inžiniera patrí aj:

- Veľký počet zamestnancov, ktorí sa navzájom nepoznajú,
- Chýbajúce školenia z oblasti bezpečnosti,
- Chýbajúca klasifikácia dát,
- Neoverovanie totožnosti osoby, ktorá žiada o informácie alebo činnosti,
- Nesprávna tvorba hesiel,
- Nevhodná likvidácia odpadu s citlivými informáciami, ...

Prevencia pred sociálnym inžinierstvom spočíva v poučení ľudí o hodnote informácií, zaškolení, ako ich majú ochraňovať a v upovedomení ich o tom, ako sociotechnici pracujú. Informovanie zamestnancov vo firmách o existencii sociotechniky a jej prevencii, by malo byť vykonávané na bezpečnostných školeniach zaoberajúcich sa bezpečnostnou politikou firmy.

„Bezpečnostná politika je chápaná ako základný dokument subjektu, obsahujúci predstavu vedenia o riešení bezpečnosti a základné požiadavky na jednotlivé bezpečnostné oblasti celého informačného systému. Vedenie subjektu by malo stanoviť jasný smer postupu v oblasti bezpečnosti informácií, ukázať jej podporu vydaním a aktualizáciou politiky bezpečnosti informácií platnej pre celú organizáciu. V každom

prípade by sa malo jednať o dokument písomný, ktorý by mal odpovedať na niekoľko základných otázok:
Čo chce právnická osoba chrániť?
Prečo to chce chrániť?
Ako to chce chrániť?
Čo bude robiť, keď dôjde k zlyhaniu systému?

Bezpečnostná politika obsahuje súhrn bezpečnostných požiadaviek pre riešenie informačnej bezpečnosti na úrovni fyzickej, personálnej, administratívnej, počítačovej a komunikačnej bezpečnosti a bezpečnosti vývojového prostredia.

Definovanie personálnych právomocí a zodpovedností jednotlivých pracovníkov, je prvým krokom pri vytváraní bezpečnostnej politiky“ [3].

Je nevyhnutné, aby na pracovisku existoval systém účinných opatrení proti možnému sociálnemu inžinierstvu. Ide o jasne zadefinované pravidlá správania sa na pracovisku, či už v podobe etických kódexov, kódexov správania sa prípadne inej formy vnútropodnikových predpisov, na základe ktorých by zamestnanec vnímal tieto normy ako záväzné, a vďaka ktorým by bolo možné vyžadovať ich dodržiavanie alebo postihovať ich porušenie. Malo by byť v záujme samotného zamestnávateľa, aby takýto systém pravidiel na pracovisku existoval, a aby sa trvalo na jeho dodržiavaní.

3.1 ŠKOLENIE

Každý je potenciálne vystavený nebezpečenstvu sociálneho útoku, preto jedinou možnou ochranou firmy sú príslušné školenia a vzdelávanie pracovníkov, ktoré učí rozpoznávať sociotechnikov a metódy, ktorými sa snažia získať prístup k dátam.

Zásady bezpečnosti nie sú univerzálne. Osadenstvo firmy má väčšinou rôzne úlohy a s každou pozíciou v práci sa viaže iné nebezpečenstvo. Mala by existovať istá základná úroveň školenia. Ľudia by mali prejsť školením zodpovedajúcim ich druhu práce a plnených povinností, čo umožní znížiť pravdepodobnosť výskytu problémov. Zamestnanci musia mať na pamäti pravidlá bezpečnosti, ktoré sú šité na mieru potrebám, veľkosti a zvyklostiam ich firmy. [10, s.86].

Prvým a najdôležitejším krokom pri školení, je oboznámenie každého člena organizácie, o existencii ľudí bez zábran, ktorí sa pokúšajú s nimi manipulovať pomocou podvodov a psychologických metód. Pracovníci musia vedieť, ktoré informácie treba chrániť a ako. Keď pochopia, ako môžu byť zmanipulovaní, budú schopní dostatočne včas útok rozoznať.

Sociotechnika, už v definícii zahrňuje istý druh interakcie medzi ľuďmi. Útočník na ceste k cieľu často využíva veľa komunikačných metód a technológií. Preto by mal dobre prepracovaný program informovanosti o hrozbách obsahovať niektoré alebo všetky nasledujúce body:

- Popis, ako útočníci používajú sociotechniku, aby oklamali ľudí.
- Metódy, ktoré sociotechnici používajú, aby dosiahli požadovaný cieľ.
- Ako postupovať v prípade podozrenia, že ide o sociotechnický útok.
- Zhrnutie bezpečnostnej politiky a vysvetlenie významu jednotlivých jej aspektov.
- Povinnosť prispôsobiť sa pokynom bezpečnostnej politiky a dôsledky v prípade ich nedodržiavania.
- Klasifikácia informácií a prostriedky jej ochrany.
- Procedúry ochrany citlivých informácií vrátane vedomostí existujúceho systému klasifikácie dát.
- Postup poskytovania dôverných informácií alebo materiálov.
- Nutnosť overovania identity každej osoby, ktorá prišla s podozrivou žiadosťou o poskytnutie informácií alebo vykonanie nejakej činnosti.
- Bezpečnostné praktiky spojené s heslami umožňujúcimi prístup k počítačom.
- Spôsob používania elektronickej pošty, nutnosť jej šifrovania a ochrany pred odcudzením e-mailov obsahujúcich citlivé informácie.
- Bezpečnostné požiadavky, spojené so systémom kontroly a riadenia vstupov ako aj povinnosť nosenia identifikátoru (visačiek).
- Vhodné spôsoby odstraňovania dôverných dokumentov a dátových nosičov, ktoré obsahujú dôverné materiály alebo ich obsahovali v minulosti.

Dobrý program školenia musí súčasne informovať, pútať pozornosť a vzbudzovať poslucháčov. Školenie a udržovanie povedomia o bezpečnosti musí zaujímať pozornosť a byť interaktívnou skúsenosťou. Používané techniky môžu demonštrovať sociotechnické metódy pomocou scénok a rozdelením rolí, prehľadu správ o posledných

prípadoch útokov na smoliarske firmy a preberanie spôsobov, ako by sa tomu mohla firma vyhnúť.

Väčšina ľudí považuje za obťažujúce všetko, čo im prekáža pri práci a preto môžu začať obchádzať všetky bezpečnostné prostriedky, ktoré sa zdajú byť len stratou času. Kľúčová je teda motivácia zamestnancov ich vzdelávaním a poučovaním tak, aby sa myslenie na bezpečnosť stalo súčasťou ich každodenných povinností.

Pracovníkom, ktorí odhalili sociotechnický útok a zabránili mu, alebo sa inak zaslúžili o úspech informačného bezpečnostného systému, má byť vyjadrené uznanie formou odmien, ktoré by ich motivovali. Existencia systému odmien by mala byť oznamovaná pracovníkom na všetkých akciách týkajúcich sa bezpečnosti a všetky prípady porušenia bezpečnostných zásad by nemali byť tolerované.

3.2 OPAKOVANIE ŠKOLENÍ A PENETRAČNÉ TESTY

Školenia „osviežujúce znalosti“ by mali byť organizované aspoň raz ročne. Podstata ohrozenia a používané metódy podliehajú stálym zmenám, preto musí byť program školenia aktualizovaný. Naviac sa ostražitosť s časom zmenšuje, a preto musia byť školenia pravidelne opakované, aby sa povedomie dôležitosti dodržovania bezpečnostných zásad upevnilo. Musí byť tiež udržiavaná motivácia pracovníkov k ich dodržiavaniu, napríklad odhaľovaním najaktuálnejších hrozieb a metód, ktoré boli zaznamenané za posledné obdobie.

Informácie sú to najcennejšie, čo môže spoločnosť mať. Musí preto spraviť všetko pre ich ochranu. Práve na podporu ochrany, konkrétne na identifikovanie slabých miest v ochrane, slúžia penetračné testy.

Penetračný test je jednou z najlepších metód detailného odhalenia chýb a slabín, pomáha IT špecialistom dosahovať ciele, riešiť problémy a zabezpečiť nenarušiteľný chod systémov, serverov, kritických aplikácií a iných technológií. I ten najbezpečnejší systém, či aplikácia má svoju slabinu, ktorú je potrebné nájsť a eliminovať.

Cieľom vykonávania penetračných testov je kontrolovane verifikovať bezpečnostné chyby, ktoré môžu ovplyvniť funkcie systému, kritických aplikácií a iných technológií.

Penetračné testy nemôžu byť videné ako komplexné audity bezpečnosti celej siete, nemôžu analyzovať každú možnú slabinu systému. Prakticky približujú a určujú body slabín bezpečnostnej infraštruktúry spoločnosti, hľadajú chyby a napomáhajú vyobraziť plán implementácie prostriedkov ochrany založenej na zavedených prioritách spoločnosti. Práve tieto priority rozhodujú o bezpečnostnej politike a množstve a razantnosti slabín bezpečnostného charakteru operačných systémov a softvérov.

Ciele penetračného testu

- vyhľadať či útočník môže preniknúť do systému a vyhodnotiť bez ďalších informácií spoločnosti dosiahnuteľnosť legitimity užívateľa,
- stanoviť pravdepodobnosť, či špecifický systém môže byť otvorený pre útočníka s určitými právami počítača pripojeného do siete spoločnosti,
- stanoviť bezpečnosť systému, nadobúdajúc schopnosť prekročiť práva normálneho užívateľa,
- prevádzkovať evidenciu verifikovanej možnosti nájdenia zraniteľného miesta a typu exploitu,
- stanoviť organizačný stupeň odhalenia útočníka na informačnú bezpečnosť spoločnosti [114]. .

Firmy, ktoré prevádzajú penetračné testy bezpečnostných systémov uvádzajú, že pokusy nabúrať sa do počítačového systému zákazníka pomocou sociotechnických metód sú skoro stopercentne účinné. Technické zabezpečenia môžu takéto útoky znížiť tým, že minimalizujú účasť ľudí v rozhodovacom procese. Jedinou skutočne účinnou metódou oslabenia tohto ohrozenia je použitie technologických zabezpečení v kombinácii s bezpečnostnými postupmi, ktoré určujú základné princípy chovania pracovníkov [10].

Penetračné testy majú tiež svoj životný cyklus. Ak sú dodržané cykly testov v určitých pravidelných obdobiach, ktoré konkrétne na mieru navrhnú špecialisti pre oblasť penetračných testov a na základe výsledkov sa budú implementovať opravy, dosiahne sa tak želaná vysoká bezpečnostná úroveň systémov, serverov, kritických aplikácií a iných technológií.

3.3 KLASIFIKÁCIA DÁT

Prienik do zabezpečenej firmy často začína od získavania informácií, či dokumentu, ktorý je zdanlivo bezvýznamný, všeobecne dostupný a nie príliš dôležitý. Väčšina ľudí v organizácii nevidí dôvod, prečo by mal byť chránený.

Základom školenia je oboznámiť zamestnancov s rozdelením dát do jednotlivých skupín podľa obsahu ich dôležitosti a zhrnúť metódy, ktoré by mohol použiť sociotechnik, aby k nim získal prístup a vedeli ako ich majú chrániť a kto má právo na prístup k nim.

Informácie by mali byť roztriedené na rôzne úrovne v závislosti na stupni ich citlivosti. Každá firma má svoju vlastnú klasifikáciu a rozdelenie dát v závislosti na ich počte a type dôvernosti. Malé podniky mávajú klasifikáciu väčšinou trojstupňovú a stredné a veľké firmy štvorstupňovú. Čím je klasifikácia zložitejšia, tým nákladnejšie bude školenie pracovníkov a dodržiavanie pokynov.

Tajné:

- najdôvernejšie informácie,
- obchodné tajomstvo, technické alebo funkčné špecifikácie, ktoré by mohol využiť konkurent,
- určené iba k vnútornej potrebe firmy,
- sprístupnené sú len veľmi obmedzenému počtu osôb, ktorí ich nevyhnutne potrebujú,
- uložené mimo bežných informácií a šifrované tak, aby odpovedali štandardom v aktuálnej dobe
- ich prezradenie nepovolanej osobe môže mať vážne dôsledky pre firmu, jej akcionárov, partnerov či klientov.

Súkromné:

- informácie osobnej povahy, ktoré sú určené pre vnútornú potrebu organizácie,
- výsledky lekárskych prehliadok pracovníkov, informácie o bankovom konte, história výplat a všetky ďalšie osobné identifikačné údaje, ktoré nie sú určené verejnosti,
- informácie, ktoré presne špecifikuje zákon o ochrane o osobných údajoch,
- maximalizácia ich bezpečnosti a zväčšovanie povedomia zamestnancov o nakladaní s týmito dátami, ak k nim majú prístup,

- ich neoprávnené sprístupnenie môže mať veľký vplyv na pracovníka alebo na firmu.

Vnútorné:

- môžu sa sprístupniť každému zamestnancovi firmy,
- všetky informácie bežne používané pri činnosti a nemali by byť známe navonok, napr.: organizačná štruktúra, názvy vnútorných systémov, procedúry vzdialeného prístupu, účtovné kódy,
- ich sprístupnenie neoprávnenej osobe, nemôže spôsobiť väčšiu škodu firme, obchodným partnerom, zákazníkom ani pracovníkom,
- sociotechnik ich môže využiť na vydávanie sa za oprávneného pracovníka či dodávateľa a oklamať nejakého pracovníka, z ktorého vymámi informácie s väčším stupňom dôvery,
- pred ich sprístupnením tretím osobám, ako sú dodávatelia, brigádnici či partnerské firmy, by sa s nimi mala podpísať zmluva o dôvernosti týchto údajov.

Verejné:

- určené verejnosti,
- informácie komerčného charakteru, slúžiace hlavne na propagáciu spoločnosti, predaj tovarov a služieb za účelom vytvorenia zisku,
- kontaktné informácie pre zákazníkov, katalógy výrobkov,
- môžu byť ľubovoľne šírené,
- každá informácia, ktorá nie je určená pre verejnosť, by mala byť považovaná za dôvernú [7] .

3.4 OVEROVANIE TOTOŽNOSTI ŽIADATEĽA O INFORMÁCIE ALEBO ČINNOSTI

Aby zlodeji informácií získali prístup k tajným informáciám, používajú prevažne ľsti – vydávanie sa za pracovníkov firmy, dodávateľov alebo obchodných partnerov. Aby sa zaistila efektívna ochrana informácií, musí pracovník, žiadaný o vykonanie nejakej činnosti alebo o poskytnutie dôvernej informácie, previesť pozitívnu identifikáciu volajúcej osoby a overiť, či má oprávnenie skôr, ako žiadosti vyhovie.

Do plánu bezpečnostného školenia by sa mal pridať bod, ktorý sa týka skutočnosti, že i keď volajúci alebo návštevník pozná mená nejakých osôb z podniku, alebo ovláda žargón a postupy, neznamená to, že je naozaj tým, za koho sa vydáva. Rozhodne tým nezískava oprávnenie k získaniu vnútorných informácií alebo k práci na podnikovom počítači. Preto si zamestnanci majú osvojiť pravidlo, že v prípade pochybností sa musí hlavne overovať.

Na školení sa zamestnanci učia odmietať pomoc alebo zverejnenie dôverných informácií ľuďom, ktorých nepoznajú osobne, dokonca i v tom prípade, keď sa žiadateľ vydáva za niekoho z vedenia. Overovacie postupy sa majú používať dokonca i vtedy, keď to znamená odmietnutie pomoci člena vedenia, ktorý sa snaží bezpečnostné štruktúry obísť.

Pracovníci nemusia odmietnuť pomoc a overovať totožnosť žiadateľa, pokiaľ spadá do výnimiek týkajúcich sa nasledujúcich situácií:

- Žiadosť pochádza od človeka, ktorého pracovník pozná, a ktorý ho požiada osobne, alebo jeho hlas v telefóne bezpochyby pozná,
- Po pozitívnom overení totožnosti žiadateľa podľa schválených pokynov,
- Keď bola žiadosť potvrdená nadriadeným alebo inou osobou na zodpovednej pozícii, ktorá osobne pozná človeka, ktorý o službu žiada [10, s.212] .

Ale keď žiadosť pochádza od osoby neoverenej musí sa vykonať proces verifikácie, aby bola žiadajúca osoba jednoznačne identifikovaná ako oprávnená dostať danú informáciu a obzvlášť pokiaľ sa žiadosť týka vykonania nejakej činnosti. Tento proces je základným zabezpečením pred sociotechnickými útokmi: pokiaľ budú pracovníci postupovať podľa overovacích procedúr, radikálne sa zníži účinnosť sociotechnických útokov.

Proces overovania žiadosti, či je odôvodnená, pri jej prijatí z komunikačných kanálov ako je telefón, e-mail alebo fax sa skladá z nasledujúcich krokov:

1) Overenie totožnosti:
   Identifikácia volajúceho – zistenie či je telefonát z firmy alebo z vonka a či číslo volajúceho zodpovedá menu, ktoré volajúci uviedol,

Spätné volanie – vyhľadanie volajúceho v telefónnom zozname a zavolanie mu späť na nájdené číslo, nie na číslo ktoré uviedol a tak sa uistiť, či je pracovníkom firmy,

Záruka – volajúceho overuje dôveryhodná osoba, ktorá ručí za žiadateľovu identitu,

Spoločné tajomstvo – použitie vnútorného spoločného firemného tajomstva, napr. hesla alebo denného kódu,

Vedúci alebo nadriadený volajúceho – telefonát bezprostredne nadriadenému volajúceho so žiadosťou o overenie,

Bezpečný e-mail – vyžaduje sa elektronický list s elektronickým podpisom,

Identifikácia hlasu – osoba, ku ktorej je smerovaná žiadosť, pozná žiadateľa natoľko dobre, aby rozoznala jeho hlas v telefóne vie, či je žiadateľ dôveryhodná osoba alebo nie,

Osoba s identifikátorom – osoba príde so žiadosťou za zamestnancom osobne, ktorý si môže overiť jej identitu pomocou identifikátoru (útočník ale môže identifikátor ukradnúť alebo si vytvoriť falošný) [10, s.271] .

2) <u>Overenie statusu pracovníka, či je ešte stále zamestnancom firmy:</u>

Kontrola zoznamu pracovníkov – ak má firma vo vnútornej sieti sprístupnený zoznam skutočného stavu pracovníkov, treba overiť, či sa na tomto zozname nachádza,

Overenie u nadriadeného – zavolanie nadriadenému volajúceho na číslo uvedené vo vnútornom telefónnom zozname, nikdy nie na číslo, ktoré uviedol žiadateľ,

Overenie na oddelení – zistenie, či žiadateľ je zamestnancom oddelenia ktoré uviedol, opýtaním sa niektorej osoby z oddelenia.

3) <u>Overenie oprávnenia k informáciám:</u>

Overenie zoznamu funkcií, pracovných skupín, pracovísk – firma by mala mať sprístupnené zoznamy popisujúce oprávnenie jednotlivých pracovníkov k rôznym informáciám,

Získanie oprávnenia od nadriadeného – pracovník sa skontaktuje so svojím alebo žiadateľovým nadriadeným, aby získal autorizáciu danej žiadosti,

Získanie autorizácie od vlastníka informácie alebo od ním poverenej osoby – vlastník informácie je konečná autorita v otázke, či má daná osoba nárok na informácie. Pri žiadosti sa musí pracovník spojiť s nadriadeným volajúceho, aby mu schválil prístup alebo priamo s vlastníkom informácie,

Získanie autorizácie pomocou zodpovedajúceho systému – veľké firmy môžu mať účelne vytvorené softwarové balíky s databázou obsahujúcou zoznam pracovníkov s ich právami k chráneným informáciám [10, s.273].

3.5 HESLÁ

Správne používaný bezpečnostný kód tvorí dôležitú ochrannú bariéru. Nesprávne používaný kód je horší, ako keby nebol žiadny, pretože vytvára ilúziu bezpečia , ktorá v skutočnosti neexistuje. Načo sú kódy, ich zamestnanci neudržia v tajnosti?

Školenie v oblasti bezpečnosti sa musí zaoberať tiež heslami, najmä tým, kedy a ako ich meniť, z čoho sa skladá prípustné heslo a aké riziko sa skrýva v angažovaní iných osôb do tohto procesu. Správna tvorba hesiel je bližšie popísaná v ďalšej podkapitole s názvom Bežní užívatelia. Školenie musí pracovníkov dôrazne upozorňovať na skutočnosť, že *každá* požiadavka spojená s heslom je podozrivá.

Heslá sú dôverné informácie, s ktorými treba pracovať veľmi opatrne, ostražito a dodržiavať nasledovné body, aby sa zabránilo ich úniku až k útočníkovi:

- Heslá nemôžu byť pod žiadnou zámienkou poskytované cez telefón,
- Svoje heslo bez písomného súhlasu zodpovedného vedúceho z oddelenia informatiky nesmie byť poskytnuté nikomu,
- Na internetových stránkach sa nikdy nepoužívajú podobné alebo rovnaké heslá ako vo firemnom počítačovom systéme,
- Žiadny užívateľ nemôže znovu použiť rovnaké alebo podobné heslo skôr, ako po osemnástich mesiacoch od jeho posledného použitia,
- Nemôžu sa používať heslá, kde jedna časť ostáva bez zmeny a druhá sa mení podľa predvídateľného vzorca, napr.: Kevin01, Kevin02, ...
- Heslo sa môže poznamenať len vtedy, pokiaľ je odložené na bezpečnom mieste ďaleko od počítača, alebo iného heslom chráneného zariadenia,
- Heslá by nemali byť vo forme prostého textu uložené v žiadnom súbore na počítači, alebo ako text objavujúci sa po stisku funkčnej klávesy. V prípade nutnosti sa dajú heslá zapísať pomocou šifrovacieho nástroja schváleného oddelením informatiky a vyhnúť sa tým hrozbe, že heslo odhalí neoprávnená osoba [10].

Vzhľadom na to, že heslo je taká citlivá informácia, mal by sa veľký dôraz dávať aj na jeho tvorbu. Preto, by správne vytvorené heslo malo vyhovovať nasledujúcim požiadavkám:

- Musí sa skladať aspoň z ôsmich znakov v prípade bežného užívateľského účtu, a aspoň dvanástich znakov u privilegovaných kont,
- Musí obsahovať aspoň jednu číslicu, aspoň jeden symbol (napr.: $, _, %, ?, !) aspoň jedno malé a aspoň jedno veľké písmeno,
- Nemôže to byť žiadny výraz z ľubovoľného jazyka, výraz spojený s rodinou, autom, prácou, registračnými značkami, rodným číslom, menom psa či iného domáceho miláčika, dátumom narodenia, ani to nemôže byť fráza obsahujúca tieto výrazy,
- Nemôže to byť obmena predchádzajúceho hesla s jednou časťou nemennou a s druhou meniacou sa napr. podľa aktuálneho mesiaca [16].

Heslo vytvorené dodržiavaním vyššie uvedených smerníc bude pre sociotechnika ťažkým orieškom, pretože programy umožňujúce odhaľovanie hesiel vyhľadávajú správnu variantu predovšetkým v zoznamoch slovnej zásoby jednotlivých jazykov. Čas potrebný na nájdenie správneho hesla je rôzny a závisí od dĺžky hesla a počtu použitých znakov (Tabuľka č. 1).

Typ hesla	**Počet znakov**	**Dĺžka hesla**				
		6	**8**	**10**	**15**	**20**
0-9	**10**	0 sec	10 sec	17 min	3,17 roka	317 tis. rokov
a-z	**26**	30 sec	6 hod	163 dní	5 mil. rokov	∞
a-z, A-Z, 0-9	**62**	1½ hod	253 dní	2660 rokov	∞	∞
a-z, A-Z, 0-9, špec. znaky	**96**	22 hod	23 rokov	212 tis. rokov	∞	∞

Tabuľka č. 1 Rýchlosť odhalenie hesla

Zdroj: http://rajo.platon.sk/doc/internet-security/#section_7

3.6 VYSKAKOVACIE OKNÁ, BROŽÚRKY, PLAGÁTY, LETÁKY

Ľudia veľmi často zabúdajú, a najmä na veci, o ktorých si myslia, že sa ich netýkajú, alebo nie sú pre nich podstatné. Preto je potrebné nájsť rad spôsobov, ako im pripomenúť vedomosti, ktoré sa naučili na školení.

Za týmto účelom sa môžu používať v počítačovom systéme okná pripomínajúce rôzne zásady bezpečnosti. Mali by byť naprogramované tak, aby zmizli až po stlačení klávesy potvrdzujúcej prečítanie. Okná by sa mali zobrazovať aspoň dvakrát za deň a mali by byť vo forme jednoduchých výstižných viet, aby nezanechávali na zamestnancoch pocit strateného času a obťažovania pri ich čítaní.

Dobrou metódou je používanie krátkych poznámok vo firemnom informačnom bulletine. Nejde o celé články, ale o krátke poznámky podobné reklamám v časopisoch, ktoré hneď upútajú pozornosť čitateľa. Takto by bolo možné, v každom vydaní spravodaja predstaviť novú otázku z bezpečnostnej oblasti formou, ktorá by priťahovala pozornosť čitateľa.

Firmy, ktoré nemajú svoje informačné brožúrky, môžu použiť namiesto nich letáky alebo plagáty, na ktorých by pomocou humoru a dôvtipu s využitím kombinácie textu a obrázkov pripomínali dodržiavanie bezpečnosti a postupov, s ktorými boli zamestnanci oboznámení na školení (Príloha A).

Každá firma, by preto mala zásady bezpečnosti nielen písomne definovať, ale mala by vynaložiť aj úsilie s cieľom presvedčiť *všetky* osoby, ktoré pracujú s informáciami alebo počítačovými systémami, aby sa zásady naučili a tiež podľa nich postupovali. Treba sa ale aj uistiť, že všetci rozumejú dôvodom, prečo boli jednotlivé princípy zavedené, aby sa ich nepokúšali z pohodlnosti obchádzať. Inak bude neznalosť pre pracovníkov vždy dobrou výhovorkou a pre sociotechnika slabinou, ktorú ochotne využije.

3.7 LIKVIDÁCIA ODPADU

Veľké množstvo informácií potrebných na útok, získavajú sociálni inžinieri z už nepotrebných alebo nepodstatných dát, ktoré sú vyhadzované do smetných košov, bez ich predchádzajúceho zničenia. Firmy, by sa preto mali zamerať a používať technológie

na deštrukciu už neúčelných informácií nachádzajúcich sa, či už na papieroch, alebo disketách, harddiskoch... a mali by sa pridržiavať nasledujúcich pravidiel, ako nakladať s odpadkami:

- Zaradenie všetkých dôverných informácií do jednotlivých kategórií podľa stupňa ich dôvernosti,
- Zavedenie pokynov v celej firme , ako sa zbavovať dokumentov obsahujúcich takéto dáta,
- Vyžadovanie, aby bol každý dokument pred vyhodením zničený,
- Nepoužívanie lacných skartovačiek, ktoré režú dokumenty na prúžky. Tie by mohol odhodlaný lovec informácií pri troche šťastia podkladať dohromady. Existujú lepšie skartovačky, ktoré zmenia dokument na neužitočnú drť,
- Pred vyhodením elektronických nosičov obsahujúcich dôverné informácie, je potrebné ich celkom odmagnetizovať alebo zničiť, a to i keď dôverné dáta už boli predtým vymazané,
- Udržovanie príslušnej úrovne kontroly nad výberom upratovacieho personálu, v prípade potreby kontrolovanie ich činnosti,
- Pripomínanie zamestnancom, aby sa zamýšľali nad tým, aké materiály vyhadzujú do koša,
- Zamykanie kontajnerov s odpadkami [10, s.175].

Vydávanie brožúr o bezpečnosti informácií alebo odkázanie pracovníkov na internetovú stránku, ktorá popisuje bezpečnostnú politiku firmy samo o sebe riziko nezmenšuje. Každá firma musí zásady nielen písomne definovať, ale musí vynaložiť ďalšie úsilie s cieľom presvedčiť *všetky* osoby, ktoré majú kontakt s informáciami alebo počítačovými systémami, aby sa zásady naučili a podľa nich aj postupovali. Je potrebné sa uistiť, že všetci rozumejú dôvodom, prečo boli jednotlivé princípy zavedené, aby sa ich nepokúšali obísť. Inak bude neznalosť pre pracovníka vždy dobrou výhovorkou a pre sociotechnika slabinou, ktorú vďačne využije.

3.8 SOFTWARE

Na zabránení prieniku útočníka do počítačovej siete a získaní informácií z nej, sa nepodieľa len hardware, ale aj softwarové vybavenie počítačov, ako sú antivírusové programy a firewally.

Antivírusový program

Antivírusový program je jeden z najpoužívanejších ochranných opatrení, ktorý sa používa proti infiltrácii škodlivého kódu (napr. červy a trojské kone, phishing) do systému. Skladá sa z častí, ktoré sledujú všetky najpodstatnejšie vstupno-výstupné miesta, ktorými by prípadná infiltrácia mohla do informačného systému preniknúť. Týmito vstupno-výstupnými miestami môže byť elektronická pošta, webové stránky alebo prenosné záznamové médiá.

Nedeliteľnou a veľmi dôležitou súčasťou antivírusových programov je ich aktualizácia cez Internet, vďaka ktorej sú schopné odhaliť väčšinu známych vírusov, ktoré vznikli pred dátumom vydania vírusovej databázy [8].

Firewall

Spoločné využívanie sieťových zariadení a spracovaných informácií môže zvyšovať hrozbu vzdialeného neautorizovaného prístupu do informačného systému, preto by mali byť do siete včlenené ochranné opatrenia na segregáciu skupín informačných služieb, užívateľov a informačných systémov.

Tieto opatrenia môžu byť implementované inštalovaním bezpečnostnej brány – firewallu medzi dve siete. Firewall je sada softvérových alebo hardvérových nástrojov, ktoré majú za cieľ prepojiť dve alebo viac sietí z rôznou úrovňou dôveryhodnosti. Táto brána by mala byť konfigurovaná na filtrovanie prenosu dát a blokovanie neautorizovaného prístupu, podľa politiky riadenia prístupu [8].

Cieľom sociotechnických útokov nie sú len právnické osoby ale aj fyzické osoby - bežní užívatelia, ktorí väčšinou ani nevedia, že existujú ľudia. ktorí sú schopní od nich vylákať rôzne citlivé informácie bez toho, aby si to uvedomili, že sa stali obeťou sociálneho inžiniera.

Preto by sa aj oni mali starať o svoju bezpečnosť, aspoň správnou tvorbou prístupových hesiel, zabezpečením údajov v osobnom počítači pomocou softwaru ako sú antivírusové programy a firewally a tiež overovaním totožnosti osôb, ktoré ich žiadajú o dôverné informácie.

4 ZMAPOVANIE SÚČASNÉHO STAVU INFORMOVANOSTI O TEJTO HROZBE

Cieľom prieskumu o informovanosti a faktoroch uľahčujúcich vykonanie sociálneho inžinierstva je zistiť, či právnické osoby sú informované o tejto hrozbe a ktorými faktormi uľahčujú sociotechnikom prienik do ich firiem.

Na základe vytýčených cieľov som stanovila nasledujúce hypotézy:

H(1) Predpokladám, že väčšina právnických osôb sa s pojmom sociálne inžinierstvo alebo sociotechnika nestretla a nevedia, čo tento pojem znamená.

H(2) Predpokladám, že firmy sa nestali obeťami útokov sociálnych inžinierov.

H(3) Predpokladám, že firmy majú pobočky a nie všetci zamestnanci sa navzájom poznajú.

H(4) Predpokladám, že vo firmách nie je fluktuácia.

H(5) Predpokladám, že firmy nerobia bezpečnostné školenia zamerané na odvrátenie sociotechnických útokov.

H(6) Predpokladám, že pri odosielaní dôverných informácií elektronickou formou, sú e-maily šifrované.

H(7) Predpokladám, že zamestnanci sú poučení o správnej tvorbe hesiel a nezapisujú si ich na papieriky nachádzajúce sa v blízkosti počítača.

H(8) Predpokladám, že firmy skartujú, alebo iným vhodným spôsobom ničia dôverné informácie určené na vyhodenie.

H(9) Predpokladám, že právnické osoby majú systém klasifikácie dát.

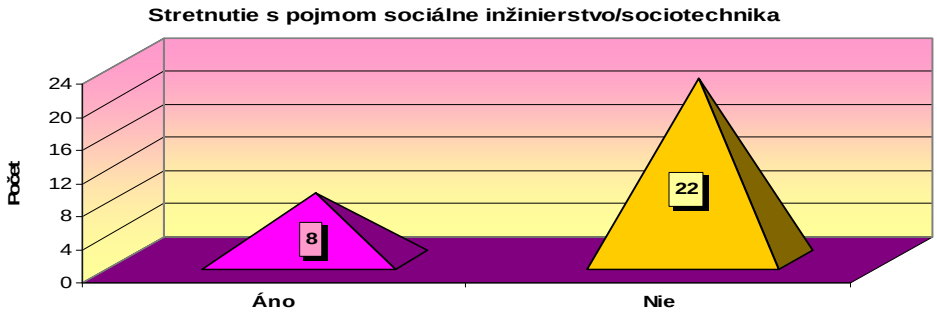
H(10) Predpokladám, že organizácie majú zabezpečený systém kontroly vstupu na ich územie.

H(11) Predpokladám, že firmy neoverujú totožnosť žiadateľa o informácie alebo vykonanie činností, či je naozaj tým, za koho sa vydáva.

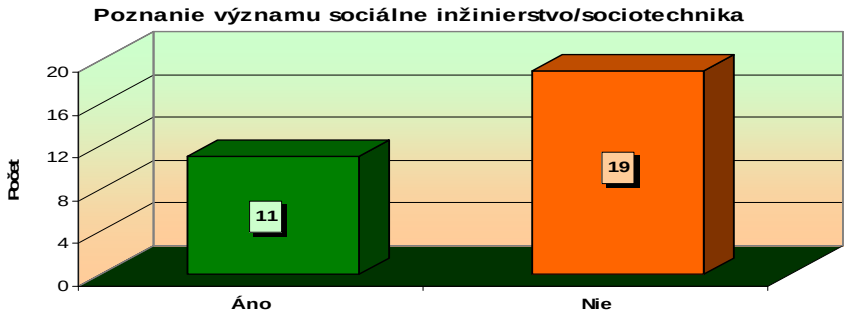
Údaje som získala formou anonymného dotazníka (Príloha B). Výskumnú vzorku tvorí 30 právnických osôb z Ružomberka. Tieto právnické osoby boli zastúpené nasledovne: 10 firiem bolo malých, ktoré majú do 10 zamestnancov, 10 firiem stredných s počtom zamestnancov od 10 do 50 a 10 veľkých firiem s kapacitou nad 50 zamestnancov. Dotazník im bol doručený v elektronickej podobe. Nachádza sa v ňom 15 otázok, ktorými som získala odpovede na jednotlivé hypotézy.

Hypotéza 1

V **H(1)** som predpokladala, že väčšina právnických osôb sa s pojmom sociálne inžinierstvo alebo sociotechnika nestretli a nevedia, čo tento pojem znamená.



Graf č.1 Stretnutie právnických osôb s pojmom sociálne inžinierstvo alebo sociotechnika



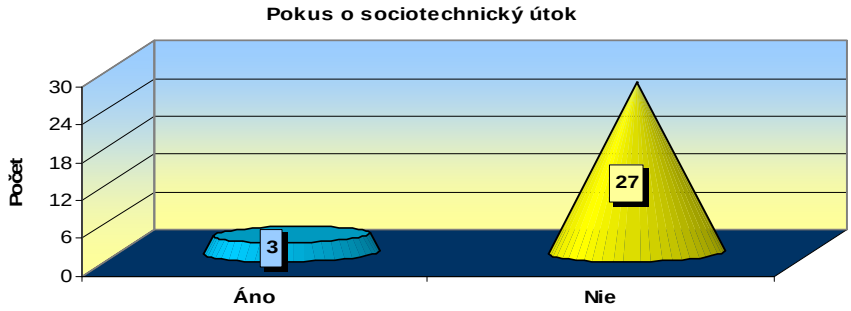
Graf č. 2 Poznanie významu slova sociálne inžinierstvo alebo sociotechnika

Analýzou údajov z grafov č. 1 a 2 som zistila, že 8 opýtaných, čo predstavuje 27% sa s pojmom sociálne inžinierstvo alebo sociotechnika ostalo do styku a len 11 respondentov, čo je 37% vedia, čo tento pojem znamená.

Predpoklad, že väčšina právnických osôb sa s pojmom sociálne inžinierstvo alebo sociotechnika nestretli a nevedia, čo tento pojem znamená bol správny.

Hypotéza 2

V **H(2)** som predpokladala, že firmy sa nestali obeťami útokov sociálnych inžinierov.



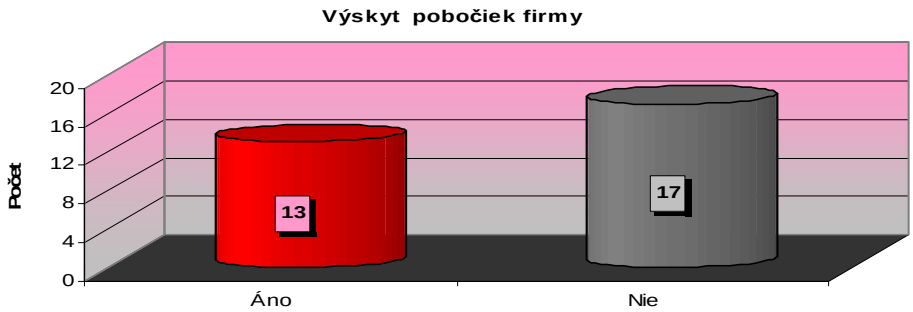
Graf č. 3 Pokus o vykonanie sociotechniky

Len v 3 firmách bol pokus o vykonanie sociotechnického útoku, čo znamená, že len 10% firiem sa priamo stretlo so sociálnym inžinierstvom. Útoky boli v dvoch prípadoch realizované prostredníctvom internetu a v treťom, pomocou internetu ale aj formou osobného stretnutia.

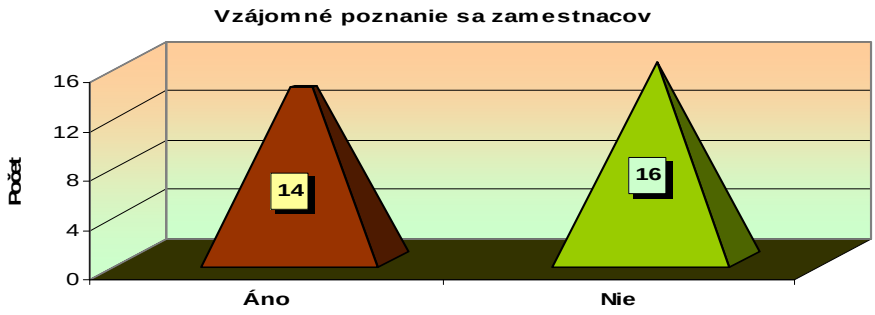
Firmy sa nestali obeťami sociálneho inžinierstva je pravdivá hypotéza. Malý počet kladných odpovedí môže byť spôsobený aj tým, že firmy si väčšinou ani neuvedomia že sa stali cieľom sociotechnických útokov.

Hypotéza 3

V **H(3)** som predpokladala, že firmy majú pobočky a nie všetci zamestnanci sa navzájom poznajú.



Graf č. 4 Výskyt pobočiek firmy



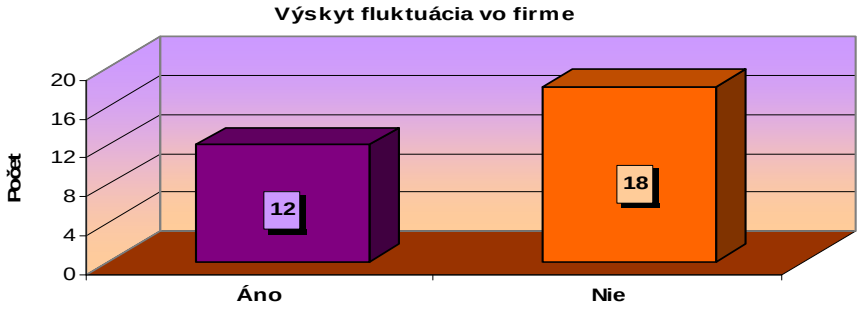
Graf č. 5 Poznanie sa všetkých zamestnancov vo firme navzájom

Firiem, ktoré majú pobočky, je len 13 z 30tich opýtaných a väčšina, predstavujúca 56% respondentov, pobočky nemá. V 14tich podnikoch sa všetci zamestnanci navzájom poznajú a v 16tich nie.

Prieskum vo väčšom percente ukázal, že prvá časť domnienky, že firmy majú pobočky je nepravdivá, ale druhá, ktorá predpokladá, že sa nepoznajú všetci zamestnanci navzájom je pravdivá.

Hypotéza 4

V **H(4)** som predpokladala, že vo firmách nie je fluktuácia.



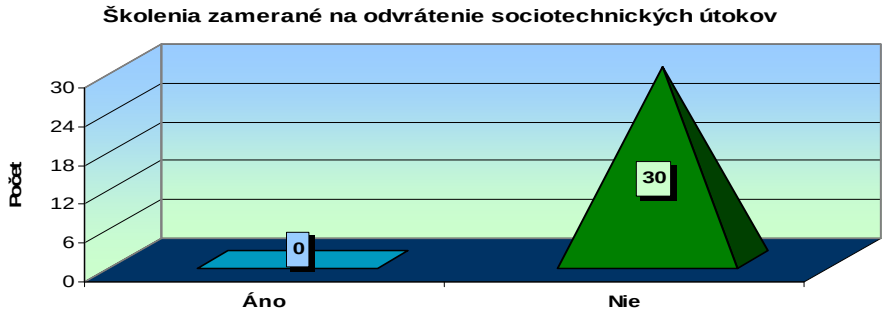
Graf č. 6 Výskyt fluktuácie vo firmách

Fluktuácia pracovných síl sa vyskytuje v 40%tách podnikoch, ktoré sa zúčastnili prieskumu a 60% firiem nepociťuje častú zmenu pracovníkov.

Hypotéza, že vo firmách sa nevyskytuje fluktuácia sa potvrdila, čo vidno aj z grafu č.6.

Hypotéza 5

V **H(5)** som predpokladala, že firmy nerobia bezpečnostné školenia zamerané na odvrátenie sociotechnických útokov.



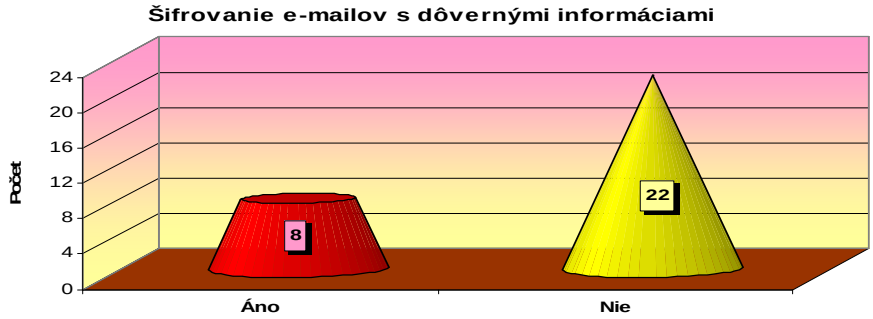
Graf č. 7 Vykonávanie bezpečnostných školení zameraných na odvrátenie sociotechniky

Graf č. 7 znázorňuje veľmi zaujímavý úkaz, že žiadna z firiem podieľajúcich sa na tvorbe tohto výskumu, neškolí svojich zamestnancov v oblasti bezpečnosti zameranej na odvrátenie a prevenciu pred sociotechnickými útokmi.

Predpoklad, že firmy nerobia bezpečnostné školenia zamerané na odvrátenie sociotechnických útokov sa úplne potvrdil.

Hypotéza 6

V **H(6)** som predpokladala, že pri odosielaní dôverných informácií elektronickou formou, e-maily sú šifrované.



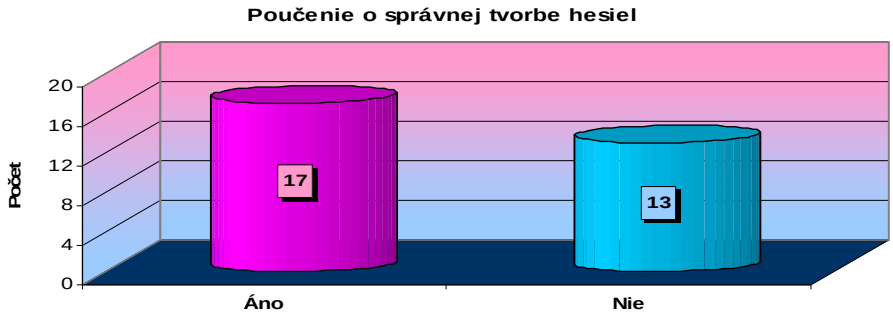
Graf č. 8 Šifrovanie e-mailov pri odosielaní dôverných informácií

Dôverné informácie odosielané formou e-mailov chráni šifrovaním len 8 firiem, čo predstavuje 27% opýtaných. Zvyšných 22 firiem nevyužíva šifrovanie e-mailov na zabránenie úniku dôležitých dát z firmy.

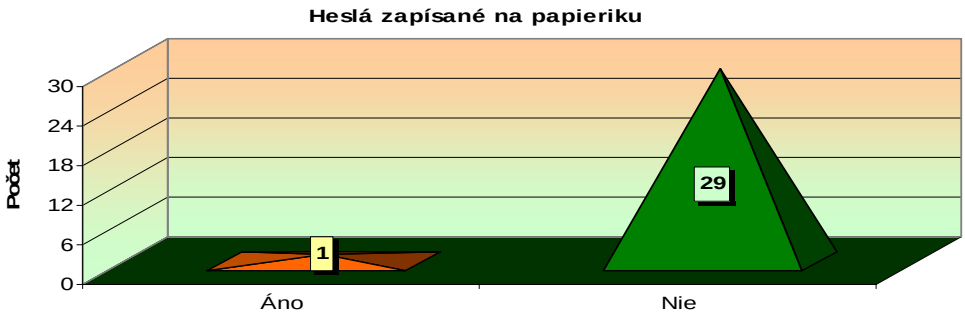
Vo väčšine firiem, sa e-maily s dôvernými informáciami nešifrujú, čo vyvrátilo očakávanie, že pri odosielaní dôverných informácií elektronickou formou, sú e-maily šifrované.

Hypotéza 7

V **H(7)** som predpokladala, že zamestnanci sú poučení o správnej tvorbe hesiel a nezapisujú si ich na papieriky, nachádzajúce sa v blízkosti počítača.



Graf č. 9 Poučenie zamestnancov o správnej tvorbe hesiel



Graf č. 10 Písanie hesiel na papieriky

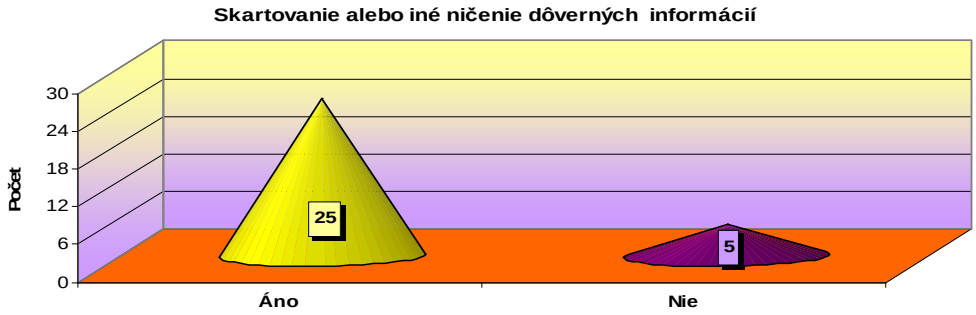
57% zamestnancov je poučených o správnej tvorbe hesiel a len 3% si zapisujú heslá na papieriky, aby si ich nemuseli pamätať.

Takmer nikto si heslá nezapisuje na papieriky a väčšina respondentov je poučená o správnej tvorbe hesiel, čo sa stotožňuje s predpokladom, že zamestnanci sú poučení o

správnej tvorbe hesiel a nezapisujú si ich na papieriky, nachádzajúce sa v blízkosti počítača.

Hypotéza 8

V **H(8)** som predpokladala, že firmy skartujú, alebo iným vhodným spôsobom ničia dôverné informácie určené na vyhodenie.



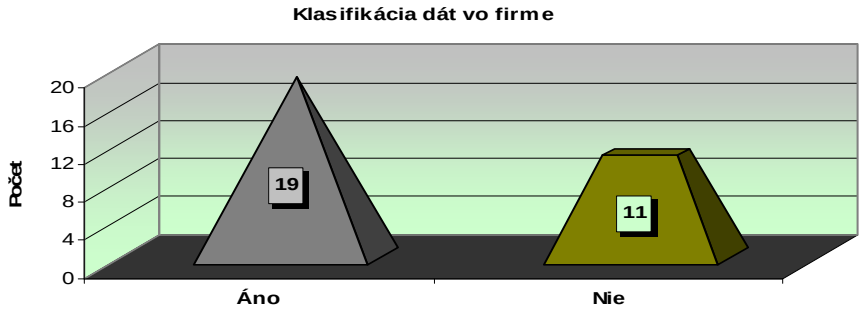
Graf č. 11 Ničenie dôverných dát určených na vyhodenie skartovaním alebo inak

Až 25 z 30tich firiem skartuje alebo iným vhodným spôsobom ničí dáta určené na vyhodenie pred ich odstránením z firmy. 7% firiem sa nezaoberá otázkou znehodnocovania údajov pred ich vyhodením.

Predpoklad, že firmy skartujú, ale iným vhodným spôsobom ničia dôverné informácie určené na vyhodenie sa potvrdil.

Hypotéza 9

V **H(9)** som predpokladala, že právnické osoby majú systém klasifikácie dát.



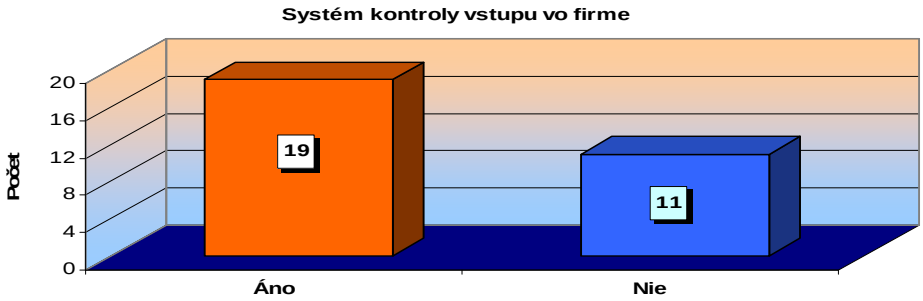
Graf č. 12 Systém klasifikácie dát v podnikoch

Podniky, ktoré sa stali súčasťou prieskumu majú v 19tich prípadoch zavedenú klasifikáciu dát, čo predstavuje väčšinu tvoriacu 63%. A len 37% z nich ju nevyužíva.

Hypotéza tvrdiaca, že právnické osoby majú systém klasifikácie dát, je správna.

Hypotéza 10

V **H(10)** som predpokladala, že organizácie majú zabezpečený systém kontroly vstupu na ich územie.



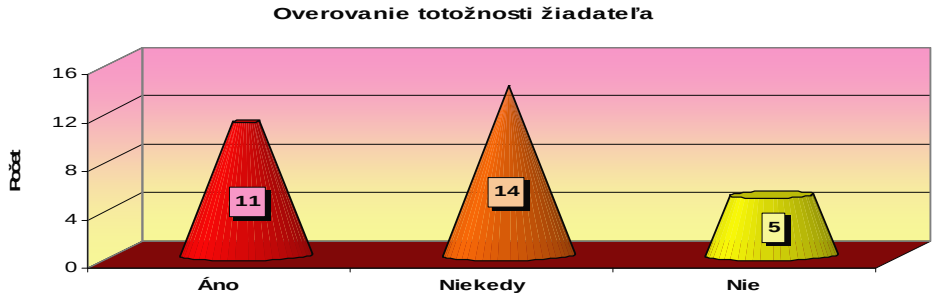
Graf č. 13 Existencia systému kontroly vstupov do firiem

Firmy, sa o svoju bezpečnosť v 19tich prípadoch postarali systémom kontroly vstupu na ich územie a 11 firiem, tvoriacich 37% respondentov ho nemá.

Systém kontroly vstupov do firiem má zavedený väčšina firiem, čo potvrdzuje predpoklad, že organizácie majú zabezpečený systém kontroly vstupu na ich územie.

Hypotéza 11

V **H(11)** som predpokladala, že firmy neoverujú totožnosť žiadateľa o informácie alebo vykonanie činností, či je naozaj tým, za koho sa vydáva.



Graf č. 14 Overovanie totožnosti žiadateľa o dáta alebo činnosti

Najväčšiu skupinu, obsahujúcu 14 respondentov, tvoria firmy, ktoré len niekedy overujú totožnosť žiadateľa, ďalšou sú firmy (11),ktoré ju overujú a 6 firiem ju neoveruje vôbec. V percentuálnom vyjadrení 47% firiem preveruje identitu žiadateľa len niekedy, 37% ju preveruje vždy a 16% ju neoveruje vôbec.

Hypotéza, že firmy neoverujú totožnosť žiadateľa o informácie alebo vykonanie činností, či je naozaj tým, za koho sa vydáva sa nepotvrdila.

Po zhrnutí zmapovania stavu informovanosti právnických osôb o tejto hrozbe a faktoroch uľahčujúcich útok sociotechnikov, som dospela k záveru, že firmy sú málo informované o tejto súčasnej hrozbe informačných systémov, pričom sa väčšina z nich ani nestretla s pojmom sociálne inžinierstvo alebo sociotechnika a ani nevedia, čo tento pojem znamená. Predpokladám, že inak to nie je ani u fyzických osôb.

Právnické osoby by sa mali začať viac zaujímať o pôsobenie sociotechnikov, ktorí im môžu zapríčiniť nemalé problémy a škody, či už finančné, alebo odcudzenie tajných informácií ako sú obchodné tajomstvo, technické špecifikácie či databáza obsahujúca osobné údaje o zamestnancoch.

Kľúčovým krokom k poznaniu nepriateľa je predovšetkým porozumieť jeho zbraniam. Preto je dôležité byť oboznamovaný o aktuálnych útokoch, či už prostredníctvom masmédií, ako sú noviny, časopisy a televízia, ale aj internet a vedieť sa proti nim brániť. Oboznamovaním širokej verejnosti o informačnej bezpečnosti, sa zaoberá projekt KRY SA! zastrešený Ministerstvom dopravy pôšt a telekomunikácií, ktorý publikuje články v novinách, na internete, ale aj rozhovory vysielané v rádiách, zaoberajúce sa internetovou bezpečnosťou a ochranou osobných údajov.

Sociotechnici sú takí šikovní a prešpekulovaní, že po svojom útoku nezanechávajú takmer žiadne stopy, za pomoci ktorých by mohli byť ich ataky odhalené, pokiaľ sa nejedná o finančné straty, a aj preto je ťažké odhaliť, či sa niekto stal ich obeťou alebo nie. O tom svedčí aj malý počet firiem, ktoré zaznamenali, že sa stali korisťou podvodníkov.

K predchádzaniu sociálneho inžinierstva je potrebné poznať faktory, ktoré umožňujú útočníkom infiltrovanie sa do firmy a prienik k potrebným informáciám, a ich následné využitie na uskutočnenie vytýčeného cieľa.

Faktory, ako je veľký počet zamestnancov pracujúcich na pobočkách firmy, ktorí sa navzájom nepoznajú a fluktuácia pracovníkov sú takmer neodstrániteľné vo veľkých podnikoch, a najmä preto, sa práve oni stávajú najčastejšími obeťami sociotechnikov, ktorí predstierajú totožnosť spolupracovníka.

Na uľahčení prieniku do podnikov sa vo veľkej miere podieľa aj chýbajúci systém kontroly a riadenia vstupov na ich územie a klasifikácie dát. Keby mala každá firma zabezpečenú kontrolu identifikácie a prípadnej verifikácie osôb vstupujúcich na jej územie, predišla by niektorým útokom. Zamestnanci by sa mali pri vstupe do objektu identifikovať čipovými kartami a následne autentizovať heslom, ktoré by mal každý zamestnanec iné, alebo biometrickým nasnímaním odtlačku palca, alebo inej časti tela, čo by bolo veľmi ťažko oklamateľné. Systém klasifikácie dát rozdeľuje údaje do jednotlivých kategórií a zároveň determinuje, kto má prístup manipulovať s danou skupinou informácií, čím je obmedzený prístup k daným dátam a zároveň sú aj utajované pred verejnosťou.

Veľmi dôležitou súčasťou prevencie sociotechnických útokov sú bezpečnostné školenia zamerané proti nim a odhaľujúce metódy používané sociálnymi inžiniermi. Z prieskumu vyplýva, že podniky takéto školenia nerobia, čím ohrozujú sami seba. Každá jedna firma môže byť potenciálnou obeťou sociotechnika a práve preto, by mali klásť veľký dôraz na vykonávanie bezpečnostných školení, ich pravidelné opakovanie a penetračné testy overujúce osvojenie informácií, ktoré zamestnanci získali na školeniach, a ako ich uplatňujú v praxi. Na školeniach by mali byť preberané aj postupy, ako správne postupovať pri overovaní totožnosti žiadateľa o poskytnutie informácií, alebo vykonanie nejakej činnosti, či je naozaj tým, za koho sa vydáva.

Medzi ďalšie činitele napomáhajúce útočníkom uskutočniť svoj cieľ patrí aj nesprávna tvorba hesiel a ich zapisovanie na papieriky nachádzajúce sa v blízkosti počítača. Nesprávne vytvorené heslo skladajúce sa z malého počtu znakov, v ktorom nie sú využité kombinácie malý a veľkých písmen, čísiel a špeciálnych znakov, je pre útočníka ľahko odhaliteľné pomocou špeciálnych programov. Sociálny inžinier môže heslo získať pozeraním ponad niečie plece, keď sa ním autentizuje ale aj z papierikov nachádzajúcich sa pri počítači.

Pri využívaní elektronickej komunikácie na odosielanie a prijímanie e-mailov s dôvernými informáciami, treba dbať na ich bezpečnosť, aby sa nedostali do rúk

hackerov a zároveň ich aj šifrovať, aby neboli odhalené informácie, ktoré sa v nachádzajú. Podniky, ktoré sa stali súčasťou prieskumu túto skutočnosť väčšinou ignorujú a svoje e-maily odosielajú nezašifrované.

Najjednoduchším spôsobom ako získať potrebné informácie, je priamo o ne požiadať, alebo ich nájsť medzi odpadkami. Firmy, si nie vždy uvedomujú, aké už pre nich nepodstatné informácie vyhadzujú, bez ich predchádzajúceho znehodnotenia. Vyhodené dáta sú pre sociotechnika tým, čím je chleba pre ľudí.

Bez poznania pojmu sociálne inžinierstvo alebo sociotechnika, metód, ktoré využívajú sociotechnici a faktorov uľahčujúcich útoky, by nemohli byť úspešne vykonávané preventívne opatrenia proti tejto súčasnej hrozbe informačných systémov.

ZÁVER

Sociotechnika je vo väčšine prípadov ten najlacnejší, a pre znalého človeka i najjednoduchší spôsob, ako narušiť bezpečnosť aj veľmi robustných systémov. Všeobecne sa o sociálnom inžinierstve dá povedať, že útoky majú veľmi vysoké percento úspešnosti a sú veľmi zákerné, pretože pri dobrom „skrývaní“ útočníka takmer nie je možné vystopovať ho. A dopad je niekedy drvivý.

Sociotechnici využívajú na zmanipulovanie obete a získanie jej dôvery rôzne metódy ktoré na nás striehnu z každej strany, či je to obyčajný dotazník cez telefón, fax, list alebo nespočetné množstvo nástrah cez internet, z ktorých najhoršie sú phishing a pharming alebo dokonca osobné stretnutie s útočníkom.

Pozor by si mali dávať najmä veľké firmy, ktoré sú najčastejšie napádané útokmi sociotechnikov, vzhľadom na ich veľký počet zamestnancov, ktorí sa navzájom nepoznajú. Mali by zväčšovať povedomie zamestnancov o tejto veľkej, takmer nepoznanej hrozbe prostredníctvom školení so zámerom informovať zamestnancov o hodnote informácií, existencii a následnej prevencii takejto formy záškodníctva, ktoré môžu ich podniku seriózne ublížiť. Tieto opatrenia by mali prispieť k zníženiu sociotechnických útokov a k zvýšeniu bezpečnosti firiem.

Vyhodnotením dotazníka určeného pre právnické osoby, bola potvrdená domnienka, že firmy nevedia, čo znamená pojem sociálne inžinierstvo alebo sociotechnika a ani sa s týmto pojmom nestretli. Ďalším poznaním bolo, že nerobia dostatočné preventívne opatrenia proti tejto hrozbe, ktoré sú podmienené faktormi uľahčujúcimi útok narušiteľa. Medzi takéto faktory patrí fluktuácia zamestnancov, chýbajúce školenia z oblasti bezpečnosti, chýbajúci systém klasifikácie dát a kontroly a riadenia vstupov, neoverovanie totožnosti osoby, ktorá žiada o informácie alebo činnosti, nevhodná likvidácia odpadu, nešifrovanie e-mailov obsahujúcich dôležité údaje, nesprávna tvorba prístupových hesiel a nepoužívanie vhodného softwaru na zabránenie prieniku narušiteľa z vonkajšieho prostredia do počítačových systémov, ako sú firewally a antivírusové programy.

V dobe, keď je nereálne fungovanie podnikov bez počítačov a existencia bez týchto strojov, uľahčujúcich každodennú prácu a komunikáciu, ktoré sa stali súčasťou bežného života je nepredstaviteľná, sa pole pôsobenia a atakov sociálnych inžinierov neustále

zväčšujú. Táto tendencia bude rásť dovtedy, pokiaľ nebudú vhodným spôsobom odstránené všetky príčiny umožňujúce vykonávanie týchto útokov, ako sú napríklad bezpečnostné diery a ľudská naivita.

ZOZNAM POUŽITEJ LITERATÚRY

1. *Ako sa brániť on-line krádežiam identity*. In: *PCrevue* [on line]. [cit. 2008-03-01]. Dostupné na: http://www.pcrevue.sk/buxus_dev/generate_page.php?page_id=46887.

2. BANNAN, K. J. 2001. Internet World, Jan 1.

3. Bezpečnostná politika. [on line]. [cit. 2008-05-25]. Dostupné na: http://fsi.uniza.sk/kbm/sluzby/politika.htm.

4. Fake Mailer [on line]. [cit. 2007-03-13]. Dostupné na: http://www.mozektevidi.euweb.cz/fakemail.php.

5. GRAGG, D. 2002. A Multi-Level Defense Against Social Engineering. [on line]. [cit. 2007-21-03]. Dostupné na: http://www.sans.org/reading_room/whitepapers/engineering/920.php.

6. HOST, Ľ. 2006. Bezpečnosť na internete. [on line]. [cit. 2007-12-01]. Dostupné na: http://rajo.platon.sk/doc/internet-security/#section_7.

7. JAROŠ, M. Bezpečnostná politika ochrany osobných dát v malej firme. [on line]. Brno, 2007. [cit. 2008-03-01]. Dostupné na: http://is.muni.cz/th/139546/fi_b/Bakalarka.pdf.

8. LOVEČEK, T. Elektrotechnické bezpečnostné prostriedky. 2007 – učebný materiál vo forme prezentácie.

9. LOVEČEK, T. Informačné systémy a škodlivé kódy od A po Z Ikaros. [on line]. č. 4 2007, roč. 11, [cit. 2007-03-13]. Dostupné na: http://www.ikaros.cz/node/4048.

10. Mitnick, K. - Simon, W. 2003. Umění klamu. Gliwice: HELION S.A., 2003.

11. MRÁZ, P. 2006. Riziká informačných technológií – vírusy (pojmy, typy vírusov, detekovanie, prevencia); kriminalita. [on line]. [cit. 2007-04-01]. Dostupné na: http://etki.php5.sk/MOInformatika/MO23IS.php?c=m

12. Nadiktujte mi prosím pozíciu F4 z vašej karty. In: Trend [on line]. [cit. 2007-12-05]. Dostupné na: http://www.etrend.sk/firmy-a-trhy/financny-sektor/nadiktujte-mi-prosim-poziciu-f4-z-vasej-karty/120719.html.

13. Rak, R. – Kummer, R. 2007. Informační hrozby v letech 2007-2017. In: Magazín Security, 2007, č. 1, s. 2 – 5.

14. SHMIDT, I. 2007 Penetračné testy. In. Infoware [on line]. [cit. 2008-03-01]. Dostupné na: http://www.itnews.sk/buxus_dev/generate_page.php?page_id=2607.

15. Social engineering. [on line]. [cit. 2007-3-26]. Dostupné na: http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci531120,00.html.

16. USA a Južná Kórea s najvyšším počtom phishingových útokov. [on line]. [cit. 2008-21-03]. Dostupné na: http://www.kry-sa.sk/index.php?yggid=8&ate_id=80.

17. WINKLER, S. I. Case study of industrial espionage through socioal engineering. [on line]. [cit. 2007-03-12]. Dostupné na: http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper040/WINKLER.PDF.

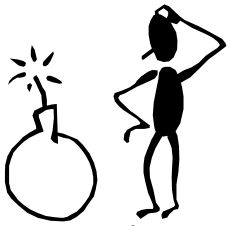
ZOZNAM PRÍLOH

PRÍLOHA A:
Návrh plagátu

Dodržiavaním bezpečnostnej politiky firmy chrániš aj svoje osobné údaje!

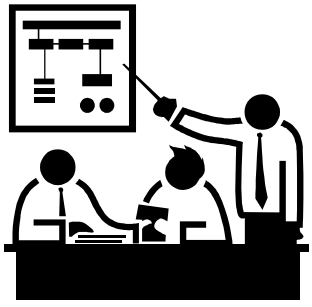
Je volajúci naozaj tým, za koho sa vydáva?

Znehodnocuješ dôverné dáta pred ich vyhodením?



Zapisuješ si heslá na papieriky?

Šifruješ dôverné informácie pred ich odoslaním e-mailom?



Dodržiavaš bezpečnostné postupy zo školení?

PRÍLOHA B: Dotazník

DOTAZNÍK - Sociálne inžinierstvo

Dostáva sa Vám do rúk dotazník, ktorý bude slúžiť k vypracovaniu bakalárskej práce na tému „Sociálne inžinierstvo ako súčasná hrozba informačných systémov“. Dotazník je anonymný a bude slúžiť len pre účely práce.
Prosím Vás, aby ste si otázky dôkladne prečítali a označili tú odpoveď, ktorá Vám najviac vyhovuje
(a) vymazaním nevyhovujúcej odpovede, b)vyfarbením vyhovujúcej odpovede c) podčiarknutím vyhovujúcej odpovede)

Ďakujem za porozumenie a ochotu spolupracovať

Barbora Balcová,
Žilinská univerzita
Fakulta špeciálneho inžinierstva

1. Stretli ste sa už s pojmom sociálne inžinierstvo alebo sociotechnika?
□ áno □ nie

2. Viete čo tento pojem znamená?
□ áno □ nie *(viď koniec dotazníka)

3. Bol vo vašej firme pokus o vykonanie sociotechniky? Ak áno, tak prostredníctvom čoho?
□ áno □ nie
□ internetu
□ telefónu
□ faxu
□ poštou
□ prehľadávaním odpadkov
□ osobným stretnutím
□ iná možnosť .....

4. Má Vaša firma pobočky?
□ áno □ nie

5. Poznajú sa navzájom všetci zamestnanci Vašej firmy?
□ áno □ nie

6. Je vaša firma?
□ malá (do10 zamestnancov)
□ stredná (od 10 do 50 zamestnancov)
□ veľká (nad 50 zamestnancov)

7. Je vo Vašej firme fluktuácia?
□ áno □ nie

8. Robí Vaša firma školenia z oblasti bezpečnosti, zamerané na odvrátenie sociotechnických útokov?
□ áno Ako často? ..... □ nie

9. Šifrujete e-maily s dôvernými informáciami?
□ áno □ nie

10. Máte na papieriku zapísané prístupové heslo do Vášho počítača?
□ áno □ nie

11. Sú vaši zamestnanci poučení o správnej tvorbe hesiel?
□ áno □ nie

12. Skartujete alebo iným spôsobom ničíte dôverné informácie, ktoré sú určené na vyhodenie?
□ áno □ nie

13. Má Vaša firma systém klasifikácie dát?
□ áno □ nie

14. Má Vaša firma zabezpečený systém kontroly vstupu osôb na jej územie?
□ áno □ nie

15. Overujete totožnosť žiadateľa o informácie, či je naozaj tým za koho sa vydáva?
□ áno □ nie □ niekedy

* *Sociálne inžinierstvo*, tiež nazývané *sociotechnika* je ovplyvňovanie a presviedčanie ľudí s cieľom oklamať ich tak, aby uverili, že sociotechnik je osoba s totožnosťou, ktorú predstiera a ktorú si vytvoril pre potreby manipulácie. Sociálny inžinier je schopný využiť ľudí, s ktorými hovorí, prípadne dodatočné technologické prostriedky (napr.: telefón, internet, prehľadávanie odpadkov, pošta, ...), aby získal hľadané informácie (napr.: prístupové heslá, PINy, osobné údaje, ...) a využil ich vo svoj prospech..