# SOCIÁLNE INŽINIERSTVO – SOCIOTECHNIKA

**Ing. Radovan Kaplan***

## ABSTRAKT

Sociálne inžinierstvo je spôsob manipulácie ľudí za účelom prevedenia určitej akcie alebo získanie určitej informácie. Termín je bežne používaný vo význame nezákonného podvodu alebo podvodného jednania za účelom získavania utajených informácií organizácie alebo prístupu do informačného systému firmy. Vo väčšine prípadov útočník neprichádza do osobného kontaktu s obeťou.

Sociálne inžinierstvo ako jednanie psychologického manipulovania bolo spopularizované známym hackerom Kevinom Mitnickom (publikované v knihe Umenie klamu). Termín bol po prvý krát spojený so spoločenskými vedami, ale jeho užívanie je teraz medzi počítačovými profesionálmi uznávaným umeleckým termínom.

**Kľúčové slová:** Sociálne inžinierstvo, ľudská stránka bezpečnosti, sociotechnik, manipulácia, umenie klamať, prevencia.

## ABSTRACT

Social engineering is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical hacking techniques; essentially a fancier, more technical way of lying. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

"Social engineering" as an act of psychological manipulation was popularized by hacker-turned-consultant Kevin Mitnick (discussed below). The term had previously been associated with the social sciences, but its usage has caught on among computer professionals and is now a recognized term of art.

**Key words:** Social engineering, manipulation, Human Element of Security, Social engineer, manipulation, Art of Illusion, prevention.

* Radovan Kaplan, Ing., QUADRIQ, a.s., Priemyselná 1, 031 01 Liptovský Mikuláš, č. mobilu +421910791278

# 1 SOCIÁLNE INŽINIERSTVO - SOCIOTECHNIKA

## 1.1 ÚVOD DO SOCIÁLNEHO INŽINIERSTVA

Človek ako taký je väčšinou najslabším článkom akejkoľvek bezpečnostnej infraštruktúry. Ľudské chyby a skutočnosť, že ľudia sa málokedy riadia presne podľa predpisov robia z ľudskej obsluhy informačných systémov veľmi lákavý cieľ. Sociálne inžinierstvo je technika zameraná na získavanie informácií pomocou presviedčania a podvádzania ľudského personálu.
Menej kvalifikovaný personál môže ľahko uveriť telefonátu z „technického oddelenia" so žiadosťou o prezradenie hesla, nutného na odstráneniu nejakej závady. Aj technicky kvalifikovaný zamestnanec iste rád poskytne technické údaje o vnútornej sieti organizácie novému „kolegovi", ktorý dostal od neobľúbeného riadiaceho pracovníka ťažkú úlohu s krátkym časovým termínom. Možností, ako podvodom získať požadované informácie je veľa a väčšinou jediné potrebné zariadenie na „útok" je telefón.

Obranou proti týmto útokom je dostatočné školenie personálu a vybudovanie prirodzených a bezpečných pravidiel spolupráce rôzneho personálu.

### Achilova päta bezpečnostných systémov

Najuznávanejší vedec 20, storočia, ***Albert Einstein,*** *vraj povedal:* ***„Iba dve veci sú nekonečné: vesmír a ľudská hlúposť. Avšak tým prvým si nie som istý."***

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

**Čo je teda sociálne inžinierstvo?**

Sociálne inžinierstvo sú systematicky používané vedomosti ľudského chovania a umenia presviedčať, aby užívateľ urobil to, čo by za normálnych okolností, pri dodržiavaní všetkých bezpečnostných pravidiel, nikdy neurobil. Tým sú samotným ľudským faktorom prelomené technologické a organizačné bezpečnostné opatrenia a je umožnený kybernetický útok.
Sociálne inžinierstvo je metóda získavania dôverných informácií pomocou manipulácie oprávnených užívateľov. Sociotechnik väčšinou používa telefón alebo internet na oklamanie (podvedenie) ľudí, aby odhalil tajné informácie. Sociálni inžinieri využívajú prirodzenú tendenciu jednotlivca veriť im, pred využívaním dier v počítačových systémoch. Spravidla to súhlasí s názorom, že „užívatelia sú najslabším článkom" v zabezpečení a toto je podstata toho, prečo je sociálne inžinierstvo uskutočniteľné.

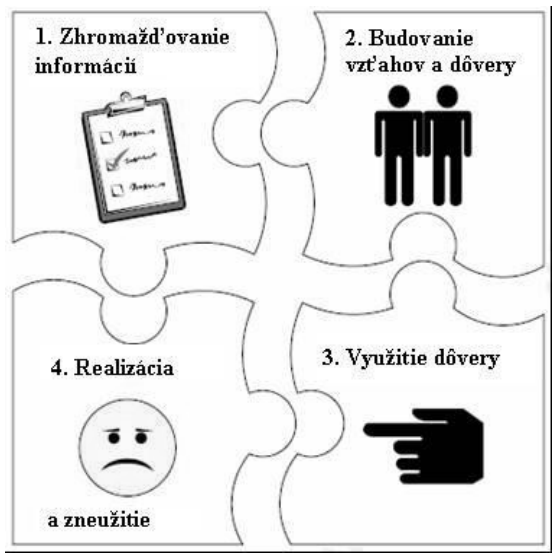
## 1.2 METÓDY KLAMU

Aby prekonal zabezpečenie, musí útočník, votrelec alebo sociotechnik nájsť metódu na oklamanie dôveryhodného pracovníka tak, aby prezradil nejakú informáciu, trik

alebo zdanlivo nedôležité nápovede, ktoré by mu umožnili dostať sa do systému. Pokiaľ sa dajú pracovníci oklamať, alebo sa dá s mini manipulovať, aby prezradili dôverné informácie, alebo keď ich činnosť spôsobuje vznik dier v zabezpečení, ktoré umožnia útočníkovi prístup do systému, potom neexistuje žiadna technológia, ktorá by mohla firmu ochrániť.

**Zneužitie dôvery**

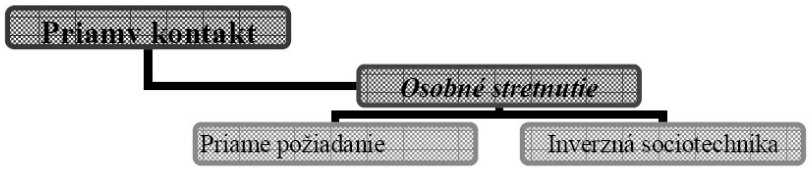
Vo väčšine prípadov majú sociotechnici veľké schopnosti pôsobiť na ľudí. Vedia byť okúzľujúci, zdvorilí. Je ľahké si ich obľúbiť – to sú vlastnosti potrebné k tomu, aby si získali porozumenie a dôveru iných. Skúsený sociotechnik, ktorý používa stratégiu a taktiku patriacu k jeho remeslu, je schopný získať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




*Obrázok 1 Sociotechnický cyklus*

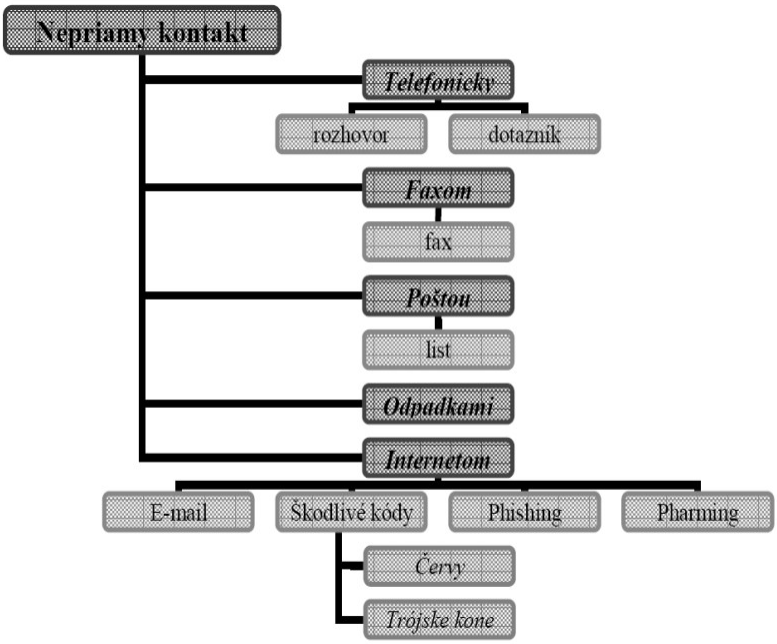
## 1.3 METÓDY ÚTOKOV SOCIÁLNEHO INŽINIERSTVA

**Mäkké** metódy vychádzajú z ľudskej dôverčivosti a ochoty pomôcť. Ide najmä o zneužitie nič netušiaceho pracovníka a to formou mailu, telefónu, listu alebo aj osobne.
**Tvrdé metódy** využívajú ľudskú slabosť ako je úplatnosť, citové lability, vydierateľnosť, frustrácia z práce, pomstychtivosť, škodoradosť alebo závisť. V tejto skupine sociotechnik využíva vydieranie, poskytnutie sa ako nástroj pomsty alebo nadviazanie intímneho vzťahu s užívateľom.
**Priamy kontakt** je využívaný pri osobnom stretnutí sociotechnika s obeťou či už pri jeho priamom požiadaní o potrebné informácie, alebo pri inverznom, tiež pomenovanom aj obrátenom sociálnom inžinierstve, kedy sociotechnik umelo vyvolá problém a čaká, pokiaľ ho poverená osoba/obeť požiada, aby eliminoval tento nežiaduci jav.




*Obrázok 2 Schéma delenia priamych kontaktov*

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




*Obrázok 3 Schéma delenia nepriamych kontaktov*

## PHISHING

Phishing je podvodná technika používaná na Internete k získavaniu citlivých údajov ( hesla, čísla kreditných kariet apod.) od obetí útoku. Princípom je rozosielanie e-mailových správ, ktoré sa tvária ako oficiálne žiadosti banky alebo inej podobnej inštitúcie a vyzývajú adresáta k zadaniu jeho údajov na odkazovanú stránku. Táto stránka môže napríklad napodobniť prihlasovacie okno internetového bankovníctva a používateľ do formulára na stránke zadá svoje prihlasovacie meno a heslo. Týmto tieto údaje prezradí útočníkom, ktorí sú potom schopní mu z účtu vykradnúť peniaze.


*Obrázok 4 Príklad podvodnej internetovej stránky*

## IVR ALEBO TELEFÓNNY PHISHING

Táto technika využíva falošný hlasový automat (IVR) s podobnou štruktúrou ako má originálny bankový automat ("Pre zmenu hesla stlačte 1, pre spojenie s bankovým poradcom stlačte 2"). Obeť je väčšinou vyzvaná e-mailom k zavolaniu do banky za účelom overenia si informácie. Následne je potom požadované prihlásenie s pomocou PIN čísla alebo hesla. Niektoré automaty následne prenesú obeť do kontaktu s útočníkom vystupujúcim v roli telefónneho bankového poradcu, čo mu umožňuje ďalšie možnosti otázok.

## BAITING

Baiting môže byť považovaný za trojského koňa v reálnom svete.

Pri tomto spôsobu útoku útočník nechá infikované CD, USB kľúč alebo iné pamäťové médium na mieste, kde ho obeť s veľkou pravdepodobnosťou nájde, napríklad v kúpeľni, vo výťahu, na parkovisku. Potom nechá pracovať zvedavosť, s ktorou obeť skôr či neskôr vloží toto médium do svojho počítača. Tým dôjde k inštalácii víru, za pomocou ktorého získa útočník prístup k počítaču alebo celej firemnej počítačovej sieti.

## QUID PRO QUO ALEBO NIEČO ZA NIEČO

Niečo za niečo znamená náhodné vytáčania čísel spoločnosti a predstavenia sa ako pracovník technickej podpory. Existuje šanca, že útočník nájde nespokojného zamestnanca s problémom, ktorému sa pokúsi po telefóne pomôcť. Na oplátku požiada obeť o inštaláciu infikovaného programu alebo zvolenú akciu vo firemnom informačnom systéme.

## 1.4 PREVENCIA

- Školenie
  Prvým a najdôležitejším krokom pri školení je upovedomenie každého člena organizácie, že existujú ľudia bez zábran, ktorí sa budú pokúšať manipulovať nimi pomocou podvodov a psychologických metód. Pracovníci musia vedieť, ktoré informácie treba chrániť a ako.
  Ako náhle pochopia, ako môžu byť zmanipulovaní, budú schopní dostatočne včas útok rozoznať.
- Overenie totožnosti osoby, ktorá o niečo žiada, či je naozaj tým za koho sa vydáva.
- Overenie, či je osoba oprávnená získať požadované informácie a či ich skutočne potrebuje.
- Bezpečnostné praktiky spojené s heslami umožňujúcimi prístup k počítaču a hlasovej pošte.
- Postup poskytovania dôverných informácií alebo materiálov.
- Spôsob používania elektronickej pošty vrátane prostriedkov chrániacich pred
- nebezpečnými programami: vírusmi, trójskymi koňmi a podobne.
- Fyzické bezpečnostné požiadavky, ako povinnosť nosenia identifikátoru (visačiek).
- Povinnosť zadržiavať tie osoby na pôde firmy, ktoré nemajú visačku.
- Zásady spojené s používaním hlasovej pošty.
- Klasifikácia informácií a prostriedky jej ochrany.
- Vhodné spôsoby odstraňovania dôverných dokumentov a dátových nosičov, ktoré obsahujú dôverné materiály alebo ich obsahovali v minulosti.

## LITERATÚRA

[1] MITNICK, K.: Umění klamu. Helion S.A., 2003.
[2] EDMÜLLER, A; WILHELM, T: 27 manipultívních technik, Grada 2010.
[3] TOMÁŠEK, J.: Úvod do kriminologie, Grada 2010.
[4] FRYŠAR, M. a kolektiv: Bezpečnost pro manažéry, podnikatele a politiky, Public History a ČABM 2006.

článok recenzoval:
doc. Ing. Zdeněk Dvořák, PhD.