EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFORMATIKY

Evidenčné číslo: 17300/I/2011/0475746395

ANALÝZA METÓD SOCIÁLNEHO INŽINIERSTVA A MOŽNOSTI ZABEZPEČENIA IT

Diplomová práca

2011 **Bc. Roman URMANIČ**

EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFORMATIKY

ANALÝZA METÓD SOCIÁLNEHO INŽINIERSTVA A MOŽNOSTI ZABEZPEČENIA IT

Diplomová práca

Študijný program: Hospodárska informatika

Študijný odbor: 9.2.10 Hospodárska informatika

Školiace pracovisko: Katedra aplikovanej informatiky

Školiteľ: Ing. Magdaléna Cárachová, PhD.

Bratislava 2011 **Bc. Roman URMANIČ**

Ekonomická univerzita v Bratislave
Fakulta hospodárskej informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Bc. Roman Urmanič
Študijný program: Hospodárska informatika (Jednoodborové štúdium, inžiniersky II. st., externá forma)
Študijný odbor: 9.2.10 Hospodárska informatika
Typ záverečnej práce: Inžinierska záverečná práca
Jazyk záverečnej práce: slovenský

Názov: Analýza metód sociálneho inžinierstva a možností zabezpečenia IT

Anotácia: Práca sa zaoberá analýzou metód sociálneho inžinierstva a ich dopadov na chod firmy a používateľov IT. Práca vychádza z teoretických poznatkov a praktických vedomostí. Popisuje súčasný stav a používané metódy útokov v oblasti sociálneho inžinierstva. Súčasťou sú tiež návrhy možných bezpečnostných riešení ako sa efektívne brániť pred týmito hrozbami pomocou rôznych prostriedkov.

Vedúci: Ing. Magdaléna Cárachová, PhD.
Katedra: KAI FHI – Katedra aplikovanej informatiky FHI
Vedúci katedry: doc. Ing. Gabriela Kristová, CSs.

Dátum zadania: 01.12.2009

Dátum schválenia: 20.12.2009

doc. Ing. Gabriela Kristová, CSs.
vedúci katedry

Čestné vyhlásenie

Čestne vyhlasujem, že záverečnú prácu som vypracoval samostatne a že som uviedol všetku použitú literatúru.

Dátum: 23. apríla 2011 **.....**

(podpis študenta)

Poďakovanie

Touto cestou sa chcem poďakovať vedúcej diplomovej práce Ing. Magdaléne Cárachovej, PhD. za cenné pripomienky a odborné rady, ochotu a pomoc, ktorými prispela k vypracovaniu predkladanej diplomovej práce.

ABSTRAKT

URMANIČ, Roman: *Analýza metód sociálneho inžinierstva a možnosti zabezpečenia IT.* – Ekonomická univerzita v Bratislave. Fakulta hospodárskej informatiky; Katedra aplikovanej informatiky. – Vedúci záverečnej práce: Ing. Magdaléna Cárachová, PhD. – Bratislava: FHI EU, 2011, 69s.

Cieľom záverečnej práce bolo analyzovať metódy sociálneho inžinierstva a útoky s ním spojené, opísať priebeh konkrétnych útokov a odporučiť adekvátne možnosti ochrany. Práca je rozdelená do štyroch kapitol. Obsahuje jeden graf, dve tabuľky a šesť obrázkov.
Prvá kapitola objasňuje teoretické pojmy a vystihuje súčasný stav v oblasti sociálneho inžinierstva, popisy jeho metód a koncepciu fungovania sociálneho inžinierstva. V druhej kapitole je popísaný cieľ diplomovej práce, metodika práce a metódy skúmania. Záverečná kapitola sa zameriava na metódy sociálneho inžinierstva v súvislosti s ich výskytom v praxi a návrhov možností ako sa voči útokom sociálneho inžinierstva chrániť. Nami navrhnuté riešenia ochrany a prevencie by mohli v budúcnosti predstavovať celkový prínos v oblasti bezpečnosti.

Kľúčové slová: Sociálne inžinierstvo, sociálny inžinier, hacker, sociotechnický cyklus, phishing, pharming, trashing

ABSTRACT

URMANIČ, Roman: *Analysis of social engeneering methods and possibilities of IT security.* – University of Economics in Bratislava. Faculty of Informatics; Department of Applied Informatics – Professional guidance: Ing. Magdaléna Cárachová, PhD. – Bratislava: FHI EU, 2011, 69p.

The aim of the thesis was to analyze the methods of social engineering and attacks associated with it, to describe the course of specific attacks and recommend adequate protection options. The thesis is divided into four chapters. It contains one graph, two tables and six pictures.

The first chapter explains the theoretical concepts and describes the current state of social engineering, descriptions of its methods and concept of operation of the social engineering. The second chapter describes the objective of the thesis, methodology and work methods of examination. The final chapter focuses on methods of social engineering in the context of their occurrence in practice and suggestions how to prevent social engineering attacks. Our proposed solutions for protection and prevention could be a great contribution to safety in the future.

Key words: social engineering, social engineer, hacker, sociotechnical cycle, phishing, pharming, trashing

OBSAH

ÚVOD

Žijeme v dobe, ktorú môžeme nazvať informačným vekom. Úspešným sa stáva ten kto dokonale ovláda schopnosti ako získať, hľadať a správne použiť informácie. Treba si však uvedomiť, že tieto informácie majú svoju hodnotu. Z toho vyplýva, že tieto cenné informácie si musíme zodpovedajúcim spôsobom chrániť.

Existuje mnoho spôsobov ako sa dostať k cudzím informáciám. Niektoré spôsoby sú veľmi sofistikované, iné používajú principiálne jednoduché metódy. Premyslenou a dobre vedenou manipuláciou človeka dokážeme od obetí získať množstvo dôležitých informácií bez toho, aby si obeť vôbec uvedomila, že sa stala predmetom útoku sociálneho inžiniera.

Sociálne inžinierstvo môžeme charakterizovať ako ovplyvňovanie a presvedčovanie ľudí s cieľom oklamať ich tak, aby uverili, že sociálny inžinier je osoba s totožnosťou, ktorú predstiera a ktorú si vytvoril pre potreby manipulácie. Vďaka tomu je sociálny inžinier schopný využívať ľudí a dodatočné technologické prostriedky, s ktorými cielene manipuluje, aby získal potrebné informácie.

Problematika sociálneho inžinierstva je opísaná v troch kapitolách diplomovej práce, ktorej predmetom je „analýza metód sociálneho inžinierstva a možnosti zabezpečenia IT“.

Prvá kapitola je venovaná konkrétnym definíciám základných pojmov bezpečnosti informačných systémov a sociálneho inžinierstva.

V druhej kapitole je opísaný cieľ diplomovej práce, ktorý poukazuje na dôkladnú analýzu metód sociálneho inžinierstva a ich dopadov na chod firmy a používateľov. V tejto kapitole sa venujeme aj opisu metodiky práce a metódam skúmania.

Tretia kapitola je zameraná na konkrétne prípady útokov pomocou sociálneho inžinierstva v praxi. Praktický opis práce sociálneho inžiniera nám umožní pochopiť

jednotlivé kroky útoku. Na konkrétnych modelových situáciách môžeme ilustrovať priebeh realizovaného útoku a taktiež sledovať správanie sa útočníka a obete. Súčasťou tejto kapitoly sú návrhy možností ochrany pred útokmi sociálneho inžinierstva jednak pomocou ľudského faktora a taktiež pomocou hardvérových a softvérových prostriedkov.

1 SÚČASNÝ STAV RIEŠENEJ PROBLEMATIKY DOMA A V ZAHRANIČÍ

1.1 Bezpečnosť informačných a komunikačných technológií

Oblasť počítačovej bezpečnosti predstavuje vedu o počítačoch, ktorá sa zaoberá odhaľovaním a eliminovaním rizík spojených s používaním informačných a komunikačných technológií.

Cieľom počítačovej bezpečnosti je zabezpečiť:[1]

- ochranu pred neoprávneným manipulovaním so zariadeniami počítačového systému,
- ochranu pred neoprávnenou manipuláciou s dátami,
- ochranu pred nelegálnou tvorbou kópií dát,
- bezpečnú komunikáciu a prenos dát,
- bezpečné uloženie dát,
- integritu a nepodvrhnuteľnosť dát.

Koncepcia počítačovej bezpečnosti spočíva v troch krokoch:

- prevencia - ochrana pred hrozbami,
- detekcia - odhalenie neoprávnenej činnosti a slabého miesta v systéme,
- náprava - odstránenie slabého miesta v systéme.

V súčasnej dobe prudkého rozmachu informačných a komunikačných technológií sa s otázkou ich bezpečnosti stretávame čoraz častejšie. Tvorba škodlivého softvéru môže mať rôzne pozadie. Niekedy ide len o snahu autora dokazovať a demonštrovať svoje schopnosti. Veľká väčšina tvorby a distribúcie škodlivého kódu má však ekonomické pozadie. Je všeobecne známe, že táto oblasť počítačovej kriminality predstavuje

[1] *Počítačová bezpečnosť*. [online]. 2011. [spracované 2011-03-22]. Dostupné na internete: <http://sk.wikipedia.org/wiki/Počítačová_bezpečnosť>

ekonomicky veľmi výnosnú oblasť. Finančná výnosnosť predmetnej oblasti sa dokonca približuje výnosom z ilegálnej drogovej činnosti. V súčasnosti je oblasť počítačovej kriminality veľmi dobre organizovaná. Už dávno nehovoríme o izolovaných indivíduách, ale o vysoko organizovaných skupinách, ktoré sú veľmi dobre finančne a technicky zabezpečené. Počítačová kriminalita sa čoraz viac zameriava na konkrétne ciele a obete. Útočníci sa snažia o svojich potenciálnych obetiach zozbierať maximálne množstvo informácií, napomáha tomu aj mohutný rozmach a obľúbenosť sociálnych sietí.

Informácie spracovávané pomocou informačných a komunikačných technológií majú často tú najvyššiu cenu. Malo by byť pre nás samozrejmé chrániť ich tak ako náš celý majetok. Z uvedených dôvodov je zrejmé, že otázke počítačovej bezpečnosti a z nej potenciálne plynúcich dopadov kriminálnych činností musíme venovať veľkú pozornosť.

Aj keď sa útočníkovi nepodarí získať informácie, ktoré sa snažil odcudziť, neznamená to, že spoločnosti nespôsobí žiadne finančné straty. Útoky často sprevádza veľa nepríjemností, ktoré majú negatívny vplyv na prevádzku jednotlivých oddelení, čo v konečnom dôsledku stojí spoločnosť nemalé finančné prostriedky. Spoločnosť Alinean vo svojej štúdii špecifikovala odhad strát spoločností pôsobiacich v rôznych priemyselných odvetviach pri prerušení ich činnosti na 1 minútu.[2]

Tabuľka 1-1: Straty spojené s výpadkom prevádzky

Odvetvie	**Odhadované straty spôsobené minútovým výpadkom**
dodávateľské služby	$11 000,00
elektronický obchod	$10 000,00
zákaznícke služby	$3 700,00
elektronické platobné systémy	$3 500,00
správa financií	$1 500,00
správa ľudských zdrojov	$1 000,00
Komunikácia	$1 000,00
Infraštruktúra	$700,00

Zdroj: Dostupné na internete: <http://archive.itmanagementnews.com/2004/0311.html>, citované dňa 27.4.2011

[2] HARRIS, S. a kol. 2008. *Hacking - manuál hackera*. 1. vyd. Praha : Grada publishing, 2008, s. 27

1.1.1 Bezpečnosť firiem a domácich používateľov

Problém v zabezpečení sa netýka len domácich používateľov. Štúdia spoločnosti Trend Micro odhalila, že 100 % všetkých zúčastnených firiem „ukrýva“ vo svojej sieti aktívny malware. Prečo je to tak? Ako je možné, že sa tento nežiaduci kód tak úspešne šíri? Problém tkvie v podstate zabezpečenia. Zabezpečenie, a to nielen na úrovni IKT (informačné a komunikačné technológie), predstavuje nikdy nekončiaci proces, ktorý zahŕňa i tú najproblematickejšiu premennú zo všetkých možných - *človeka*.

Každý podnik potrebuje formálne definovanie realizovaných procesov, ktoré by sa v tomto prípade malo premietnuť do bezpečnostnej politiky organizácie. Jej absencia alebo jej nedôsledné dodržiavanie vedie potom k úspešným útokom proti informačnému systému. Zostavenie bezpečnostnej politiky organizácie nie je jednoduché a jej tvorbu je vhodné konzultovať so špecialistami, ktorí majú v tejto oblasti bohaté skúsenosti a poznajú medzinárodné štandardy a normy. Ich integrácia tiež prispieva k skvalitneniu procesu riadenia kvality, a tým aj k príslušnej certifikácii podľa normy ISO.

Samozrejmú súčasť zabezpečenia podnikovej siete by malo tvoriť už všeobecne známe trio – pravidelné a bezodkladné aplikovanie opráv operačného systému a nainštalovaného programového vybavenia, pravidelne aktualizovaný antivírusový systém a aktívny firewall. Ideálne sú také riešenia, ktoré umožňujú centralizovanú konfiguráciu a správu v podnikovom prostredí, integráciu s inými bezpečnostnými prvkami siete a tvorbu reportov a prehľadov ich aktivít.[3]

1.1.2 Definovanie a správa oprávnení

Ďalší nevyhnutný element zabezpečenia je definovanie potrebných oprávnení každého používateľa vzhľadom na informačný systém organizácie a následné pridelenie týchto oprávnení používateľovi. Žiaľ, veľmi často sa možno stretnúť s prípadmi, keď používatelia bez ohľadu na svoju pracovnú pozíciu pracujú s právami lokálneho

[3] ULÍK, B. *Bezpečnosť ako nikdy sa nekončiaci proces.* [online]. 2009. [spracované 2011-03-29]. Dostupné na internete: < http://www.itnews.sk/tituly/infoware/2009-10-22/c129785-bezpecnost-ako-nikdy-sa-nekonciaci-proces>

administrátora, či dokonca s administrátorskými právami i v rámci siete. Platí takisto, že každý používateľ by mal mať pridelený svoj používateľský účet na prístup do informačného systému a v žiadnom prípade by nemalo dôjsť k zdieľaniu tohto účtu medzi viacerými používateľmi, pretože v opačnom prípade nemožno efektívne vykonávať audit prístupu k zdrojom informačného systému organizácie.

1.1.3 Autentizácia

Z hľadiska bezpečnosti sa vyžaduje autentizácia používateľov. Ide o overenie identity používateľa. Inými slovami môžeme povedať, že autentizácia predstavuje proces dokazovania pravej identity používateľa, ktorý sa snaží o prístup do systému. Najčastejšie sa realizuje použitím prihlasovacieho mena a hesla. Existujú však aj ďalšie možnosti autentizácie, napríklad odtlačok prsta, geometria ruky, sietnica alebo dúhovka oka.

Podľa spôsobov dokazovania identity používateľov rozdeľujeme autentizáciu do nasledovných skupín:[4]

- Niečo poznám – obyčajne heslo alebo prístupový PIN kód. Prístup do systému je povolený osobe, ktorá pozná toto tajomstvo.
- Niečo mám – najčastejšie kľúč alebo prístupovú kartu. Prístup do systému je povolený osobe, ktorá vlastní tento objekt.
- Niekto som – prístup do systému získa len ten kto je nositeľom príslušných biometrických údajov.

Pri autentizácii heslom ide o snahu dodržať maximálnu úroveň bezpečnosti pri tvorbe hesla. Je potrebné, aby heslo bolo dostatočne dlhé, komplexné, nie ľahko odvoditeľné, pravidelne obmieňané, neopakujúce sa a samozrejme utajené. Tieto podmienky sú však nezlučiteľné s prirodzenou povahou človeka, a preto sa dnes dostávajú do popredia nástroje viacfaktorovej autentizácie v podobe čítačiek biometrických údajov či použitia tzv. Smart Cards. Aj tu je nevyhnutné použiť heslo, ktoré však už nepredstavuje jediný autentizačný prvok.

[4] *Budúcnosťou bezpečnosti je biometria.* [online]. 2003. [spracované 2011-03-29]. Dostupné na internete: <http://www.zive.sk/buducnostou-bezpecnosti-je-biometria/sc-3-a-256257/default.aspx>

1.1.4 Hodnota a ochrana dát

Otázka overenia identity používateľa a priradenia prislúchajúcich oprávnení však nie je jediná výzva zabezpečenia. Mnohé štúdie zaoberajúce sa bezpečnosťou tiež odhalili, že problém spôsobujú aj čoraz intenzívnejšie používané mobilné zariadenia. Na prenosných počítačoch a dokonca už aj na mobilných telefónoch možno ukladať súbory, ktorých strata zvyčajne predstavuje väčšiu škodu, ako je hodnota ukradnutého notebooku či strateného USB kľúča. Zarážajúca je skutočnosť, že množstvo organizácií si túto skutočnosť uvedomuje a neimplementujú pritom žiadnu formu šifrovania súborov a e-mailov, hoci potrebné nástroje sa dajú nájsť už priamo v operačnom systéme. Spomeňme napríklad šifrovanie pomocou EFS (Encrypting File System – systém šifrovania súborov) alebo technológiu BitLocker spoločnosti Microsoft, ktorá umožňuje šifrovať priamo celé disky alebo výmenné médiá. Samozrejme, nemôžeme zabudnúť ani na pravidelné zálohovanie súborov.

Mobilné zariadenia predstavujú hrozbu i z iného dôvodu. Ich používatelia sa počas svojej práce pripájajú do rozličných sietí s rozličnou úrovňou zabezpečenia (napr. v hoteli, na letisku, u klienta alebo prostredníctvom verejnej bezdrôtovej siete). V prípade, že dôjde k infikovaniu škodlivým kódom v týchto prostrediach, vynára sa tu hrozba rozšírenia nežiaduceho softvéru aj do vlastnej podnikovej siete. Nie je preto prekvapujúce, že narastá záujem o technológie, ktoré poskytujú účinný spôsob ochrany v tomto smere.[5]

1.2 Sociálne inžinierstvo

Pri výbere motta tejto kapitoly by azda najvýstižnejšie znela známa citácia Alberta Einsteina: „Len dve veci sú nekonečné: vesmír a ľudská hlúposť; aj keď tým prvým nie som si celkom istý“. Dejiny sociálneho inžinierstva sú dejiny ľudskej hlúposti a slabín ľudského vnímania. Sú to vlastnosti, ktoré sú zneužívané každý deň počas celej histórie ľudstva.[6]

[5] ULÍK, B. 2009. *Bezpečnosť ako nikdy sa nekončiaci proces.* [online]. 2009. [spracované 2011-03-29]. Dostupné na internete: <http://www.itnews.sk/tituly/infoware/2009-10-22/c129785-bezpecnost-ako-nikdy-sa-nekonciaci-proces>

[6] JIROVSKÝ, V. 2007. *Kybernetická kriminalita.* 1. vyd. Praha : Grada publishing, 2007, s. 195

1.2.1 História sociálneho inžinierstva

Jeden z najznámejších sociálnych inžinierov všetkých čias Kevin Mitnick svoje prvé pokusy zacielil na spôsob, akým oklamať dopravný systém v Los Angeles a ako využívať platené služby hromadnej dopravy úplne zadarmo. Zistil, že systém cestovných lístkov funguje na základe sústavy dierok označovaných na cestovnom lístku. Tieto označenia predstavovali dátum, čas a číslo linky. Už vtedy prišiel na to, že priateľsky naladený vodič ochotne zodpovedal na všetky jeho premyslené otázky a poradil mu, kde je možné zakúpiť strojček na označovanie cestovných lístkov. Získať nepoužité cestovné lístky bola tiež maličkosť. Odpadové koše na autobusových nástupištiach boli plné nevyplnených bločkov, ktoré vodiči na konci zmeny zahadzovali. Už v tomto rannom období využil niekoľko metód sociálneho inžinierstva, ktoré mu umožnili bezplatný presun po celom meste.[7]

Z nedávnej histórie je známa ďalšia metóda nazývaná *phreaking.* Pomocou tejto metódy bolo možné preniknúť do telefónnych sietí vďaka zneužitiu informácií pracovníkov telefónnej spoločnosti a znalosti fungovania tejto telekomunikačnej siete. Umožňovala napríklad:

- získať všetky informácie o ľubovoľnom používateľovi v telefónnej sieti,
- využívať tajné testovacie čísla na dlhé medzimestské hovory,
- zmanipulovať telefónnu ústredňu pomocou rôznych techník.

Aj šikovne uskutočnený telefonát s pracovníkom telekomunikačnej firmy s použitím príslušného žargónu, procedúr a s využitím informácii o sieti poskytoval množstvo informácií, ktoré sa dalo získať.

Slovo *hacker* nepredstavovalo vždy osobu v negatívnom slova zmysle. Spájalo sa s ľuďmi, ktorí trávili veľa času experimentovaním s počítačmi, programovaním alebo hľadaním rôznych riešení v tejto oblasti. Až postupným časovým vývojom získalo

[7] MITNICK, K. – SIMMON, W. 2003. *Umění klamu*. 1. vyd. Gliwice : Helion, 2003, s. 3-4

oslovenie hacker negatívne črty, ktoré významovo označujú osobu ako nebezpečného zločinca.

1.2.2 Definícia pojmu sociálny inžinier

V kultovej knihe o sociálnom inžinierstve „Umenie klamu“ Kevin Mitnick definuje rozdiel medzi podvodníkom a sociálnym inžinierom nasledovne: „Ten kto mámi od ľudí peniaze je obyčajný podvodník, ale kto využíva manipuláciu a presvedčovanie so zámerom získania informácií je sociálny inžinier.“ Práve táto aféra z uvedenej knihy upozornila na jeden z najslabších článkov počítačových systémov – na človeka. Tajomstvo ľahkosti prekonávania zábran a získavania prísne tajných informácií spočíva v osobnosti sociálneho inžiniera. Aj sociálny inžinier podobne ako osobnosť podvodníka musí v prvom rade vzbudzovať dôveru. Techniky ovplyvňovania ľudí uvádzané v jeho knihe nie sú nové, sú len prenesené do súčasného prostredia a dôvtipne využívajú manipuláciu prostredníctvom moderných technológií. Bolo preukázané, aká klamná je predstava bezpečnosti súkromných a firemných dát a aké jednoduché je obísť bezpečnostné systémy za milióny dolárov zneužitím ľudí, ktorí ich obsluhujú.

Americký Computer Security Istitute uviedol vo svojich výskumoch, že v priebehu roka zaznamenalo 85 % skúmaných organizácií narušenie počítačového zabezpečenia a 64 % zaznamenalo straty z dôvodov počítačových lúpeží napriek tomu, že boli implementované najrozličnejšie bezpečnostné technológie. Aj napriek snahe minimalizácie rizika sa často zabúda na to najdôležitejšie - na *ľudský faktor*. Dá sa očakávať, že s vývojom stále dokonalejších bezpečnostných technológií sa budú útočníci stále viac zameriavať na ľudské slabosti. Prekonanie ľudskej bariéry je častokrát omnoho jednoduchšie. Niekedy vyžaduje investície len na realizáciu telefónneho hovoru, nehovoriac o podstatne nižšom riziku odhalenia.

Existuje veľa definícií sociálneho inžinierstva, ktoré sú viac menej podobné:

Sociálne inžinierstvo sa označuje za „umenie ako prinútiť ľudí, aby splnili Vaše priania“ alebo za psychologické triky hrané na oprávnených používateľov systému za

účelom získania prístupu do tohto systému. Vo všeobecnosti ide o zneužitie najslabšieho článku, o šikovnú a premyslenú manipuláciu prirodzenej dôverčivosti človeka.[8]

Sociálne inžinierstvo predstavuje systematicky používané vedomosti ľudského správania sa a umenia presviedčať, aby používateľ 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.[9]

Sociálny inžinier pseudonymom Harl vo vystúpení na jednom fóre uvádza nasledovné: „Na svete neexistuje žiadny počítačový systém, ktorý by nebol závislý na ľuďoch. To znamená, že táto bezpečnostná slabina je univerzálna, nezávislá na platforme, sieti či druhu vybavenia. Ktokoľvek, kto má prístup k akejkoľvek časti systému, fyziky či elektronicky, predstavuje potenciálne bezpečnostné ohrozenie.“

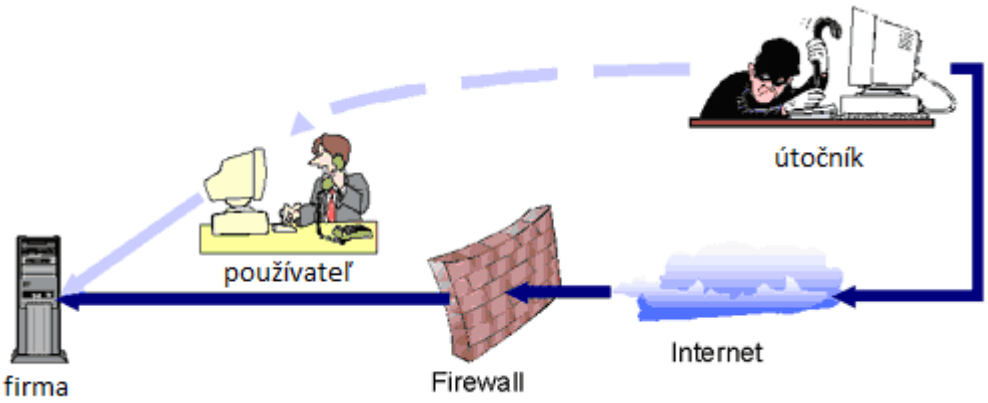
Sociálne inžinierstvo je metóda, prax či postup pomocou ktorej útočník získava dôveryhodné informácie využitím manipulácie používateľov. Sociotechnik zvyčajne využíva telefón alebo internet, aby zmanipuloval používateľov k vyzradeniu citlivých informácií alebo vo vykonaní nejakej akcie, ktorá nie je v súlade s typickou firemnou politikou. Táto metóda skôr zneužíva prirodzenú tendenciu osôb dôverovať slovám iných, ako by využívala prítomnosť bezpečnostných dier informačných systémov. Je všeobecne známe, že používatelia sú najslabším prvkom bezpečnosti a presne tento fakt robí sociálne inžinierstvo reálnym. Bezpečnosť je založená na dôvere – na dôvere v ochranu a autenticitu. Publikovaním článkov o konkrétnych hrozbách ich možno iba redukovať. Neskorší vývin situácie závisí len od kompetentností používateľov ako sa zachovajú v situáciách, keď príde k ohrozeniu.[10]

Po zhrnutí definícií dostávame vysvetlenie, že sociálne inžinierstvo alebo tiež používaný názov *sociotechnika* je útok narušiteľa z vonkajšieho prostredia, ktorý využíva

[8] JIROVSKÝ, V. 2007. *Kybernetická kriminalita.* 1. vyd. Praha : Grada publishing, 2007, s. 195
[9] RAK, R. – KUMMER, R. 2007. *Informační hrozby v letech 2007-2017*. In: Magazín Segurity, 2007, č. 1, s. 2 – 5
[10] GRANGER, S. 2001. *Social Engineering Fundamentals, Part I: Hacker Tactics*. [online]. 2001. [spracované 2011-03-22]. Dostupné na internete: <http://www.securityfocus.com/infocus/1527.html>

psychologické triky, city, vyhrážky na oprávnených používateľov informačných systémov, aby vyhoveli prianiam útočníka.

Podstatu sociálneho inžinierstva výstižne ilustruje nasledujúci obrázok. Názorne vysvetľuje, že pre útočníka je jednoduchšie zmanipulovať niekoho zvnútra - z prostredia spoločnosti, ktorý pomôže k prieniku. Podstatne zložitejší spôsob je pokus o prienik cez dobre zabezpečenú zónu firewallov a bez využitia sociotechnických metód.



Obrázok 1-1: Postavenia útočníka a obete

Zdroj: Dostupné na internete: <http://dnetzone.in/dhawaldamania/2011/04/05/what-is-social-engineering-well-it-is-not-what-it-reads-social-engineering-examples-and-prevention/#axzz1KirACZfp >, citované dňa 20.04.2011

Ochrana proti útokom sociálneho inžinierstva spočíva v dobre zapracovanej bezpečnostnej politike firmy a v jej dôslednom dodržiavaní.

Útoky použitím sociálneho inžinierstva sa odohrávajú v dvoch rovinách:

- fyzickej,
- psychologickej.

1.2.3 Sociotechnický cyklus

Tak ako každý trestný čin má všeobecný vzor, tak aj všetky útoky sociálneho inžinierstva sú všeobecne uskutočňované podľa vzorovej schémy tiež nazývanej sociotechnický cyklus. Každý útok sociálneho inžinierstva je jedinečný, pretože môže

zahŕňať viacnásobné fázy a 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.

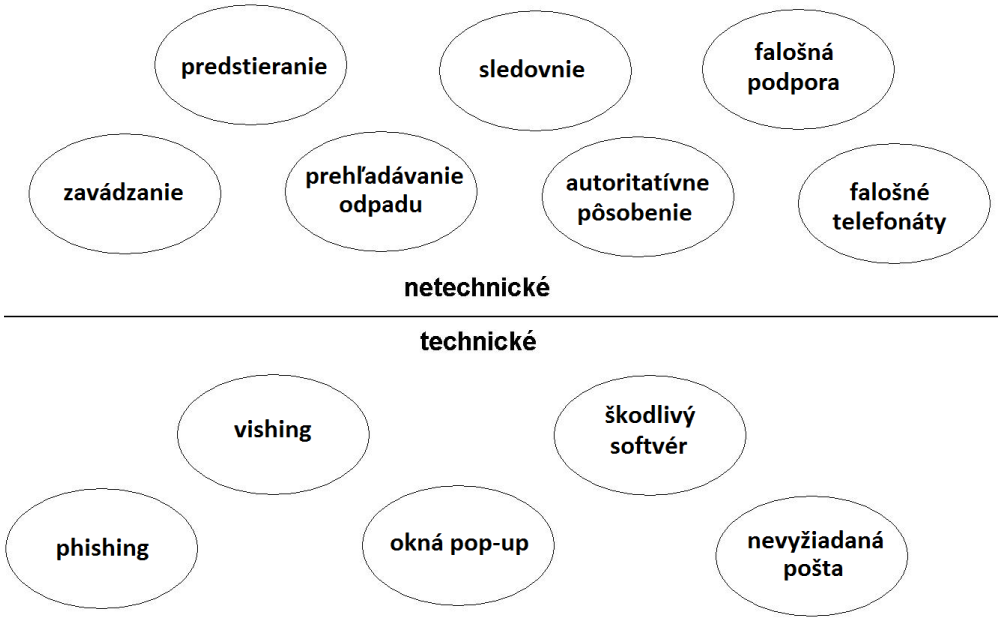
Obrázok 1-2: Sociotechnický cyklus

Techniky založené na zlyhaní ľudského faktora alebo využívajúce podvedomé zvyky a vlastnosti jedinca sú základom metód sociálneho inžinierstva. Sociálny inžinier zneužíva slabé miesta v bezpečnostnej politike firmy, svoje schopnosti manipulácie a vytvárania pripravených situácií. Vlastná práca sociálneho inžiniera začína prieskumom voľných a dostupných zdrojov informácií, najčastejších webových stránok firmy, rôznych marketingových materiálov alebo inzerátov.

Na základe zistených skutočností začína budovať vzťahy s vytipovanými osobami a získava si ich dôveru, ktorú následne zneužije pre získanie potrebných informácií. Tu by mal sociotechnický cyklus skončiť, avšak veľakrát sa opakuje v novom prostredí, lebo získanie jednej informácie v tomto cykle nemusí viesť k dokončeniu plánovaného útoku.[11]

1.2.4 Zhromažďovanie informácií s využitím sociotechnických metód

Vo fáze zhromažďovania údajov sociotechnici veľmi radi využívajú najrôznejšie metódy. Nasledujúci obrázok prehľadne zobrazuje väčšinu z nich:



Obrázok 1-3: Metódy sociálneho inžinierstva

Zdroj: Dostupné na internete:
http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf, citované dňa 15.4.2011

Voľné zdroje

Pod voľnými zdrojmi si môžeme predstaviť informácie prístupné verejnosti, ktoré sú dostupné na sieti internet, v tlačenej podobe alebo iné materiály získané inými zákonnými postupmi, napr. na tlačovom oddelení spoločnosti, uplatnením zákona o slobodnom prístupe k informáciám a podobne. Niekedy je až neuveriteľné, čo všetko

[11] JIROVSKÝ, V. 2007. *Kybernetická kriminalita.* 1. vyd. Praha : Grada publishing, 2007, s. 196

môžeme zistiť pomocou internetových vyhľadávačov. Užitočné sú aj rôzne databázy, ktoré sú plné obchodných a iných kontaktov. Podstatným zdrojom sú webové stránky cieľovej spoločnosti, jej reklamné brožúry, obchodná história a iné. V týchto zdrojoch sa vyskytuje veľké množstvo mien, telefónnych čísel, e-mailových adries a ďalších zdanlivo neužitočných informácií, ktoré pre šikovného sociálneho inžiniera skladajúceho tieto útržkovité informácie do jedného celku predstavujú nesmierne dôležitý zdroj informácií.

Internet však skrýva pre sociálne inžinierstvo veľa možností, kde rola sociotechnika nemusí byť len pasívna. K nim patria nasledovné metódy:

Priamy prístup k informáciám

Táto metóda je časovo náročnejšia, ale výsledný efekt býva najlepší, pretože iba osoby, ktoré si získali určitú úroveň dôvery cieľovej osoby (zamestnanec, podriadený, obchodný partner, upratovačka, opatrovateľka, ošetrovateľka, priatelia, spolubývajúci) môžu postupne získať oficiálny prístup do určitých objektov a odcudziť požadované informácie, resp. môžu získať prístup k vašim osobným údajom, informáciám o platoch, poistení alebo k bankovým informáciám. Týmto spôsobom môžu získať všetky druhy dôverných informácií, ktoré môžu byť ďalej zneužiteľné. Získanie dôvery však vyžaduje dôkladnú prácu so subjektom, aby tento neprehliadol ich nekalé záujmy.

Krádež hardvéru a dokumentov

Táto metóda je najčastejšia, lebo je pomerne jednoduchá. Ľudia často podceňujú dátový obsah svojich elektronických zariadení, a preto na nich majú aj informácie, ktoré by tam mať nemali. Z toho dôvodu môže byť aj krádež mobilného telefónu pre dosiahnutie cieľa kľúčová. Sú v ňom telefónne čísla, kontaktné informácie, v plánovači je možné nájsť dátumy narodenín, schôdzok a množstvo iných, zdanlivo nepodstatných informácií, ktoré však môžu byť zručnými manipulátormi veľmi dobre zneužité. Po krádeži techniky z budov, v MHD, z peňaženky, z tašky na ulici či z hotelov, sú ukradnuté dokumenty a technika podrobne analyzované s cieľom získať akékoľvek použiteľné informácie pre neskoršie možné využitie.

Reverzné sociálne inžinierstvo

Technici a správcovia sietí v organizáciách nie sú dokonalí a častokrát sa stretávajú s problémami, ktoré nie sú schopní vyriešiť sami. Toto sú priam otvorené dvere pre sociotechnikov, ktorí vedia zahrať úlohu radcu a v dialógu vylákajú z obete množstvo cenných informácií. Aj v tomto prípade nemusí sociotechnik len pasívne čakať na príležitosť. Pokiaľ aspoň čiastočne pozná prostredie, môže problém sám vopred spôsobiť a následne už len čakať. Správca musí vzniknutý problém riešiť a sám sa pri tom chytí do nastraženej pasce sociálneho inžiniera.

Reverzné sociálne inžinierstvo má 3 fázy:

1. Sabotáž – útočník spôsobí chybu v systéme.
2. Inzercia – útočník ponúka svoje vedomosti a pomoc na vyriešenie problému.
3. Asistencia – útočník skutočne pomáha chybu odstrániť, medzitým však získava inak neprístupné informácie.

Phishing

Slovo phishing je odvodené z anglického slova fishing (rybárčenie). Phishingom nazývame metódu sociálneho inžinierstva, ktorá využíva podvodné e-maily a webové stránky predstierajúce legálne obchodné aktivity, aby tak od používateľov vylákali dôverné informácie. Sociotechnici veľmi často využívajú možnosť vytvoriť webovú stránku, ktorá pôsobí navonok seriózne a ponúka používateľovi bezplatnú registráciu. Registrácia je zvyčajne motivovaná nejakým darčekovým predmetom a následne slúži ako trójsky kôň pre získavanie hesiel zaregistrovaných obetí. Úspešnosť tejto aktivity je pomerne vysoká - okolo 20 %.

Iný spôsob šírenia phishingových správ je, keď správy napodobňujú bankové alebo obchodné listy a ich cieľom je zmanipulovať ľudí k odovzdaniu osobných informácií ako čísla kreditných kariet, čísla účtov a heslá k nim. Typickým príkladom sú tzv. „Nigérijské listy“, falošné webové stránky bánk alebo on-line obchodov navádzajúce obete k uvádzaniu citlivých osobných informácií a identifikačných údajov. Legálne webové

stránky spoločností sa bránia proti phishingu tak, že informujú používateľov o tom, že vás nikdy nebudú kontaktovať uvedeným spôsobom.[12]

Sociotechnici, ktorí využívajú metódy phishingu sa nazývajú *Phisheri.* Najlepšia ochrana proti phishingu je nedôverovať stránkam a e-mailom, pomocou ktorých sa sociálny inžinier snaží od obete vylákať citlivé údaje, najmä heslá. Zároveň sa odporúča použiť rôzne prihlasovacie údaje. Osvedčenou metódou je kontrola odkazov v phishingových správach nasledovným spôsobom. Keď ukážeme kurzorom myši na priložený odkaz, v ľavom dolnom rohu sa objaví skutočná adresa odkazu.[13]

Obrázok 1-4: Príklad podvodnej stránky internet bankingu vyžadujúce viacnásobné vyplnenie identifikačných údajov

Zdroj: Dostupné na internete:
< https://moja.tatrabanka.sk/cgi-bin/ibanking/start/help_page.jsp?type=priklady&lang=sk>,
citované dňa 09.04.2011

[12] *Social Engineering.* [online]. 2009. [spracované 2011-02-02]. Dostupné na internete: http://www.cknow.com/cms/vtutor/social-engineering.html
[13] *Phishing.* [online]. 2011. [spracované 2011-02-08]. Dostupné na internete: http://sk.wikipedia.org/wiki/Phishing

Obrázok 1-5: Príklad podvodnej stránky internet bankingu vyžadujúce viacnásobné vyplnenie identifikačných údajov

Zdroj: Dostupné na internete:
< https://moja.tatrabanka.sk/cgi-bin/ibanking/start/help_page.jsp?type=priklady&lang=sk>,
citované dňa 09.04.2011

Thrashing - prehľadávanie odpadu alebo odpadkových košov

V anglickej literatúre sa s touto metódou stretneme pod názvom dumpster diving. Na prvý pohľad sa nám môže zdať táto metóda nepohodlná až nehygienická, ale predstavuje veľmi bohatý zdroj informácií. Je až neuveriteľné, koľko citlivých informácií dokážu potenciálne obete týmto spôsobom vyprodukovať. Častokrát sa v odpade vyskytnú účty za telefón, výpisy z bankových účtov, rôzne obchodné materiály, aktuálne informácie o stave spoločnosti, plány, kontakty, firemné telefónne diáre, organizačné štruktúry spoločností, manuály, kalendáre schôdzok, formuláre, údaje o termínoch dovoleniek, výnimkou nie sú aj vytlačené dôverné materiály, prihlasovacie mená a heslá, zdrojové kódy, CD-ROM a iné záložné médiá, starý nefunkčný hardvér a mnoho iných. Skúsený sociotechnik takýto bohatý zdroj otvorených informácií určite nevynechá. Útočníkovi tieto informácie poskytnú množstvo informácií o obetiach – ich mená, telefónne čísla, postavenie v spoločnosti, kalendár. Systémové manuály, zdrojové texty, prihlasovacie mená a heslá sú návodmi ako vykonať útok na informačné technológie firmy.

Z poškodeného hardvéru a pamäťových médií sa overenými postupmi dá zrekonštruovať ich dátový obsah a ten náležite využiť.[14]

Pharming

Slovo pharming je odvodené z anglického slova pharming (farmárčenie). V podstate sa jedná o zdokonalenú metódu phishingu, ktorá presmeruje internetové spojenie medzi IP adresou a cieľovým serverom. Každej mennej adrese napríklad http://moja.tatrabanka.sk prislúcha číselná IP adresa napríklad 213.215.88.236.

K zneužitiu metódou pharmingu môže dôjsť napadnutím a modifikáciou servera DNS, ktorý prekladá tieto menné adresy na IP adresy alebo na lokálnom počítači prostredníctvom „Trójskeho koňa", ktorý vykoná príslušné modifikácie súborov. Následne pri každom prístupe používateľa na adresu správnej stránky je podvodne presmerovaný na falošnú stránku bez toho, aby zadal do príkazového riadku prehliadača nesprávnu adresu. Falošné webové stránky často predstavujú veľmi dokonalé kópie a sú na nerozoznanie od originálnych webových stránok.Tu nám niekedy nepomôže ani obozretnosť a ani opatrnosť, pretože útok bol vykonaný voči službe DNS (Domaine Name System) serverov poskytovateľa internetového pripojenia, na ktorú v podstate nemáme priamy dosah.[15]

Advance-fee fraud

Táto metóda predstavuje veľmi triviálny až naivný, no v realite dobre fungujúci spôsob zneužitia, kde jedinci svojím neuváženým správaním môžu prísť k značným stratám na majetku. Podstatou je zavádzanie a snaha o vymámenie peňazí na zdanlivo charitatívne účely zabalené do rozprávkových príbehov apelujúcich na ľudskú chamtivosť. Útočníci veľmi často predstierajú svoj príbeh ako dramatický boj o život v neľudských podmienkach a potenciálnej obeti ponúknu možnosť získať obrovské množstvo majetku.

Tento druh zneužitia sa často nazýva „Nigérijskými listami". Majú pôvod z Nigérie, kde sa prvý krát objavili v roku 1980 a začali sa šíriť po svete. Na začiatku boli distribuované klasickou poštou, neskôr zasielaním faxov až dnes e-mailom. Do tejto

[14] MITNICK, K. – SIMMON, W. 2003. *Umění klamu.* 1. vyd. Gliwice : Helion, 2003, s. 108-109
[15] *Phishing a Pharming – krátke predstavenie 2.* [online]. 2007. [spracované 2011-02-15].
Dostupné na internete: http://dennik.inet.sk/clanok/5038-phishing-a-pharming-kratke-predstavenie-2/

skupiny podvodov radíme aj fiktívne oznámenie o výhre v lotérii po tom, ako bola vylosovaná vaša e-mailová adresa.[16]

Krádež klasickej pošty a jej presmerovania

Krádež korešpondencie z poštovej schránky je veľmi jednoduchá záležitosť, pretože bežná poštová schránka absolútne nechráni bankovú korešpondenciu (bankové karty, výpisy z účtov a iné), formuláre, ponuky kreditných kariet a ďalšie. Rovnako nie sme chránení ani pred nepoctivými pracovníkmi pošty. Tieto dokumenty sú neoceniteľné, pretože použitím Vášho mena a zaslaním dokumentov späť môže neznáma osoba požiadať o zmenu adresy, zaslanie platobnej karty a pod.

Čítanie cez plece

V anglickej literatúre sa označuje ako *shoulder surfing*. Táto známa metóda opisuje prípady, keď sa vám môže stať, že pri výbere hotovosti z bankomatu sa okolo vás ponevierajú ľudia, ktorí môžu mať záujem o získanie vašich osobných informácií, akými sú napr. vaše osobné PIN kódy k platobným kartám. Spomínaná metóda je často využívaná vo veľkej miere.

1.2.5 Budovanie vzťahov a dôvery

Najčastejšie je sociotechnický útok zameraný na osobu, ktorá si neuvedomuje dôležitosť informácií, s ktorými pracuje a ktoré poskytuje iným. Prvým predpokladom úspešnej práce sociotechnika je, že pracovníci firiem nie sú naivní a očakáva podozrievavosť alebo odpor. Plán útoku musí byť vždy vopred dokonale pripravený podobne ako v šachovej partii, kde je nutné predvídať otázky, aké mu môže obeť klásť a mať pripravené patričné odpovede.

Typickou prácou sociotechnika v tejto fáze je budovanie pocitu dôvery a vytvorenie vzťahov s obeťou. Útočník si uvedomuje, že jeho práca je časovo náročná, že nemôže na obete vyvíjať nátlak, a tak sa obvykle prvý rozhovor týka obyčajných každodenných záležitostí. V situácii, keď ľudia nemajú dôvod k podozrievavosti, si útočník ľahko získa

[16] *"Advance Fee Fraud" Schemes.* [online]. 2010. [spracované 2011-02-15]. Dostupné na internete: http://www.sec.gov/answers/nigeria.htm

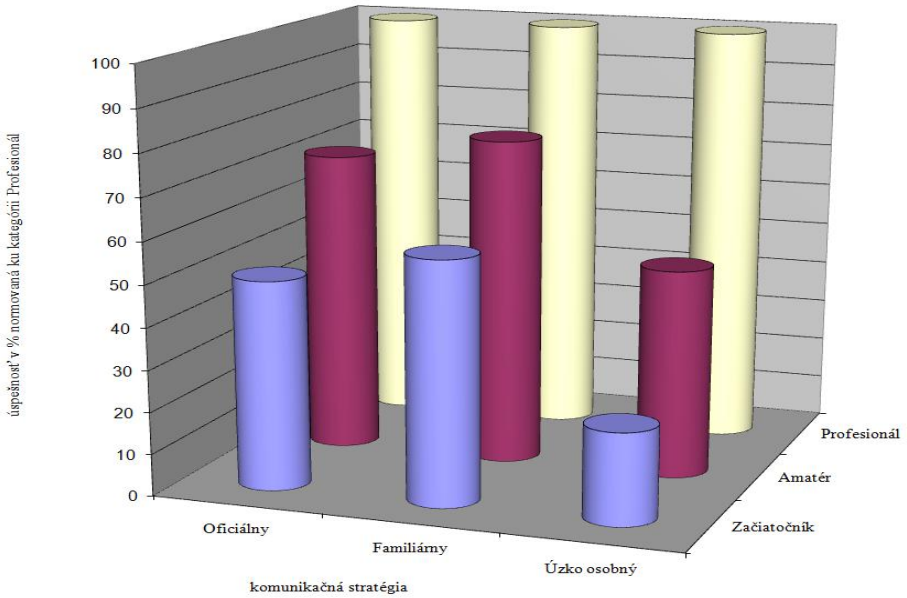
ich dôveru. Neskôr nastáva obdobie vyťažovania obete, keď tieto obyčajné rozhovory môžu byť doplnené zdanlivo nevinnými otázkami vedúcimi k získaniu požadovanej informácie. Často obeť ani netuší, že sa stala zdrojom dôležitých informácií.

Súčasťou sociotechnického útoku je vhodne zvolená komunikačná stratégia. V zásade je možné tieto stratégie rozdeliť na tri základné prístupy, ktoré útočník volí podľa svojho odhadu mentality cieľovej obete:

- *Oficiálna komunikačná stratégia* – keď v rozhovore nie je prípustný familiárny tón, celá komunikácia prebieha veľmi pôsobivo, pracovne a seriózne, počas tohto typu rozhovoru nemusí útočník poznať osobné údaje o cieľovej osobe, je však nutné, aby komunikácia vyznievala veľmi profesionálne, útočník sa musí veľmi dobre orientovať v odbore zamerania cieľovej osoby.

- *Familiárna komunikačná stratégia* – vychádza zo znalosti niektorých osobných údajov a rysov cieľovej osoby, často sú útoky vedené voči obeti opačného pohlavia, pričom sa volí žartovný až flirtujúci tón. Táto stratégia vyžaduje nielen orientáciu v prostredí cieľovej osoby, ale aj isté herecké vlohy, ktoré umožňujú útočníkovi využívať moduláciu hlasu ako súčasť zvolenej stratégie.

- *Úzko osobná komunikačná stratégia* – stratégia spočíva vo vyvolaní presvedčenia v cieľovej osobe, že sa dlho poznáme a sme dôverní priatelia. Ide o najzložitejší sociotechnický útok vyžadujúci množstvo podrobných informácií o obeti. Tento typ útoku môže veľmi často stroskotať na neznalosti nepatrného detailu, prípadne ak útočník nepôsobí dostatočne presvedčivo. Ak sa komunikácia vyvíja týmto smerom môže to vyvolať dominový efekt narastajúcej nedôvery.



Graf 1-1: Úspešnosť útoku podľa typu komunikácie

Zdroj: JIROVSKÝ, V. 2007. *Kybernetická kriminalita.* 1. vyd. Praha : Grada Publishing, 2007, s. 200

Význam a dôležitosť voľby vhodnej komunikačnej stratégie vyplýva najmä zo skutočnosti, že len nepatrné percento sociotechnických útokov zahrňuje fyzické stretnutie útočníka a cieľovej osoby – obeti. Veľká väčšina útokov je realizovaná pomocou telekomunikačných prostriedkov alebo internetu, čo výrazne zjednodušuje predstieranie totožnosti a manipulácie s cieľovou osobou.

1.2.6 Prostriedky a ciele sociotechnického útoku

Pri sociotechnických útokoch sú používané najrôznejšie kombinácie prostriedkov, metód a prostredia. K základným prostriedkom patrí telefón, e-mail, internetový chat v reálnom čase, bežná papierová korešpondencia alebo osobný kontakt. Posledný menovaný prostriedok môžeme považovať za jeden z najrizikovejších. Preto sa častejšie volia menej rizikové spôsoby.

Telefónne útoky

Medzi najstaršie metódy sociálneho inžinierstva patria telefónne útoky, ktoré sú založené na anonymite volajúceho. Predstavujú zároveň najobľúbenejšie a najúčinnejšie zbrane útočníka, dajú sa v nich skryť emócie a hlavne skutočná podoba či identita

volajúceho. Aj keď so zavedením signalizácie a identifikácie prichádzajúceho hovoru už nie je také jednoduché predstierať skrytú identitu a „skryté číslo“ je vždy podozrivé, obľúbenosť tejto metódy neklesla. Medzi najviac zraniteľné oblasti zamerania útočníka patria informačné linky spoločností – *helpdesk*. Pracovníci týchto liniek sú na jednej strane trénovaní v asertívnom správaní k volajúcim a sú vedení k tomu, aby boli ochotní, priateľskí a podávali požadované informácie. Na druhej strane, operátorom helpdesku je v princípe jedno, kto volá a prečo potrebuje práve tieto informácie, ktoré si klient žiada. Vzdelávaniu operátorov helpdesku v odbore bezpečnosti nebýva často venovaná osobitná pozornosť. Ak v tomto smere nie je presne definovaná bezpečnostná politika a nie je jednoznačne ohraničená štruktúra a rozsah informácií, ktoré môžu zamestnanci helpdesku podávať, býva táto oblasť skutočným rajom pre sociálnych inžinierov.

V telefonických útokoch majú veľkú výhodu osoby ženského pohlavia. Príjemne znejúci ženský hlas na druhom konci linky žiadajúci drobnú informáciu má veľkú výhodu, obzvlášť pri komunikácii s príslušníkom opačného pohlavia. Najvýznamnejšiu úlohu však hrá schopnosť sociotechnika odhadnúť psychické rozpoloženie obete útoku a adekvátna reakcia na neho.

Pokiaľ útočník nepoužije techniku priameho dotazu, je dôležité rozčleniť konverzáciu do množstva nepodstatných otázok a odpovedí a medzi túto „hovorovú vatu“ vložiť otázky, ktoré nás skutočne zaujímajú. Útočník nikdy hovor neukončuje ihneď po tom, keď sa dozvedel pre neho dôležité informácie, lebo obeť si spravidla najviac pamätá niekoľko posledných okamžikov telefonátu. Posledný čas rozhovoru má byť venovaný väčšinou nejakej neškodnej konverzácii. Nikdy nie je dobré na obeť naliehať, môže to celé úsilie zmariť. V prípade, že sa rozhovor nevyvíja tak ako by mal, je dobré radšej hovor nenápadne ukončiť použitím nejakých zdvorilostných fráz. Dobre zvládnuť telefonický hovor nie je ľahké a vyžaduje to schopnosť improvizácie a isté herecké vlohy. Sociotechnik musí byť vnímavý a nesmie podľahnúť panike pri nepatrných odchýlkach správania sa obete, keď sa rozhovor nevyvíja podľa jeho predstáv. Cesta k úspešnému zvládnutiu útoku pomocou telefonického rozhovoru vedie cez dlhé roky praxe. [17]

[17] JIROVSKÝ, V. 2007. *Kybernetická kriminalita.* 1. vyd. Praha : Grada publishing, 2007, s. 201

Metódy presvedčovania obetí

Všetky metódy sociotechnického útoku majú spoločný cieľ – oklamať obeť útoku. Medzi základné faktory, ktoré ovplyvňujú výsledok útoku patrí:

- Schopnosť sociotechnika presvedčiť obeť, že je pánom situácie a že všetko robí zo svojej vlastnej vôle a bude za to odmenená. Odmena pritom nemusí byť hmotná, stačí napríklad dobrý pocit z potešenia nadriadeného alebo dobrého skutku priateľskej výpomoci.

- Nebyť príliš vtieravý, nevyvíjať veľký nátlak na obeť. Ten často vedie k podráždeniu obete a následnému neúspechu.

- Byť priateľský. Keď už zlyhá všetko, tak priateľský úsmev a tón hlasu môže pomôcť aj v inak prehratej situácii. Väčšina z nás totiž verí v dobrotu a poctivosť ostaných ľudí.

S použitím týchto pravidiel využívajú sociotechnici psychické vlastnosti obetí, ktoré tvoria prakticky neodstrániteľné bezpečnostné diery. Medzi najbežnejšie slabiny v tejto oblasti, ktoré sú sociotechnikmi využívané patria:

- Pocit zbavenia sa zodpovednosti – obeť jednoduchšie plní útočníkove požiadavky, keď má pocit, že zodpovednosť za toto konanie nenesie sama. Pre vyvolanie tohto stavu stačí spomenúť pár ďalších mien spolupracovníkov, ktorí sú už zapojení do celého procesu alebo prehlásiť, že nejaký vyšší nadriadený už všetko schválil.

- Nádej na lepšie postavenie v spoločnosti – keď obeť uverí, že po splnení úlohy dostane nejakú odmenu, vždy ju to povzbudí k splneniu úlohy.

- Dôvera – vytvorenie pocitu dôvery, ako už bolo spomínané, je jedným z najdôležitejších krokov v sociotechnickom cykle.

- Morálna povinnosť – snaží sa vyvolať v obeti pocit presvedčenia, že obeť svojím konaním zabráni bezpráviu, keď splní požiadavky útočníka.

- Pocit viny – vytvorením scenára a situácie, ktoré zapôsobia a vytvoria psychický tlak na obeť, ktorá sa bude snažiť zbaviť pocitov viny a urobí všetko čo je potrebné.

- Túžba byť užitočný – človek má vrodenú vlastnosť dobrého pocitu z vykonania dobrého skutku a tak rád niekomu pomôže.

Útoky použitím nástrojov internetovej komunikácie

Medzi nástroje priamej komunikácie patria komunikačné nástroje s okamžitým pripojením, kam môžeme zaradiť napr. ICQ, Skype, Netmeeting, IRC alebo rôzne iné webové chaty. Veľmi silným nástrojom komunikácie je elektronická pošta. Princípy sociotechnickej práce, aj keď ide o iné médium, ostávajú rovnaké – využitie ľudských slabostí pre získanie požadovanej informácie.

K najbežnejším nástrojom na vylákanie potrebnej informácie je elektronická pošta, kde medzi základné metódy patrí už spomínaná metóda pishingu. Podobne ako použitím metódy phishingu je možné zneužiť aj iný prostriedok hromadnej diskusie – fórum alebo internetový chat. O zneužití fóra pre získanie informácií, keď sociotechnik predstiera radcu a pomocníka sme sa už zmienili. Chat má svoje špecifiká, ktoré vyplývajú z jeho priebehu v reálnom čase s virtuálnymi komunitami, ktoré sa v chatovacej miestnosti nachádzajú. Základom útoku je znalosť prezývky obete, ktorú nie je vždy jednoduché získať. Jednoduchšie sa niekedy dá získať zoznam IP adries účastníkov chatu a na jeho základe možno potom vybrať adresy prislúchajúce cieľovej sieti. Takýto útok má všetky atribúty sociálneho inžinierstva a spĺňa aj sociotechnický cyklus.[18]

Počiatočné nadväzovanie kontaktu vyžaduje predbežné štúdium správania sa cieľovej osoby, zistenie okruhu tém, ku ktorým prispieva alebo názorov, ku ktorým sa prikláňa. Na základe vytvoreného psychologického profilu cieľovej osoby potom útočník vypracováva plán, ktorým by sa mal útok riadiť.

[18] MCCLURE, S. – SCAMBRAY, J. – KUTZ, G. 2007. *Hacking bez záhad.* 1. vyd. Praha : Grada Publishing, 2007. s. 28-32

V zásade existujú 2 plány:

- priateľský - pri priateľskom útoku je snaha nadviazať s cieľovou osobou čo najužší kontakt a postupne od nej vylákať požadované informácie,

- ofenzívny – tento útok je náročnejší vzhľadom na to, že cieľová osoba je najskôr podrobená napádaniu zo strany útočníka. Existuje však riziko, že obeť z chatovacej miestnosti odíde. V prípade ofenzívnej metódy zvyčajne útočník používa dve prezývky – jednu pre napádanie a druhú pre obranu osoby. Obeť bude po obrane tou druhou osobou náchylnejšia viac dôverovať. Aj keď táto taktika má celý rad rizík, je väčšinou úspešnejšia a rýchlejšia ako iné taktiky.

Prostriedky priamej komunikácie vyžadujú bližšiu znalosť cieľovej osoby alebo komunity, v ktorej sa táto osoba pohybuje. Hoci identifikátory účastníkov sú k dispozícii na adresárových serveroch, je veľká pravdepodobnosť, že neznáma osoba bude odmietnutá, pokiaľ nepríde s nejakým konkrétnym návrhom alebo témou. Možno hovoriť teda o internetovej podobe telefónneho útoku, ktorá však má tú výhodu, že odpoveď cieľovej osoby bude zaznamenaná, bude ju možné ďalej skúmať, a tak dôkladnejšie pripraviť odosielaný text. Rovnakú výhodu má však aj druhá strana, a preto je väčšia pravdepodobnosť odhalenia útoku.

1.3 Ochrana pred sociálnym inžinierstvom

Základom každej úspešnej obrany je dobre spracovaná bezpečnostná politika, ktorá vymedzuje časti organizácie, kde sa vyžaduje vysoký stupeň ochrany dát. Často sa aj vo veľmi dobre spracovaných bezpečnostných politikách zanedbávajú menej samozrejmé, no rovnako zraniteľné oblasti. Patria sem pracovníci na nižších pracovných pozíciách, ktorí prichádzajú do styku s okolitým prostredím organizácie – klientmi, dodávateľmi, spolupracujúcimi firmami a pod. Túto oblasť nazývame *oblasť prvej línie* a patria sem napríklad sekretárky, pracovníci helpdesku, call centier a recepcie a pod. Tieto osoby prvej línie bývajú často primárnym cieľom vznikajúceho sociotechnického útoku. Je preto dôležité oboznámiť ich, s príznakmi sociotechnického útoku a vysvetliť im, ako sa v

prípade podozrenia útoku zachovať. Je potrebné objasniť, aký stupeň utajenia majú jednotlivé informácie a ktoré z nich môžu či nemôžu poskytovať iným osobám. Je nevyhnutné, aby títo ľudia zvládli niekoľko základných techník overovania totožnosti pri kontakte s inými osobami. Existuje viacero základných postupov pre zníženie miery nebezpečenstva pred sociotechnickými útokmi:

- Metóda z dôb prohibície – ide o zabezpečenie chránenej informácie, ktoré vyžaduje znalosť miesta, kde sú informácie umiestnené, a hesla, ktoré umožňuje do tohto miesta v počítačovom systéme vstup.

- Zdôrazňovanie dôležitosti a významu hesiel ako aj ich správnej voľby, tak aj manipulácie s nimi. Súčasťou takéhoto postupu je aj nekompromisné odstraňovanie prvotných prístupových hesiel zo zariadení. Prvotné heslo je prístupové heslo, ktoré sa do zariadenia vkladá pri výrobe a umožňuje prvý prístup k zariadeniu pri jeho inštalácii. Firma je často presvedčená o svojej dokonalej ochrane, no veľakrát sa v zariadeniach ponechávajú prvotné heslá, čo predstavuje vážne bezpečnostné riziko. Pre skúseného útočníka to vytvára takú situáciu, ako keby tam žiadne heslo nebolo.

- Prepracovaný mechanizmus práce s bezpečnostnými kódmi – musia existovať jednoznačné smernice o ich používaní a musia byť definované kroky, ako postupovať pri vyžadovaní bezpečnostného kódu v neadekvátnych prípadoch alebo pri zlyhaní overovacieho procesu.

- Jasné a rýchle postupy pri zrušení pracovného pomeru a v priebehu výpovednej lehoty zamestnancov – skúsenosti a štatistika hovoria, že najväčšie nebezpečenstvo hrozí zo strany bývalých zamestnancov. Títo majú detailné znalosti o miestach, kde sú uložené dôležité informácie a vedia, kde môžu zaútočiť tak, aby škody boli čo najväčšie. Je preto nevyhnutné prepusteného pracovníka ihneď vyškrtnúť zo zoznamu zamestnancov a pokiaľ možno poskytnúť túto aktualizáciu aj ostatným spoločnostiam, s ktorými firma úzko spolupracuje. Prepustený zamestnanec musí tiež odovzdať všetky identifikátory, kľúče a elektronické prístupové zariadenia.

- Preverovanie zamestnancov – informatikov – veľká väčšina z nich má totiž privilegovaný prístup do podnikovej siete, lebo je to súčasť ich práce. Je potrebné zvážiť, komu a čo sprístupniť, zaviesť mechanizmy kontroly prístupu k citlivým údajom. Niektoré firmy dokonca sledujú svojich informatikov, či u nich nedošlo k nejakej podstatnej zmene správania, či nemajú príliš drahé koníčky, neholdujú hazardným hrám, drogám a iným finančne náročným aktivitám.

Ochrana pred sociotechnickými útokmi nie je jednoduchá, lebo smeruje na najmenej spoľahlivý, a pritom najzložitejší element celého systému – na človeka. Nasledujúca tabuľka zahrňuje jednotlivé oblasti sociotechnického útoku spolu s najpoužívanejšími taktikami a spôsobmi obrany.

Tabuľka 1-2: Oblasti sociotechnických útokov, taktika a ochrana

Oblasť útoku	**Sociotechnické taktiky**	**Ochrana**
telefón (help desk)	predstieranie identity, presvedčovanie	zamestnanci nesmú uvádzať žiadne heslá a dôverné informácie
vchod do budovy	vniknutie v prezlečení	preukazy, bezpečnostná služba, tréning zamestnancov
kancelária	nahliadanie cez rameno	heslá písať len s istotou, že sa nikto nepozerá
kancelária	prehľadávanie budovy a hľadanie odomknutých dverí	každý hosť by mal byť sprevádzaný
serverové miestnosti	pokus o prihlásenie sa, odstránenie vybavenia, nahratie škodlivého softvéru	serverové miestnosti by mali byť permanentne uzamknuté, mal by byť vedený inventár ich vybavenia
telefónna ústredňa	krádež liniek a presmerovanie	kontrola ústredne, monitoring uskutočnených hovorov
odpadkové koše	prehľadávanie odpadkov	odpadkové kontajnery v zabezpečenej a monitorovanej oblasti, skartovať všetky dôležité dokumenty, bezpečné mazanie magnetických médií
internet - intranet	softvér na odchytávanie hesiel	sledovanie programového vybavenia počítačov, antivírusové vybavenie
kancelária	odcudzenie dokumentov	hierarchia dôveryhodnosti dokumentov a adekvátne zaobchádzanie s nimi

Zdroj: JIROVSKÝ, V. 2007. *Kybernetická kriminalita.* 1. vyd. Praha : Grada Publishing, 2007, s. 207

2 CIEĽ PRÁCE, METODIKA PRÁCE A METÓDY SKÚMANIA

Hlavným cieľom diplomovej práce je dôkladná analýza metód sociálneho inžinierstva a ich dopadov na chod firmy a používateľov. Cieľom je podrobné zmapovanie hrozieb súvisiacich s bezpečnosťou informačných a komunikačných technológií v súvislosti so sociotechnickými útokmi, dôkladná prevencia a možnosť ako v maximálnej možnej miere týmto útokom predchádzať. Ďalším cieľom diplomovej práce je zhodnotiť súčasný stav v predmetnej oblasti a ponúknuť riešenia ochrany a prevencie pred dopadmi týchto útokov.

V súčasnej dobe prudkého rozmachu informačných a komunikačných technológií patrí otázka bezpečnosti medzi najviac preferované oblasti. Oblasť sociálneho inžinierstva v rámci bezpečnosti informačných a komunikačných technológií sa sústreďuje na najzraniteľnejší a zároveň najkomplikovanejší článok, a tým je človek sám. Správanie sa ľudí ako najslabšieho článku počítačových systémov je z hľadiska bezpečnosti informačných systémov kľúčové.

Správne informácie v správny čas a na správnom mieste predstavujú základ dobrých rozhodnutí pri konkrétnych otázkach v budúcnosti. Žijeme doslova v záplave informácií, z ktorých sú niektoré kľúčové, iné menej dôležité. Práve metódy sociálneho inžinierstva predstavujú negatívny fenomén v snahe premyslenou manipuláciou prirodzenej dôverčivosti človeka tieto informácie vylákať a následne ich zneužiť. Dôkladné poznanie práce sociálneho inžiniera, jeho metódy, myslenie, postupy nám následne umožňujú vyvinúť efektívny a dôsledný systém ochrany pred týmito hrozbami.

Dôvera predstavuje základ medziľudských vzťahov vo svete ľudí. Avšak prílišná dôvera a neopatrnosť človeka, ktorý neuvážene poskytuje informácie druhým, predstavuje vážne bezpečnostné riziko. Také riziko má často fatálne dôsledky na život človeka samého najmä vtedy, keď ide o citlivé osobné informácie, prípadne dopad na fungovanie celej spoločnosti. Vnímajúc tieto skutočnosti prichádzame na to, že osveta v oblasti sociálneho inžinierstva v počítačovej bezpečnosti je veľmi dôležitá. Naučiť ľudí zodpovednému

a opatrnému narábaniu s informáciami vyžaduje orientáciu v danej problematike. Nie vždy si spoločnosť uvedomuje, aký závažný problém sociálne inžinierstvo predstavuje. A práve na túto tému a súvisiace otázky sme chceli v tejto diplomovej práci nájsť odpovede.

Pri písaní kvalifikačných prác sa veľakrát používa niekoľko metodických postupov. Najviac sa využívajú empirické metódy a všeobecné teoretické metódy abstrakcie, analýzy a syntézy, indukcie a dedukcie.

Pri písaní tejto diplomovej práce sme využili z *empirických metód* metódu pozorovania a experimentu. *Metóda pozorovania* pozostávala zo sledovania a porovnávania rôzneho druhu zabezpečenia informačných a komunikačných technológií v praxi. Sledovali sme niekoľko konkrétnych spoločností, akým spôsobom je detailne riešené ich informačné zabezpečenie, prípadné aké chyby sa v zabezpečení vyskytujú. Zo zistení sme sa následne inšpirovali a analyzovali možnosti náprav a vylepšení súčasnej bezpečnostnej situácie.

Ďalšou z empirických metód, ktorú sme vo vypracovaní diplomovej práce využili, bola *metóda experimentu.* Realizovali sme niekoľko experimentov v oblasti zabezpečenia informačných a komunikačných technológií. Svojím spôsobom sme sa snažili vcítiť do úlohy útočníka, a zistiť tak, akým spôsobom by implementoval škodlivý softvér, prípadne využil nedostatky v zabezpečení informačných systémov, a tým vykonal útok.

Zo skupiny všeobecných metód sme využili *abstrakciu*. Z prečítanej literatúry sme oddelili menej dôležité časti skúmaných vlastností a sústredili sa na tie záležitosti a charakteristiky, ktoré sú pre nás prvoradé, lebo nám umožnili preniknúť k podstate problému. Pomocou abstrakcie sme získali pojmy a kategórie, ktoré sú kľúčové pre naše úvahy a konštrukcie. Z množstva informácii sme tak vyčlenili istú množinu potrebných informácií, ktoré nám umožnili venovať sa podstate problému a podrobiť ich komplexnej analýze.

Následne sme aplikovali súvisiacu dvojicu metód – *analýzu* a *syntézu*. Analýzou sme rozčlenili zložitú problematiku na menšie časti, čím sme ich mohli dokonalejšie

spoznať a vniknúť do ich hĺbky. Prehĺbenejšou analýzou jednotlivých častí sa utvorili vhodné podmienky na systematické poznanie o stave problematiky.

Využitím syntézy, ktorá v porovnaní s analýzou predstavuje opačný proces, sme výsledky analýzy vhodne doplnili. Práve syntéza umožnila spojenie jednotlivých častí, ktoré sme oddelili analýzou, do jedného celku. To nám pomohlo bližšie spoznať vnútornú štruktúru skúmaných javov spolu s ich vzájomnými vzťahmi.

Ďalšia z metód, ktorú sme v diplomovej práci použili je *komparatívna metóda*. Porovnávaním rôznych situácií a vlastností sme stanovali zhodné a rozdielne znaky našich zistení. Následne *metóda analógie*, ktorá sa opiera o metódy porovnávania, pomohla vytvoriť myšlienkový postup, kde sme pri porovnávaní viacerých vlastností posudzovali ich zhodu.

Téma zabezpečenia informačných a komunikačných technológií s prihliadnutím na metódy sociálneho inžinierstva predstavuje veľmi zaujímavú oblasť. Tému sme si nezvolili náhodne, keďže ide o veľmi blízky okruh záujmu autora diplomovej práce. Úzko súvisí s jeho povolaním a pracovným zameraním, ktorému sa systematicky venuje už dlhšie obdobie. Teoretickou analýzou a syntézou poznatkov z okruhu uvedenej problematiky sa podarilo získať a systematizovať viacero nových skutočností. Práve tie predstavujú hlavný prínos diplomovej práce. Ide vskutku o zaujímavú, zodpovednú a náročnú oblasť, v rámci ktorej sociálne inžinierstvo zohráva dôležitú úlohu.

3 VÝSLEDKY PRÁCE A DISKUSIA

V časti výsledky práce sa detailne sústredíme na konkrétne metódy sociálneho inžinierstva. Praktický opis metódy umožňuje lepšie pochopiť prácu sociotechnika i jeho snahu o vylákanie dôležitých informácií a ich následné zneužitie. Každú metódu ilustrujeme prostredníctvom modelových situácií. V jednotlivých modelových situáciách krok za krokom prichádzame k detailnému opisu a skutočnostiam o tom, ako prebieha útok, jeho príprava, pohnútky (motivácia k útoku), realizácia (útoku), úskalia. V závere každej modelovej situácie navrhujeme, aké sú možnosti ochrany ľudským faktorom a tiež pomocou použitia vhodných technických (hardvérových a softvérových) prostriedkov.

3.1 Metódy phishingu

Ako sme spomínali v teoretickej časti, pod metódou phishingu rozumieme podvrhnutie falošných dokumentov, či už ide o šírenie správ prostredníctvom elektronickej pošty alebo falošných webových stránok, ktoré sa navonok tvária ako dôveryhodné dokumenty. Každý variant vyžaduje od používateľa nejaký druh interakcie, či už vyplnenie formulára, uvedenie citlivých dát vo formulári prípadne inú požadovanú aktivitu. Ak sa obeť nechá zmanipulovať a začne konať podľa predstáv útočníka, dochádza k zneužitiu dôvery, podvodnému vylákaniu a získaniu citlivých informácií, ich následnému zneužitiu a ďalším vážnym škodám.

3.1.1 Modelová situácia – podvodná registrácia

V tejto časti sa budeme zaoberať situáciou, keď sociálny inžinier nečaká pasívne na svoje obete, ale aktivizuje sa. Metóda pozostáva z vytvorenia falošnej webovej stránky – fiktívneho registračného formulára, kde navádza používateľov k registrácii. Registrácia predstavuje časovo nenáročný proces vyplnenia jednoduchého formulára, kde sa požadujú rozličné informácie o registrujúcej sa osobe. Dokončením registrácie sa úloha obete skončila. Už len samotným vyplnením registračného formulára útočník získava množstvo zaujímavých informácií o poškodenom.

Vo formulári sa zvyčajne od obete vyžaduje vyplniť meno a heslo. Používatelia vo všeobecnosti volia rovnaké meno a heslo pre využívanie viacerých prípadne všetkých služieb. A tu sa naskytne skvelá možnosť útočníka vyskúšať uvedené meno a heslo na prihlásenie do viacerých služieb. Napr. uvedením mena a priezviska v registračnom formulári si vieme odvodiť jeho skutočnú e-mailovú adresu v tvare meno.priezvisko@gmail.com aj napriek tomu, že obeť túto e-mailovú adresu neuviedla. Podľa prieskumov tento formát používa viac ako 90 % používateľov služby Gmail.

Aby útočník znásobil svoje šance na úspech a naviedol k registrácii čo najväčší počet ľudí, často motivuje obete nejakou odmenou, USB kľúčom, prípadne získaním nejakej bezplatnej služby. K samotnému odovzdaniu odmeny za registráciu však spravidla neprichádza.

V niektorých zriedkavých prípadoch sa môže reálne obdarovaniu obete aj uskutočniť. Túto výnimku však môžu predstavovať situácie, keď sa vyžaduje viacnásobná interakcia používateľa s fiktívnou stránkou, najmä ak ide o pokus o získanie informácií vo viacerých etapách. To znamená, že obdarovaním používateľa si získame jeho dôveru a on je neskôr schopný vyhovieť ešte viac premysleným požiadavkám sociálneho inžiniera. Azda najprefíkanejší spôsob je darovanie USB kľúča obeti, kde sa nachádza škodlivý kód, ktorý sa aktivuje v zariadení obete, a ktorý zhromažďuje informácie a zasiela ich priamo sociálnemu inžinierovi.

Iným ukážkovým príkladom je pokus o získanie prístupových údajov k e-mailu obete. Útok prebieha nasledovným spôsobom. Na verejných fórach a na iných verejne prístupných portáloch útočník rozšíri informáciu o zaručenom spôsobe, ako získať prístupové údaje k cudzím e-mailovým účtom. Podmienkou je uvedenie všetkých prístupových údajov o svojom účte, vrátane svojho prihlasovacieho mena a hesla. Ak obeť podľahne, útočník naplno vyhral. Má všetky údaje, ktoré potrebuje na prístup k e-mailového účtu obete. Dokonca disponuje aj ďalšími osobnými informáciami. Spolu s kompletnou e-mailovou komunikáciou, ku ktorej sa sociotechnik dostane, predstavuje pre útočníka skutočný raj a živnú pôdu pre ďalšie útoky.

Tento zaujímavý príklad názorne ukazuje črty dôverčivosti ľudskej povahy i charakterizuje spôsob, ako vyprovokovať a zneužiť nič netušiace obete.

Možnosti ochrany prostredníctvom ľudského faktora

V uvedených prípadoch zohráva azda najdôležitejšiu úlohu osveta a informovanosť používateľov. Je nevyhnutné vychovávať ľudí k maximálnej obozretnosti a opatrnosti. Vysvetliť im, že poskytnúť svoje osobné údaje bez toho, aby vedeli, akým spôsobom budú v budúcnosti použité, je veľmi nebezpečné, lebo vzniká riziko najvyššieho stupňa. Upozorniť ich na to, že prehnaná dôvera v zradných zákutiach internetových sietí, môže predstavovať snahu zmanipulovať ich za účelom poskytnutia a následnému zneužitiu ich osobných údajov.

Možnosti ochrany prostredníctvom technických prostriedkov

Oblasť ochrany pomocou týchto prostriedkov sa do značnej miery v mnohých takýchto prípadoch ukazuje ako komplikovaná. Jedným z mála možných riešení sú reštriktívne opatrenia, kde vhodnou konfiguráciou hardvérových a softvérových ochranných prostriedkov, zablokujeme prístup k určeným zdrojom možného rizika. Najjednoduchším je zablokovanie prístupu na určité webové stránky, ktoré sa svojou podvodnou podstatou snažia o zneužitie získaných údajov akýmkoľvek spôsobom.

3.1.2 Modelová situácia – podvody v elektronickom bankovníctve

Podobnou, no už omnoho pokrokovejšou a sofistikovanejšou metódou je vytvorenie fiktívnych webových stránok elektronického bankovníctva. Predstavuje dokonalé aplikovanie metódy phishingu na najcitlivejšiu oblasť obete, ktorou sú osobné financie a majetok. Pri prístupe k elektronickému bankovníctvu existuje celý rad autentifikačných nástrojov a metód, pomocou ktorých sa autentifikujeme a preukazujeme tým našu pravú totožnosť a právo prístupu. Následne je nám umožnená manipulácia s účtom, realizácie prevodných príkazov a ostatných záležitostí, ktoré sa týkajú práce s účtom.

Princíp metódy phishingu v tejto oblasti spočíva vo vytvorení falošných webových stránok elektronického bankovníctva, ktoré verne imitujú originálne stránky bankovej inštitúcie. Dizajnovo ide zvyčajne o dôkladné napodobneniny výzoru týchto stránok, ktoré sú na nerozoznanie od ich originálnych verzií. Neskúsená obeť veľmi ľahko podľahne, je totiž presvedčená, že všetko je v poriadku, a obeť tak vykonáva svoju „bežnú“ prácu s účtom. Stáva sa však obeťou dôkladnej práce neľútostného sociálneho inžiniera, ktorý neváha takto získané údaje zneužiť vo svoj prospech.

Vyplnením údajov podvodnej webovej stránky elektronického bankovníctva sa dostávame k citlivým prístupovým údajom, patria k nim: identifikačný prístupový kód a heslo zákazníka. Každá banková inštitúcia má viacero foriem zabezpečenia. Pri nižšom stupni zabezpečenia ako napríklad ochrana GRID kartou, môže falošná webová stránka navádzať k úplnému alebo čiastočnému vyplneniu kombinácií GRID karty. Ak sú údaje GRID karty spolu s prihlasovacím menom a heslom jedinými autentifikačnými údajmi, v tomto prípade útočník získava plný prístup k účtu.

V dnešnej dobe sú už k dispozícii modernejšie nástroje viacfaktorovej autentifikácie. Sociálny inžinier však postupuje trpezlivo a informácie si skladá po častiach. Aj získanie prvotných údajov, ako sú prístupové meno a heslo predstavuje pre sociotechnika úspech a vytvárajú odrazový mostík a možnosť ich využitia v ďalších fázach útoku.

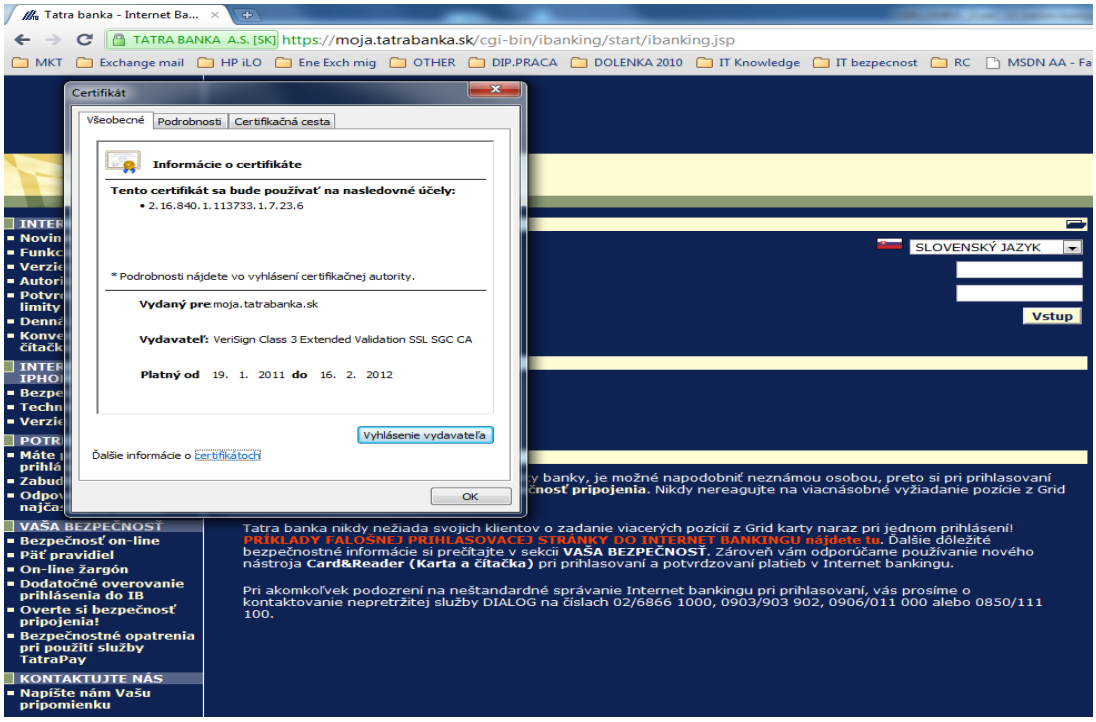
Iným príkladom aplikácie phishingu je zasielanie podvodných e-mailových správ, ktoré na prvý pohľad vzbudzujú dojem, že sú zaslané z konkrétnej bankovej inštitúcie. V nich často nachádzame požiadavky na oznámenie a zaslanie prístupových a osobných údajov. Ide však o jednoznačný podvod, lebo k informáciám sa nedostáva nik iný, iba pôvodca útoku.

V tejto oblasti sa príklady phishingu nemusia konkrétne vzťahovať iba na elektronické bankovníctvo. Veľmi často sa stretávame s aplikáciou takýchto podvodov aj v elektronickom obchode či v rámci služieb, kde používateľ musí nutne uplatniť svoju autentifikáciu, a tak sa zvyšuje aj pravdepodobnosť zneužitia takýchto údajov.

Možnosti ochrany prostredníctvom ľudského faktora

V súvislosti s veľmi citlivou oblasťou, ako sú práve súkromné financie, je v tomto smere veľmi dôležitá osveta používateľov. Mohli by sme ju zhrnúť do niekoľkých podstatných častí.

Rozpoznať základné bezpečnostné prvky stránky ako je bezpečné kryptované spojenie označované v záhlaví webovej adresy ako *https*. V súčasnosti sú všetky stránky elektronického bankovníctva zabezpečené šifrovaným pripojením SSL (Secure Socket Layer). K zabezpečenému pripojeniu prislúcha aj kvalifikovaný certifikát, ktorý vydáva niektorá z prestížnych certifikačných autorít. Na obrázku vidíme označenie zabezpečeného šifrovaného pripojenia https a kvalifikovaný certifikát vydaný prestížnou certifikačnou autoritou, v tomto prípade spoločnosťou VeriSign.



Obrázok 3-6: Zabezpečené šifrované pripojenie na internet banking

Zdroj: <Dostupné na internete: http://moja.tatrabanka.sk>, citované dňa 01.03.2011

V prípade, že niektoré z uvedených bezpečnostných prvkov chýbajú, alebo sa nám zdajú byť zmenené, odporúča sa stránku okamžite opustiť, a prípadne o tejto skutočnosti informovať banku.

Žiadna banková inštitúcia nepožaduje od používateľa oznamovanie autentifikačných a prístupových údajov spôsobom e-mailovej komunikácie. Takéto e-mailové správy sú falošné. Ich cieľom je iba zneužiť dôverčivosť obete a podvodným spôsobom od nej vylákať citlivé informácie, ktoré sociálny inžinier následne využije vo svoj prospech.

Pri prístupe cez webové stránky elektronického bankovníctva banka nikdy nepožaduje zadávanie všetkých kombinácií autentifikačných údajov naraz (napríklad kompletné vyplnenie všetkých údajov GRID karty).

Možnosti ochrany prostredníctvom technických prostriedkov

Ani v tomto prípade nie je nasadenie technických prostriedkov ochrany všemocné. Závisí od spôsobu, akým došlo k aktivácii podvodných stránok elektronického bankovníctva. Aj tu je viacero možností.

V situácii, keď je počítač používateľa nakazený nejakým škodlivým softvérom (či už ide o vírus, keylogger, trójsky koň alebo iný škodlivý kód), by riešením mohlo byť napríklad nasadenie zodpovedajúceho bezpečnostného antivírusového produktu. Ak je počítač chránený takýmto riešením, je pravdepodobné, že k tejto situácii by nikdy nedošlo. Aj ochrana pred nevyžiadanou poštou môže značne redukovať výskyt podvrhnutých e-mailových správ, ktoré sa tvária ako hodnoverné a snažia sa používateľa ovplyvniť, či už k návšteve falošných webových stránok alebo adresáta správy navádzajú zaslať citlivé osobné informácie, čísla kreditných kariet, čísla účtov, heslá a podobne.

Ak nejde o žiadnu infiltráciu a používateľ dobrovoľne inicioval otvorenie falošnej stránky, boj voči tomuto riziku vedie len cez trpezlivú a dôkladnú osvetu a vzdelávanie používateľov.

3.2 Metódy advance-fee fraud

Metóda sa vo svojej podstate snaží o oklamanie používateľa zasielaním listov, kde sú uvedené informácie, ktorými sa snažia používateľa nalákať na vysokú finančnú odmenu. Ak sa podarí obeť zmanipulovať, jediným výsledkom bude to, že príde o nemalé finančné prostriedky. S uvedenou metódou sa stretávame veľmi často, hlavne prostredníctvom šírenia nevyžiadanej pošty.

3.2.1 Modelová situácia – podvodné „Nigérijské listy“

Internetom a hlavne e-mailovou komunikačnou formou sa už dávnejšie šíria podvodné a zavádzajúce príbehy, takzvané Nigérijské listy.

Ich úlohou je predostrieť potenciálnej obeti ľútosť vzbudzujúci príbeh o nešťastnom životnom osude. Príbeh sa odohráva väčšinou v chudobných afrických krajinách, utečeneckých táboroch alebo na miestach, ktoré postihla napríklad prírodná katastrofa. Ich cieľom je apelovať na sociálne cítenie a vrodenú snahu človeka pomôcť. Iným variantom týchto listov býva závratne vysoká finančná čiastka, ktorej získanie má často motivujúci účinok na obete. Zasielanie týchto listov nie je nič iné ako kriminálna aktivita organizovaných skupín. Cieľom týchto aktivít je od obete získať čo najviac osobných údajov, bankových informácií, a tak sa pokúsiť o nelegálny zisk finančných prostriedkov od obete. V minulosti sa na distribúciu týchto podvodných listov využívali aj iné komunikačné prostriedky, napr. telefón, fax, klasická pošta.

Ako príklad jedného z mnohých uvedených listov uvádzame nasledovné:

From: Mrs. Maryann Koko.
Phone: +27-83-740-8314.
ATTN:
With much regards and good purpose of request, I write to seek for your co-operation and assistance to secure a financial deposit made by my late husband who is now late.

I am MRS Maryann Koko from Sierra Leone.My husband who is Mr. OSMOND Koko deposited as family valuables this fund in a private Security company here in Johannesburg South Africa.

However, he was the vice president of the Sierra Leone National Mining Corporation, popularly called the Diamond Corporation because of its mineral produce, which is our country's major mineral resource. During the war, with obvious reasons because he could not leave the country due to his top government position in the mining corporation, he had to shift his personal funds out of our country for safekeeping.

At that time he had to arrange for me and my children to leave the country and stay in South Africa to seek asylum pending when the civil war will be over. Unfortunately he died during the re-election which took place on 2003 through cardiac arrest.

The war has ended and there has been re-election in my country, which the former president in the name of Mr. Tijan Kabah still won for another term of office. In view of this deposit, I am soliciting for your sincere help to enable me transfer it to a foreign account of yours/company where it will be effectively utilized for investments and project in your country or any other country in overseas.

I would like to know if I could confide in you in this transaction so that we can find a way to go in more details have kept this issue very confidential because I am woman decided to look for a foreign partner because I do not trust people around me over here. I am willing to give you (25%) of the total fund and 5%for of the total fund for any expenses that will made in this Transaction and also bear in mind that this transaction is 100% risk free.

The deposited amount is (16,400,000.00 dollars) be that I am a woman with two (2) children I thought it wise to entrust this transaction with a foreigner, either individual or company account that can accommodate this fund and suggest a good investment where it could be well utilized. You can contact my son Adams koko with the above phone and fax number he will give you more information.

I look forward to your earliest response for more Details.
Best regards.
MRS.Maryann Koko

Možnosti ochrany prostredníctvom ľudského faktora

Ochrana spočíva hlavne v šírení osvety. Ľuďom je potrebné vysvetliť, že je to iba dobre premyslený podvod. V princípe je ochrana pred útokmi tohto druhu veľmi jednoduchá. Na uvedené listy a oslovenia netreba nikdy a nijakým spôsobom reagovať; predmetné správy treba ihneď zmazať.

Ak sa náhodou poškodená osoba dala akýmkoľvek spôsobom vtiahnuť do tejto špinavej hry a prípadne investovala nejaké finančné prostriedky, odporúčame, aby sa taká obeť, rozhodne obrátila na orgány činné v trestnom konaní. V žiadnom prípade sa neodporúča pokus o osobný kontakt s podvodníkmi. V prípade osobného kontaktu s podvodníkmi sa obeť môže dostať ešte do väčších problémov, v krajnom prípade do ohrozenia života.

Možnosti ochrany prostredníctvom technických prostriedkov

V súčasnej dobe existuje mnoho hardvérových a softvérových prostriedkov, ktoré tvoria účinnú ochranu proti metódam tohto typu. Tieto falošné výzvy predstavujú v podstate nevyžiadanú poštu - *spam*, ktorá vykazuje mnoho spoločných znakov, takými sú typické kľúčové slová, názov predmetu správy, oslovenia, uvedenie typických lokalít a ďalšie. Kvalitným antispamovým filtrom je možné odfiltrovať väčšinu týchto správ, aby sa vôbec nedostali k potenciálnym obetiam – používateľom. V súčasnosti disponuje kvalitným filtrom nevyžiadanej pošty veľké množstvo softvérových riešení bezpečnostnej ochrany počítača. Táto globálna ochrana predstavuje integráciu viacerých modulov ochrany – antivírová ochrana, ochrana proti spyware, osobný firewall, ochrana pred nevyžiadanou poštou a ďalšie. Či už ide o ochranu pomocou softvérových prostriedkov (antivírové programy, filtre nevyžiadanej pošty, softvérové firewally, a iné) alebo sú to riešenia tej istej ochrany pomocou hardvérových prostriedkov, ich princíp a účinnosť je rovnaká.

3.3 Metódy telefonických útokov

Útoky sociotechnikov prostredníctvom telefónnych hovorov predstavujú asi najbežnejšiu metódu pre získavanie citlivých informácií. Nespornou výhodou je relatívna anonymita volajúceho, ktorý málokedy prichádza do osobného styku s volaným. Ako sme už spomínali v teoretickej časti, najzraniteľnejšou oblasťou sú vstupné body spoločností, kde prichádza k prvému kontaktu s telefonujúcimi osobami a odovzdávaniu informácií. Takými sú najčastejšie call centrá, sekretariáty a helpdesk.

3.3.1 Modelová situácia – podvodný telefonát s obchodnou firmou

V úvodnej modelovej situácii, ktorú si vykreslíme, nejde o zložitý sociotechnický útok. Nespomenúť ho však by bola veľká škoda, keďže opis prebehne podľa skutočných udalostí, ktoré sa stali v našej spoločnosti.

Počiatočnou fázou práce sociotechnika bol zrejme zber údajov z voľných zdrojov, hlavne internetovej stránky našej spoločnosti. Sú na nej uvedené referencie spoločnosti a zoznam firiem, s ktorými naša spoločnosť úzko spolupracuje. Taktiež je na nej prístupný zoznam zamestnancov a ich zaradenie. Aj toto málo stačilo útočníkovi, aby tieto informácie náležite využil pre svoje ciele.

Úvodné telefonáty z fiktívnej spoločnosti útočníka predstavovali úplne bežnú komunikáciu s obchodným oddelením, kde sa dotyčný nezáväzne informoval o parametroch, dostupnosti a cenách nami ponúkaných tovarov. Nezabudol spomenúť niekoľko vplyvných názvov spoločností a mien, ktoré boli na zozname referencií našej spoločnosti. Tí sú vraj jeho dobrými známymi a kontaktuje nás len na základe ich odporúčaní, s cieľom zrealizovať zaujímavý obchod.

Po nejakom čase, sme ho začali vnímať ako bežného zákazníka, ktorý sa zaujíma o naše služby a z času na čas si žiada cenové ponuky. Obchodné oddelenie vždy spracovalo a zaslalo mu cenovú ponuku. Neskôr ju s nami konzultoval, prípadne si vyžiadal jej doplnenie. Väčšinou sa žiaden obchod nezrealizoval, ale predmetný objem zákazky bol vždy veľmi zaujímavý.

Až prišiel čas, keď po zaslaní ponuky prišlo zo strany útočníka k objednávke. Tvrdil, že tovar potrebuje dodať veľmi rýchlo a faktúru uhradí ešte v ten deň. Na jeho naliehanie došlo k odovzdaniu tovaru. Faktúra však nikdy nebola uhradená.

Možnosti ochrany prostredníctvom ľudského faktora

V uvedenom prípade je na mieste maximálna ostražitosť. Keď ide o peniaze, nemôžeme dôverovať nikomu. Odvolávanie sa na referencie a nám blízke mená spolupracovníkov nemusí vždy znamenať, že ide o dôveryhodnú osobu. Podozrenie by v nás mala vzbudiť aj snaha o naliehanie alebo urýchlenie konania. Pri osobách, ktoré nepoznáme, by mala byť najskôr vystavená predfaktúra. Až po jej úhrade by mal byť dodaný tovar.

Možnosti ochrany prostredníctvom technických prostriedkov

V tomto prípade neexistuje možnosť ochrany pomocou žiadnych technických prostriedkov. Je to zlyhanie ľudského faktora.

3.3.2 Modelová situácia – podvodný telefonát so súkromnou osobou

Útok sa však nemusí uskutočniť len voči komerčnému prostrediu. Veľmi zaujímavé informácie možno získať aj od súkromných osôb. Na konkrétnej modelovej situácii ilustrujeme, ako dá získať požadovaná informácia od súkromnej osoby, pričom si osoba ani neuvedomí, že sa stala obeťou útoku sociálneho inžiniera.

Rozhovor by mohol prebiehať zhruba takto:

Útočník: *Dobrý deň, dovolal som sa pani Pokornej? Tu je ... .*
Hneď vec rozoberiem, len potrebujem vedieť, či volám so správnou osobou, lebo dnes som už 3x zle zavolal.
Obeť: *Áno, pri telefóne pani Pokorná.*
Útočník: *Pani Pokorná, máte vskutku sympatické meno.*

Ale k veci. Organizujem stretávku pre môjho brata Petra zo základnej školy a mám nejaký chabý zoznam mien, podľa ktorých musím nájsť 30 ľudí. A mám na starosti ešte aj koláče, alkohol, objednávku kultúrneho domu a pozvanie jednej mŕtvej učiteľky. Som rád, že mi pomáhate.

Obeť: *Uff, máte toho moc. Ako Vám môžem pomôcť?*

Útočník: *Mohli by ste mi povedať svoje meno za slobodna? Aby som si vás odfajkol, u mužov je to totiž ľahšie. My, keď prídeme do autoservisu aspoň nám mechanik povie pravdu. (... smiech ...)*

Obeť: *(... smiech ...) Jasné, moje za slobodna bolo Lukášová.*

Útočník: *A triedna Vám bola pani Javorová? Pretože tá je už po smrti.*

Obeť: *"Nie pani Javorovú nepoznám. Naša triedna učiteľka sa volala pani Dubová, s ktorou sa doteraz stretávam.*

Útočník: *To mi nesedí, chodili ste na ZDŠ do ... v rokoch .... ?*

Obeť: *Nie, to nie som ja ... ja som ...*

V uvedenom rozhovore môžeme nájsť hneď niekoľko techník, pomocou ktorých sa útočník snaží o manipuláciu obete:

- Útočník bol veľmi komunikatívny, a tým nevzbudzoval takú mieru podozrenia ako keby zavolal niekto a sucho sa opýtal: *"Dobrý deň, ste pani Pokorná?"*.

- Útočník aspoň do istej miery vopred očakával otázky a mal pripravené adekvátne odpovede v dialógu tak, aby sa neodchyľoval od požadovaného smeru vývinu konverzácie. V prípade, že sa dialóg odchýli neočakávaným smerom, dôležitá je schopnosť improvizovať.

- Väčšina otázok nebola položená spôsobom, aby sa na ne dalo odpovedať jednoducho áno – nie, ale iba celou vetou.

- Sociotechnik vložil do rozhovoru vtip, ktorým sa snažil o uvoľnenie atmosféry. Nemusel síce obeti pripadať vtipný, ale dôležité je, že sa vtipný zdal nám a pôsobili sme uvoľnene. V takom prípade si obeť určite nepomyslí nič podozrivé.

- V rozhovore sa spomína aj mŕtva osoba, čiže ak obeť predpokladá, že ide o správne cielený hovor, určite ju táto skutočnosť vyvedie z miery a naruší jej sústredenie.

Takýto rozhovor by si mal sociotechnik dôkladne pripraviť. Niekedy stačí iba trochu dedukcie a pozorovania správania sa obete. Ak k tomu pridáme príjemné, sympatické vystupovanie a milý tón, výsledok rozhovoru a získanie požadovaných informácií bude s najväčšou pravdepodobnosťou úspešné.

Aby sme poodkryli konkrétny cieľ, ktorý sme sledovali v uvedenom rozhovore, spomenieme dôležitú skutočnosť. Od obete sme sa snažili vylákať dve hlavné informácie – priezvisko obete za slobodna a priezvisko jej triednej učiteľky. Tieto zdanlivo neškodné informácie nám môžu skvele poslúžiť pri pokuse o prístup na niektorú z webových služieb, kde zadávame pri registrácii odpoveď na otázky typu: meno vašej matky za slobodna prípadne meno vašej triednej učiteľky. Pri voľbe zabudnutého hesla je možné pomocou správnych odpovedí na tieto otázky vynulovať prístupové heslo a následne získať plný prístup k uvedenej službe.

Možnosti ochrany prostredníctvom ľudského faktora

V tomto prípade je len na konkrétnej osobe, ako sa chrániť pred spomínanými útokmi. Najlepšia rada, ktorej by sme sa mali držať, je neveriť nikomu, prípadne si volajúceho človeka dokonale preveriť. Aj keď nás volajúci ohuruje množstvom mien, poznatkov, lokalít a skutočností, ktoré sú nám známe, nemusí mať volajúci dobrý úmysel. Základom je obmedziť komunikáciu s cudzími ľuďmi na nevyhnutné minimum. Aj keď nás zahŕňa komplimentmi, vtipmi, má sympatický hlas a príjemne vystupovanie, musíme si uvedomiť, že o ňom nevieme nič a je pre nás cudzí. My od neho nechceme nič, naopak, on sa dožaduje nejakých informácií o nás. Niekedy je ťažké sa podľa týchto odporúčaní riadiť, keďže útočiaci sociotechnik je skutočný profesionál a používa tie najdokonalejšie metódy ovplyvňovania a manipulácie.

Možnosti ochrany prostredníctvom technických prostriedkov

Ochrana pomocou technických prostriedkov je v tomto prípade značne obmedzená. Ako jednu z mála možností predstavujú funkcie zobrazenia volaného čísla CLIP. Znamená to, že sa nám zobrazuje číslo volaného a máme možnosť si toto číslo overiť spätným volaním. Útočníci totiž často používajú systém oklamania signalizácie hovoru a používajú fiktívne telefónne čísla, na ktoré sa nikdy naspäť nedovoláme. Na prvý pohľad sa nám táto možnosť nemusí zdať reálna, no opak je pravdou. Úmyselná zmena telefónneho čísla volajúceho na fiktívne číslo je technicky veľmi jednoduchá.

3.3.3 Modelová situácia – podvodný telefonát s bankou

Podvodníci sa vo všeobecnosti veľmi radi sústreďujú na útoky, ktoré majú finančné pozadie a predstavujú možnosť, ako ľahko prísť k cudzím peniazom. Oblasť elektronického bankovníctva vskutku ponúka mnoho príležitostí pre sociotechnikov. Vhodným aplikovaním metód sociálneho inžinierstva a premyslenou manipuláciou obete dochádza k podvodu a nelegálnemu transferu finančných prostriedkov. Pre sociálnych inžinierov predstavuje táto oblasť v prípade neskúsených a naivných obetí doslova rajskú záhradu.

Predstavíme zložitejšiu modelovú situáciu, v ktorej je potrebné vymedziť niektoré podmienky a skutočnosti, v rámci ktorých by útok mohol prebiehať.

Postavenie obete:

- obeť využíva komunikáciu s call centrom elektronického bankovníctva príslušnej finančnej inštitúcie na vykonávanie finančných operácií na svojom účte,
- obeť pozná telefónne čísla kontaktného call centra,
- obeť dôveruje komunikácii s call centrom,
- obeť používa niektorú z nedokonalých resp. zastaraných metód autentifikácie prihlasovania sa na svoj účet a realizácii finančných operácii (napr. GRID karta).

Postavenia sociálneho inžiniera:

- útočník pozná množstvo osobnostných čŕt a správanie sa obete,
- útočník vie, že obeť na manipuláciu s účtom využíva služby call centra elektronického bankovníctva príslušnej finančnej inštitúcie a dôveruje mu,
- útočník pozná spôsob autentifikácie, akým obeť pristupuje k účtu buď formou odpozorovania jej práce alebo z iných zdrojov informácií,
- útočník je v tomto prípade reprezentovaný dvoma fyzickými osobami, z ktorých jedna komunikuje s obeťou a druhá priamo s call centrom banky.

Opis priebehu útoku:

1. fáza útoku

Keďže útočník vie, že obeť používa služby call centra príslušnej finančnej inštitúcie pre prístup na svoj účet, základy dôvery sú vybudované. Formou krátkej textovej správy zaslanej obeti ju informuje, že v krátkej dobe bude kontaktovaná pracovníkom call centra z dôvodu zisťovania nejakých dôveryhodných informácií. V odoslanej SMS správe sa nachádza aj zmenené číslo odosielateľa tak, aby sa zhodovalo s číslom príslušného call centra banky. Manipulácia čísla odoslanej SMS správy nie je pre skúseného sociálneho inžiniera problémom. Dá sa využiť aj druhý variant, a to zaslanie SMS správy, v ktorej je namiesto telefónneho čísla odosielateľa uvedený len text, napr. [Tatrabanka]. V obeti táto správa nemá dôvod vzbudzovať nedôveru. Vidí predsa korektné číslo odosielateľa, ktoré sa zhoduje s kontaktným číslom banky.

2. fáza útoku

Za krátky čas je obeť naozaj kontaktovaná, no na druhej strane linky sa už nachádza útočník. V tejto časti je na improvizácii sociálneho inžiniera ako obeť zmanipulovať tak, aby ju presvedčil na realizovanie nejakého platobného príkazu. Ako bolo spomenuté, útočníci sú dvaja – prvý komunikuje s obeťou a druhý komunikuje s call centrom banky. Útočníci majú navzájom prepojené telefónne linky tak, aby každý z nich počul, čo obeť hovorí. Následne, ak sa podarí obeť naviesť k realizácii akejkoľvek finančnej transakcii, prvá osoba z útočníkov si vypýta údaje pre realizáciu platby, ako sú: číslo cieľového účtu, suma, konštantný symbol, variabilný symbol, poznámka prípadne

ďalšie. Druhý útočník okamžite transparentne diktuje získané údaje call centru banky, iba s tým podstatným rozdielom, že číslo cieľového účtu je zmenené na číslo účtu útočníka.

3. fáza útoku

V poslednej fáze útoku po potvrdení nadiktovaných údajov o transakcii prvej osobe útočníkov sa za účelom overenia platby od obete požadujú ešte autentifikačné údaje z GRID karty alebo iného média. Po ich získaní druhá útočnícka osoba ich ihneď nadiktuje call centru banky, a tak sa celá podvodná platba zrealizuje.

Výhody a jednoduchosť realizácie útoku z pozície sociálneho inžiniera:

- Sociálny inžinier nemusí poznať žiadne prístupové údaje k účtu obete, ani ďalšie autentifikačné údaje k schváleniu samotnej finančnej transakcie. Je to obrovská výhoda, stačí ak má detailný prehľad ako prihlásenie k účtu a autentifikácia v danej aplikácii internet bankingu prebieha.

- Závisí len od schopností sociotechnika vyvinúť dostatočný psychologický nátlak, aby obeť zmanipuloval, aby útočníkovi uverila a úspech je na dosah.

Možnosti ochrany prostredníctvom ľudského faktora

Keďže v tomto prípade ide o vysoko sofistikovaný a premyslený útok, nie je jednoduché vymedziť jednoznačné možnosti ochrany. No vieme spomenúť aspoň niekoľko hlavných bodov, ktorých by sa mala pridržiavať osoba, využívajúca služby elektronického bankovníctva prostredníctvom call centra:

- Kontaktné call centrá, ktoré poskytujú asistenčné služby používateľom elektronického bankovníctva príslušnej banky, nezvyknú kontaktovať zákazníkov. Hoci sa táto možnosť nedá úplne vylúčiť, zriedkavo ku kontaktovaniu zo strany banky prísť môže.

- Ak často využívame služby call centra, určite máme uložené ich kontaktné čísla a poznáme ich. Ak nepoznáme telefónne číslo, z ktorého nás pracovník call centra práve kontaktuje, hovor by sme mali okamžite ukončiť.

- Netreba slepo dôverovať signalizácii prichádzajúceho hovoru alebo prijatej textovej správy a pamätať si, že aj v dnešnej dobe technických výdobytkov ako je napríklad už bežná služba CLIP – zobrazenie čísla volajúceho, je stále možné toto číslo zmanipulovať a pozmeniť.

- Ak nás už aj niekto z call centra kontaktuje, je možné, že od nás požaduje všeobecné informácie, ktoré sa týkajú zodpovedania nejakej ankety, prieskumu spokojnosti, prípadne nám ponúkne nejakú informáciu o službe banky, ktorá predstavuje v jej portfóliu novinku a call centrum sa snaží o nej klientov informovať. Zodpovedanie na prípadnú anketu alebo prieskum je vždy dobrovoľné a z tohto dôvodu nepodliehajme žiadnemu nátlaku. Nikdy by sme sa nemali dať zlákať na zrealizovanie finančnej transakcie, ktorú nám veľmi okato až nátlakovo navrhuje uskutočniť pracovník call centra. V tomto prípade je lepšie telefónny hovor okamžite ukončiť a dobré je o tejto skutočnosti ihneď informovať banku.

- V prípade, že je nám telefonický hovor akýmkoľvek spôsobom podozrivý, môžeme hovor ukončiť a využiť možnosť spätného zavolania na overené kontaktné čísla call centra banky. Následne si vieme overiť, či osoba, ktorá nás predtým kontaktovala, je zamestnancom banky, prípadne či ide o pracovníka povereného týmto konaním.

Možnosti ochrany prostredníctvom technických prostriedkov

Technické prostriedky vo vzťahu k prevencii, pred uvedenou realizáciou útoku tvoria nezanedbateľný potenciál možnej ochrany. Nie je ich veľa, ale mali by sme ich mať na zreteli. Často môžu predstavovať kľúčový faktor, ako útoku odolať. Uveďme si ich teda:

- Autentifikačné nástroje ako napríklad GRID karty, čítačky, USB tokeny, SecurID karty a podobne sú z hľadiska bezpečnosti kľúčovými nástrojmi, od ktorých závisí bezpečnosť celého procesu prihlásenia a realizácie platobnej transakcie v internet bankingu. Z tohto dôvodu je nesmierne dôležité používať ich najnovšiu a najbezpečnejšiu verziu. Mnohé z nástrojov sú už prekonané a z hľadiska bezpečnosti nevyhovujúce. A práve na tie sa sústreďujú a zameriavajú sociálni inžinieri v útokoch na obete.

- Je veľmi vhodné z času na čas kontaktovať banku osobne alebo telefonicky a opýtať sa na to, či nástroje, ktoré k autentifikácii používame predstavujú naozaj bezpečný spôsob ochrany. Kvalifikovaní a školení pracovníci banky nám vedia v tejto oblasti poskytnúť hodnoverné informácie, či nami používané nástroje spĺňajú všetky bezpečnostné kritéria. Ak ich nespĺňajú, nie sme chránení voči potenciálnym útokom prostredníctvom sociálneho inžinierstva, ktoré zneužívajú najmä slabé a nedokonalé formy ochrany.

3.4 Metódy reverzného sociálneho inžinierstva

V teórii spomínaná metóda reverzného sociálneho inžinierstva využíva slabiny správcov systému informačných a komunikačných technológii. Ani tí nie sú všemocní a často hľadajú odpovede na konkrétne otázky súvisiace s problémami, ktoré sa vyskytli v infraštruktúre IT ich organizácie. V spojitosti s metódami reverzného sociálneho inžinierstva, môže mať táto situácia ďalekosiahle rozmery a dopady na bezpečnosť.

3.4.1 Modelová situácia – útok reverzným sociálnym inžinierstvom

Objasnime a opíšme si 3 fázy útoku zneužitím tejto metódy:

1. *Fáza – **sabotáž***

V tejto fáze spôsobí útočník chybu v systéme infraštruktúry informačných a komunikačných technológií obete. Je veľa spôsobov, akým sa dá táto skutočnosť

docieliť. Sociotechnik na spôsobenie chyby môže použiť niektorú zo známych metód alebo ich kombináciu. Je len na ňom, či zvolí niektorú z foriem phishingu, teda rozoslania falošnej e-mailovej správy, ktorej otvorením a spustením sa prejaví spôsobenie chyby. Ak mu to okolnosti dovoľujú použije priamy prístup k technológiám obete, ak sa napríklad v jej systéme vyskytuje niektorá vážna bezpečnostná diera, ktorá nie je náležite zaplátaná.

2. *Fáza –* ***inzercia***

Chyba do technológie obete je úspešne vnesená a náležitým spôsobom sa prejavuje. Správca o nej vie, len nie je schopný ju svojimi silami odstrániť. Očakávame teda, že je zodpovedný a bude hľadať externé zdroje informácií a pomoc ako záležitosť vyriešiť. Práve teraz prichádza vhodný čas na kontaktovanie obete, kde útočník ponúka svoje vedomosti a pomoc na vyriešenie problému. To je možné docieliť viacerými spôsobmi. Jedným z nich je uverejnenie inzerátu alebo príspevku na niektorom z diskusných fór, ktoré sa zaoberajú riešením danej problematiky. Je možné aj priame oslovenie obete, či už na diskusnom fóre, sociálnej sieti, e-mailom alebo inými kanálmi. Tu do hry vstupuje psychológia a manipulácia obete, ako ho čo najvernejšie presvedčiť, že útočník je ten pravý, aby mu s problémom pomohol. Ak je aj tento krok úspešný a útočník si získa dôveru obete, nič mu nebráni vstúpiť do tretej fázy.

3. *Fáza –* ***asistencia***

Útočník v tejto fáze na jeden strane skutočne pomáha vykonať nápravu v poškodenom systéme obete, čo obeť veľmi oceňuje. Na druhej strane však útočník získava aj mnoho iných citlivých informácií z cieľového systému, prípadne autentifikačné údaje pre vstup do systému. Pri tom si vie konfiguráciou systému sprevádzkovať nejaké zadné dvierka, nainštalovať iný škodlivý kód prípadne modifikáciou konfigurácie systému umožniť neskorší neautorizovaný vstup pre úplné ovládanie systému za účelom získania pravidelného zdroja informácií. Po dokončení tejto fázy sú obidve strany spokojné. Obeť má dobrý pocit, kvázi opravený systém a útočník má pod kontrolou zdroj informácií a dôveru obete pre prípadné vykonanie budúcich útokov.

Ako vidíme, opisu útoku, predstavuje komplexnú metódu, ktorá si vyžaduje znalosť technologického zabezpečenia infraštruktúry obete, jej psychologického zmýšľania ako aj dokonalú prípravu útoku zo strany sociálneho inžiniera.

Možnosti ochrany prostredníctvom ľudského faktora

Existuje viacero odporúčaní ako predísť spomínanej situácii:

- Aj keď zlyhanie technickej infraštruktúry predstavuje závažný problém, ktorý nám spôsobuje problémy s chodom spoločnosti, čo sa informačného zabezpečenia týka, snažme sa riešiť problémy vždy s chladnou hlavou a eliminujme cudzí nátlak, naliehanie a stres. Tieto negatívne pocity skúsený sociotechnik ihneď využije vo svoj prospech a snaží sa nás zmanipulovať.

- Vo všeobecnosti nedôverovať ľuďom, ktorí sa snažia byť nápomocní pri riešení nejakého technického problému, hlavne keď ich nikto neoslovil so žiadosťou o pomoc.

- Ak už hľadáme riešenie pomocou internetových zdrojov, je dôležité si uvedomiť, aký rozsah informácií poskytneme pri opise nášho problému. Treba mať na pamäti, že poskytnuté informácie putujú internetom a ktokoľvek z návštevníkov diskusného fóra k nim má prakticky neobmedzený prístup.

- Ak sa rozhodneme pre riešenie pomocou internetových fór a diskusných skupín, voľme radšej prestížne portály, ktoré sa zaoberajú profesionálnym prístupom a pomocou pri riešení problémov v danej oblasti. Prístupy na uvedené služby sú väčšinou spoplatnené, čo odrádza len povrchných sliedičov a vyhľadávačov informácií za účelom ich neskoršieho zneužitia. Investícia do spomínanej platenej služby je veľmi výhodná.

- Pri opise problému nezverejňujeme prílišné detailné informácie o našej technológii, ktoré by umožnili prípadnému útočníkovi poskladať si z nich dokonalú mozaiku nášho riešenia a vydedukovať možné slabiny a ciele útoku. Problém sa dá vykresliť

aj jednoducho len prostredníctvom všeobecných a nie príliš detailných informácií, z ktorých sa útočník veľa nedozvie.

Možnosti ochrany prostredníctvom technických prostriedkov

Veľmi dôležitým faktorom je aj zabezpečenie pomocou adekvátnych softvérových a hardvérových prostriedkov. Medzi najdôležitejšie patrí:

- Udržiavať akékoľvek softvérové vybavenie aktualizované, čo sa týka aplikácie najčerstvejších bezpečnostných záplat a softvérových aktualizácií.

- Sledovať vývoj v oblasti bezpečnosti používaného riešenia, čo sa týka iných prevencie hrozieb, možných narušení, útokov a zneužití, ktoré nerieši ani dôkladné aplikovanie všetkých bezpečnostných aktualizácií.

- Treba mať nasadené spoľahlivé a renomované antivírové a antispyware riešenie. Je nutné overiť, či je nainštalovaná najnovšia vydaná verzia produktu, prípadne treba zvážiť zabezpečenie upgrade produktu na novšiu generáciu. Najdôležitejšie je, aby toto riešenie bolo pravidelne a včas aktualizované, čo sa týka definícií vírusových databáz a vzoriek, na základe, ktorých prebieha detekcia a dezinfekcia škodlivého kódu.

- Súčasťou tohto bezpečnostného riešenia niekedy býva aj modul antispamovej ochrany pred nevyžiadanou poštou, ktorá zabráni šíreniu rôznych podvrhnutých správ, ktorých využitie útočník často predpokladá. Antispamová ochrana nemusí byť integrovanou súčasťou, ale môže tvoriť separátny produkt. Aj tejto oblasti je potrebné venovať veľkú pozornosť.

3.5 Spôsoby ochrany pred sociálnym inžinierstvom

3.5.1 Ochrana budov strážnou službou

Hoci osobný kontakt je z pohľadu sociálneho inžiniera najmenej preferovanou alternatívou, stávajú sa aj prípady pokusov o fyzický prienik sociotechnikov do objektov spoločností. Základom ochrany proti fyzickému vniknutiu do objektu za účelom odcudzenia informácií by mala zabezpečovať strážna služba. Pri akomkoľvek incidente by mala postupovať podľa nariadení. Uvádzame niektoré podstatné postrehy, vychádzajúce zo skutočných prienikov sociotechnikov, ktoré by sa mali dodržiavať.

- Ak je to zamestnanec spoločnosti, ktorá sídli v objekte, mala by strážna služba dôsledne skontrolovať jeho preukaz, ktorý ho oprávňuje k vstupu do budovy. Ak na to nie je implementovaný automatizovaný systém, je potrebné manuálne zaznačiť jeho osobné údaje, dôvod návštevy, čas príchodu, miesto pobytu, čas odchodu, prípadne ďalšie.

- Ak ide o návštevníka, strážna služba je povinná požiadať ho o preukázanie sa dokladom totožnosti, zapísať si všetky potrebné osobné údaje, dôvod návštevy, čas príchodu, miesto pobytu, čas odchodu, prípadne ďalšie.

- Odporúčaným a veľmi často používaným prvkom ochrany je sprevádzanie návštevy v objekte až k navštívenému, prípadne privolanie navštíveného na vrátnicu, aby si návštevu sám vyzdvihol. Predíde sa tým nekontrolovanému pohybu návštevníkov po objekte.

- Každá osoba bez ohľadu na to, či je zamestnancom alebo návštevníkom, by mala mať stanovené časové rozmedzie, odkedy – dokedy sa môže pohybovať po budove. Ak ide o osobu, ktorá v danom čase nemá v objekte čo hľadať a nevie sa preukázať, treba postupovať podľa bezpečnostných smerníc. Základom by malo byť osobu odviesť a vypočuť. Ak sa odvoláva na mená a príkazy nadriadených, netreba váhať a dotyčných nadriadených kontaktovať za účelom overenia.

- To, že sa návštevník alebo zamestnanec správa prirodzene a vystupuje nanajvýš dôveryhodne ešte neznamená, že nemôže ísť o sociotechnika podnikajúceho práve pokus o prienik do stráženého objektu. Preniknutie sa často podarí aj veľmi mladým útočníkom, u ktorých už navonok mladý vek vzbudzuje podozrenie. Ráznym, prirodzeným alebo autoritatívnym vystupovaním však dokážu oklamať strážnu službu a bez akýchkoľvek prekážok im umožní vstup s následnou možnosťou krádeže informácií, ktoré sa v objekte vyskytujú v akejkoľvek forme.

3.5.2 Telefonické hovory a poskytovanie informácií

- Oslovený pracovník by nikdy nemal poskytnúť citlivé informácie, či už sú to telefónne čísla, údaje o firemnej sieti, prihlasovacie mená, heslá, prípadne akékoľvek iné bez dôkladného overenia osoby, ktorá sa poskytnutia týchto údajov dožaduje.

- Útočiaci sociotechnik sa zvyčajne snaží predstierať, že je dôveryhodná osoba, kolega z inej pobočky, pracovník kooperujúcej spoločnosti. Hlavne v prípade spoločností s veľkým počtom zamestnancov, kde sa títo navzájom nepoznajú, je nevyhnutné dôkladne si preveriť, s kým vlastne komunikujeme.

- Často sa útočník vydáva za vyššiu autoritu, alebo sa odvoláva na vyššie postavených zamestnancov. Používa pritom psychologický nátlak a vyhráža sa sankciami, ktoré obeť postihnú, ak nesplní jeho požiadavku.

- Vo všetkých prípadoch je namieste podozrievavosť a nedôvera. Je vhodné položiť si otázky: Prečo práve telefonuje mne? Kto je ten človek, ktorý sa dožaduje informácií? Ako si môžem byť istý, že je dôveryhodný a oprávnený na získanie požadovaných informácií? Ak sa včas dôkladne zamyslíme a položíme si otázky v tomto duchu, môže nám to pomôcť pochopiť celú situáciu a uvedomiť si mieru rizika, ktorú by spôsobilo naše unáhlené konanie.

- Ako minimálny ochranný prostriedok by malo slúžiť zaznamenanie mena volajúceho, jeho telefónneho čísla, číslo kancelárie alebo oddelenia a miesto odkiaľ volajúci hovor uskutočňuje. Je možné aj ukončenie hovoru a realizovanie spätného volania. Predtým je však nutné overiť si, či na danom oddelení naozaj pracuje osoba s príslušným menom a či sa jej telefónne číslo zhoduje s oficiálnym telefónnym zoznamom spoločnosti. Vo väčšine prípadov aplikovaním tejto jednoduchej taktiky sa dá overiť, či volajúci je naozaj ten, za koho sa vzdáva. Iný spôsob overenia identity volajúceho je skontaktovať sa s jeho nadriadeným a touto cestou verifikovať informáciu.

3.5.3 Heslá a kódy

- Prístup na všetky hardvérové aj softvérové zariadenia by mal byť chránený bezpečným menom a heslom. Neprípustné sú štandardné heslá, ktoré sú na zariadeniach nastavené od výroby. Sú všeobecne známe a ich zoznamy sa dajú nájsť na stránkach internetu. Uvedené heslá je nevyhnutné zmeniť. Ponechanie štandardných hesiel nepredstavuje pre skúseného sociotechnika žiadnu prekážku. V takom prípade je zariadenie zraniteľné, ako keby vôbec nebolo chránené heslom.

- Zvolené heslá musia spĺňať isté požiadavky, ktoré sa týkajú ich štruktúry a zložitosti, aby boli bezpečné. Mali by sa skladať z dostatočného počtu znakov, čísel, symbolov, veľkých a malých písmen, presne podľa toho, ako to stanovuje bezpečnostná politika firmy.

- Používanie hesiel a kódov by malo posilňovať pocit bezpečnosti a vytvárať účinnú ochrannú bariéru. Ich správa by mala byť v súlade s bezpečnostnou politikou spoločnosti, ktorá presne udáva, ako a kedy ich používať. Kódy a heslá by sa mali udržiavať v tajnosti a nevyzrádzať ich hocikomu. Inak sa vytvára len ilúzia bezpečia. Pracovníci danej spoločnosti by mali byť o týchto skutočnostiach pravidelne a dôkladne preškolení.

- Dôležitou súčasťou bezpečnosti je hlásenie podozrivých pokusov a bezpečnostných incidentov, pri ktorých dochádza k prezradeniu hesiel a kódov.

3.5.4 Telefónna ústredňa

Manipulácia sociotechnikov s telefónnymi linkami na úrovni telefónnych ústrední sa v súčasnosti už nevyužíva v takej miere ako v minulosti. Aj v tomto smere je potrebné byť vždy obozretný, čo sa týka správy firemnej ústredne a prideľovania telefónnych liniek. Dodržiavať by sa mali najmä nasledovné zásady:

- Prístup k telefónnej ústredni by mal byť pod dohľadom a možnosť zásahov do nej by mali mať len osoby na to určené a oprávnené, aby sa zabránilo manipulácii s linkami.

- Ak je telefónna ústredňa prístupná prostredníctvom siete, mal by byť prístup k nej adekvátne chránený. Medzi základné prvky by mali patriť – voľba bezpečného hesla a povolenie prístupu len z príslušných segmentov siete (napr. z povolených IP adries).

3.5.5 Nakladanie s odpadmi

Ako sme už spomínali v teoretickej časti, metódou prehľadávanie odpadu, ktorý produkujú spoločnosti, je možné nájsť veľmi cenné informácie. Z tohto hľadiska je dôležité stanoviť postupy, ako sa bude nakladať s odpadovým materiálom, ktorý môže obsahovať citlivé informácie:

- *Papierové dokumenty*, ktoré obsahujú akékoľvek citlivé informácie, by mali byť pred vyhodením skartované. Dôležitú úlohu tu zohráva aj kvalita skartovania. Pri menej kvalitných skartovacích zariadeniach je ešte možná rekonštrukcia dokumentov. Ak sa zvolia skartovacie zariadenia vyššej triedy, výsledkom skratrovania je prášok z papiera. Túto úroveň možno považovať za najbezpečnejšiu.

- *Pamäťové média typu pásky, CD-ROM, diskety, a iné* by mali byť taktiež zlikvidované v špeciálnych skartovacích prístrojoch presne na to určených. Výsledkom by mal byť odpad, z ktorého nie je nijakým spôsobom možné zrekonštruovať údaje.

- *Vonkajšie kontajnery s odpadom*, do ktorých sa sústreďuje odpad z celého objektu by v žiadnom prípade nemali byť prístupné komukoľvek, kto by prehľadávaním odpadu chcel získať nejaké informácie.

- *Taktiež upratovacia služba,* ktorá sa stará o vynášanie obsahu odpadkových košov, nesmie v nich nájsť žiadne materiály, z ktorých by sa dali získať informácie akéhokoľvek druhu.

- Znie to možno paradoxne, ale je veľmi dôležité naučiť ľudí, čo a ako vyhadzovať. Jediná cesta vedie cez vzdelávanie zamestnancov aj v tomto smere a zoznámiť ich s prípadnými rizikami, ktoré môžu nastať, ak sa nedodrží bezpečný postup likvidácie akéhokoľvek média s cennou informáciou.

3.5.6 Správa softvérového a hardvérového vybavenia počítačov

Počítače sú už najbežnejšou súčasťou práce takmer každého zamestnanca. K ich bezproblémovému fungovanie patrí správa z hľadiska hardvéru aj softvéru. Veľmi dôležitým bezpečnostným prvkom je rozhodnutie, aké programové vybavenie a v akom hardvérovom prostredí sa bude na nich prevádzkovať. Nemalo by sa zabúdať predovšetkým na tieto skutočnosti:

- Je potrebné definovať oprávnenia používateľov na počítači. Zbytočné povolenie administrátorského prístupu môže mať negatívne následky.

- Je vhodné zakázať svojvoľné inštalovanie programového vybavenia, ktoré nesúvisí s prácou zamestnanca. Inštalácia tohto softvéru môže neskôr spôsobovať veľké problémy, dokonca môže predstavovať škodlivý vplyv. Inštaláciou softvéru tohto

typu môže byť počítač vystavený útočníkovi, ktorý k nemu dokáže pristupovať na diaľku a má tak otvorenú cestu ku všetkým dokumentom. Môže tiež získať prístup ku všetkému, čo používateľ píše, najmä k prihlasovacím menám a heslám.

- Dôležitou súčasťou je prevádzka kvalitného antivírového riešenia, ktoré zabráni stiahnutiu a prípadnej inštalácii škodlivého softvéru. Antivírová kontrola by mala byť nainštalovaná tak, aby ju používateľ nemohol vypnúť, odinštalovať alebo iným jednoduchým spôsobom obísť. Tak by sa totiž otvorili dvere útočníkovi, ktorý je takýto škodlivý softvér schopný sprevádzkovať a získať nad počítačom kontrolu.

- Stáva sa, že návštevník alebo iná nepovolaná osoba získa prístup k firemnej sieti cez voľne prístupné zásuvky štruktúrovanej kabeláže. Z tohto dôvodu je veľmi dôležité, aby boli všetky voľne prístupné zásuvky, ktoré sa permanentne nepoužívajú, prípadne sú umiestnené tak, že sú voľne prístupné, boli vypnuté alebo priradené len do zóny s obmedzeným prístupom k firemnej sieti.

ZÁVER

Otázka vplyvov počítačových systémov a informatizácie spoločnosti v súvislosti s fenoménom bezpečnosti informačných a komunikačných technológií sa stala veľmi populárnou témou. Bezpečnosť v oblasti informačných a komunikačných technológií patrí určite k najdôležitejším a najrýchlejšie sa vyvíjajúcim oblastiam v informatike.

Manipulácia, ovplyvňovanie, snaha oklamať ľudí a prinútiť ich konať tak ako sám manipulátor zamýšľa, je myšlienka tak stará ako je ľudstvo samo. Spôsobujú to negatívne črty ľudskej povahy, ktoré sú známe od ranných štádií vývoja spoločnosti.

Sociálne inžinierstvo predstavuje vážnu hrozbu do budúcnosti. Umožňuje jednoduchý a pritom finančne nenáročný spôsob ako narušiť bezpečnosť inak veľmi dobre zabezpečených systémov. Sociotechnické metódy sa dajú aplikovať v širokom meradle a na najrôznejších subjektoch. Jeho metódy sa sústreďujú na najslabšie stránky ľudskej povahy ako sú napríklad: dôverčivosť, ochota pomôcť, snaha byť užitočný. To robí zo sociálneho inžinierstva naozaj nebezpečného protivníka. Sociotechnici apelujú na dobré stránky ľudskej povahy, aby ich zneužili na dosiahnutia svojho cieľa.

Zabezpečenie informačných a komunikačných technológií použitím technických prostriedkov je stále dokonalejšie. Pri neustálom zdokonaľovaní techniky sa akosi zabúda na kritický a najslabší článok v tomto reťazci – na človeka. V porovnaní s miliónovými investíciami do technologického zabezpečenia je naďalej podceňovaný ľudský faktor. Osveta a vzdelávanie ľudí by mali tvoriť základ procesu ochrany voči útočníkom. Len dôkladne informované a vyškolené osoby vedia rozoznať nebezpečenstvo, ktoré nám hrozí aplikovaním najrozličnejších metód sociálneho inžinierstva. Peniaze investované do ľudí v tomto duchu sú rozhodne návratnou investíciou.

Oblasť sociálneho inžinierstva je veľmi zaujímavou no zároveň aj obsiahlou témou. Nie je možné dopodrobna zmapovať všetky aspekty tejto témy v jednej práci. Myšlienky uvedené v tejto diplomovej práci by mali významnou mierou prispieť k minimalizovaniu dopadov sociotechnických útokov a k zvýšeniu bezpečnosti informačných a komunikačných technológií. Taktiež by táto téma mala vstúpiť do povedomia ľudí, aby

boli oboznámení a pripravení na číhajúce nástrahy, ktoré môžu mať negatívne dôsledky v rôznych oblastiach. Prínos tejto diplomovej práce predstavuje podrobné oboznámenie sa s metódami sociálneho inžinierstva a s možnosťami ako sa pred nimi chrániť.

ZOZNAM POUŽITEJ LITERATÚRY

Bibliografia:

[1] DOSEDĚL, T. 2004. *Počítačová bezpečnost a ochrana dat.* 1. Vyd. Praha : Computer Press, 2004. 190 s. ISBN: 80-251-0106-1.

[2] HARRIS, S. a kol. 2008. *Hacking – manuál hackera.* 1. vyd. Praha : Grada Publishing, 2008. 400 s. ISBN 978-80-247-1346-5.

[3] JIROVSKÝ, V. 2007. *Kybernetická kriminalita.* 1. vyd. Praha : Grada Publishing, 2007. 288 s. ISBN 978-80-247-1561-2.

[4] LONG, J. 2005. *Google HACKING.* 1. vyd. Praha : Zoner, 2005. 472 s. ISBN 80-86815-31-5.

[5] MCCLURE, S. – SCAMBRAY, J. – KUTZ, G. 2007. *Hacking bez záhad.* 1. vyd. Praha : Grada Publishing, 2007. 520 s. ISBN 978-80-247-1502-5.

[6] MITNICK, K. – SIMON, W. 2003. *Umění klamu.* 1. vyd. Gliwice : Helion, 2003. 348 s. ISBN 83-7361-210-6.

[7] PERKINS, Ch. – STREBE, M. 2003. *Firewally a proxy – servery Praktický průvodce.* Praha : Computer Press, 2003. 442 s. ISBN 80-7226-983-6.

[8] RAK, R. – KUMMER, R. 2007. *Informační hrozby v letech 2007-2017.* In: Magazín Segurity, 2007, č. 1, s. 2 – 5.

[9] SHIMOMURA, T. – MARKOFF, J. 1996. *Poľovačka na Kevina.* 1. vyd. Bratislava : Archa, 1996. 288 s. ISBN 80-7115-128-9.

[10] THOMAS, M. 2005. *Zabezpečení počítačových sítí bez předchozích znalostí.* Praha : Computer Press, 2005. 338 s. ISBN 80-251-0417-6.

[11] NORTHCUTT, S. a kol. 2005. *Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě.* Praha : Computer Press, 2005. 592 s. ISBN 80-251-0697-7.

Internetové zdroje:

[12] GRANGER, S. 2001. *Social Engineering Fundamentals, Part I: Hacker Tactics* [online]. 2001. [spracované 2011-03-22]. Dostupné na internete: <http://www.securityfocus.com/infocus/1527.html>

[13] ASHIS, T. 2010. *Social Engineering,* [online]. 2010. [spracované 2011-03-05]. Dostupné na internete: <http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf>

[14] *Social Engineering.* [online]. 2009. [spracované 2011-02-02]. Dostupné na internete: <http://www.cknow.com/cms/vtutor/social-engineering.html>

[15] *Nekradou vám náhodou identitu?* [online]. 2007. [spracované 2011-02-02]. Dostupné na internete: http://www.computerworld.cz/cw.nsf/print/CDC9ECF819BAAACCC125726A0069222E

[16] *Open source DIY hardware keylogger*. [online]. [spracované 2011-03-05]. Dostupné na internete: <http://www.keelog.com/diy.html>

[17] *Počítačová bezpečnosť.* [online]. 2011. [spracované 2011-03-22]. Dostupné na internete: <http://sk.wikipedia.org/wiki/Počítačová_bezpečnosť>

[18] ULÍK, B. *Bezpečnosť ako nikdy sa nekončiaci proces.* [online]. 2009. [spracované 2011-03-29]. Dostupné na internete: <http://www.itnews.sk/tituly/infoware/2009-10-22/c129785-bezpecnost-ako-nikdy-sa-nekonciaci-proces>

[19] *Budúcnosťou bezpečnosti je biometria.* [online]. 2003. [spracované 2011-03-29]. Dostupné na internete: <http://www.zive.sk/buducnostou-bezpecnosti-je-biometria/sc-3-a-256257/default.aspx>

[20] *Phishing.* [online]. 2011. [spracované 2011-02-08]. Dostupné na internete: <http://sk.wikipedia.org/wiki/Phishing>

[21] *Phishing a Pharming – krátke predstavenie 2.* [online]. 2007. [spracované 2011-02-15]. Dostupné na internete: <http://dennik.inet.sk/clanok/5038-phishing-a-pharming-kratke-predstavenie-2/>

[22] *"Advance Fee Fraud" Schemes.* [online]. 2010. [spracované 2011-02-15]. Dostupné na internete: http://www.sec.gov/answers/nigeria.htm