# Sociální inženýrství

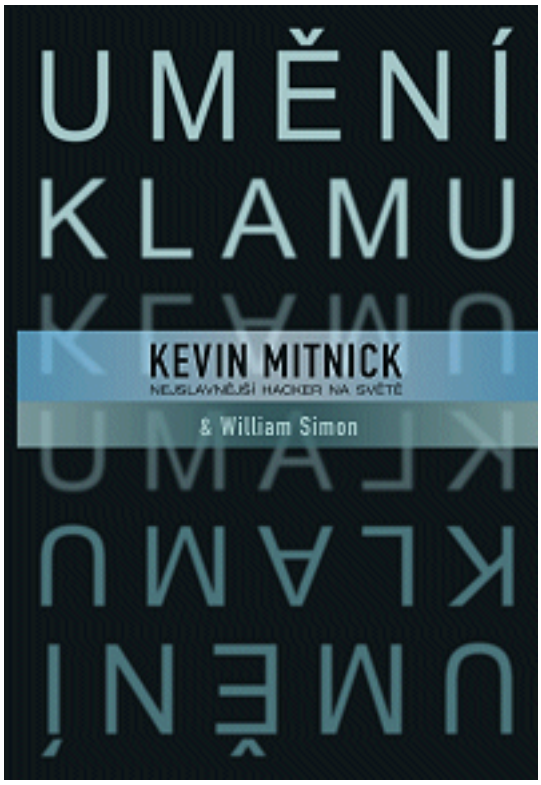
Vložil/a cm3l1k1 [1], 25 Listopad, 2004 - 19:15

- Hacking [2]
- Hacking method [3]
- Security [4]

V tomto článku popíšu jak sociotechnici využívají socialního inženýrství k vniknutí do systémů, přístupu k tajným informacím apod.

Předem bych chtěl napsat pár slov ke knize ze které jsem čerpal informace...

Dne **25.9.2003 přijel Kevin Mitnick do Prahy** na autogramiádu své knihy Umění klamu, která se konala v Domě Knih na Václavském náměstí. Fronta před knihkupectvím byla opravdu nevýdaná a k mému nepochopení jako první tam stála babička, které mohlo být asi tak 60, s knížkou od Mitnicka v ruce a plným úsměvem na tváři. I když byla autogramiáda plánovaná na 16:00, tak začala v 17:00 což zrovna nepotěší. A jak je v Praze zvykem neobešlo se to ani bez místních bezdomovců, které velice zajímalo co se rozdává zadarmo, když je tady taková fronta. Zřejmě nepochopily můj smysl pro humor když jsem jim řekl, že za 300Kč dostanou maximálně podpis.
Nyní již k samotné knize...




**Název:** Umění klamu
**Titul originálu:** The Art of Deception. Controling the Human Element of Security
**Autor:** Kevin D. Mitnick & William L. Simon
**Vazba:** tvrdá s přebalem
**Formát:** A5
**Počet stran:** 348
**Maloobchodní cena:** 299 Kč
**ISBN: 83-7361-210-6**

Kniha byla vydaná polským nakladatelstvím HELION S.A. (http://www.helion.pl [5]) a „nejslavnější hacker na světě“ Kevin Mitnick v ní popisuje, jak lze jednoduše manipulovat s lidmi. Teď trochu odbočím… Kevin Mitnick není všeobecně uznáván jako hacker, ale jako výborný sociotechnik, který se právě díky sociálnímu inženýrství dokázal dostat téměř do každého systému. V knize je na toto téma spousta ukázkových příběhů, které čtenářům lépe přiblíží oč vlastně jde a na co si dát pozor. Metody které sociotechnici používají, aby si získali naši důvěru jsou opravdu všelijaké. Lidé řeknou svá hesla jakoby nic, ale nejde tu jen o hesla, ale spoustu jiných na první pohled nedůležitých informací, které sociotechnici dále použijí pro úspěšný průnik. Firemní bezpečnostní politika by určitě neměla opomenout možnost sociotechnických útoků a zavést školení svých pracovníků. Tato kniha bude určitě dobrým rádcem např. manažerům bezpečnosti při vytváření takové politiky.

## Sociotechnika

= přesvědčování a ovlivňování lidí s cílem oklamat je tak, aby uvěřili že jste někdo jiný a zmanipulovat je k vyzrazení některých informací nebo provedení určitých úkonů.

Já jsem si během četby této knihy zapisoval poznámky, které by měli shrnout metody ovlivňování lidí popsaných v knize. Takže v bodech…

## Sociotechnikem krok za krokem

- nejdůležitější pro sociotechnika je, aby získal před útokem co nejvíce dostupných informací:
+ o struktuře firmy
+ jména pracovníků a šéfů firmy
+ používaný žargon

- pokud chce sociotechnik někoho zmanipulovat, tak ideálním terčem je firemní nováček. Sociotechnik mu zavolá, pěkně ho přivítá v "jejich“ firmě a začne např. s bezpečným nastavením hesla a připojením k síti. Nováček nadšený tím, že se o něj tak pěkně starají by pro něj udělal skoro cokoliv.

- aby si získal důvěru, tak se ve většině případů vydává za pracovníka stejné firmy, ale např. v jiné pobočce (kdo by nepomohl kolegovi, že?)

- sociotechnici se ptají na, na první pohled nezajímavé, nedůležité informace, které nedávají žádný smysl, ale pak je postupně poskládají dohromady a pokusí se o úspěšný útok.

- praktický příklad: firma má 1 000 zaměstnanců, sociotechnik pošle všem email, ve kterém bude stát, že prvních 500 lidí, kteří se zaregistrujou dostanou např. zdarma vstupenku do kina. Součástí formuláře bude aby si uživatel zvolil heslo a protože si spousta lidí dává všude stejné heslo, tak se určitě nějaký maník chytí a zadá si stejné jako při logování na firemní server. Sociotechnik odzkouší zadaná hesla a…

- dalším z tahů k oklamání lidí je získat si jejich důvěru (např. Dobrý den, já jsem Petr z oddělení xxx pracuju s Filipem a Honzou, znáte Honzu? Říkal mi, že se mu moc líbíte ;) oběť (dívka) věří útočníkovi, že zná jejího kamaráda Honzu, který mu říká i věci z jeho soukromého života, takže mu bude "plně" důvěřovat.

- ovlivňování lidí pomocí autority: Pokud například sociotechnik na oběť naléhá, že je to pro jejího šéfa a už to dávno mělo být hotové (např. výpis čísel nových kreditních karet atp.), tak chudák sekretářka ze strachu udělá co řekne.

- další ne moc používanou, za to velice účinnou metodou je trashing (prolézání firemních odpadů, za účelem nalezení dokumentů o struktuře sítě, jmen pracovníku, hesel atp.)

- pokud si sociotechnik vybírá oběť, tak buď nováčka, nebo níže postaveného pracovníka… V jednom

z příběhů sociotechnik výborně využil i pracovníka ostrahy.

- pokud sociotechnik naléhá na důležitost daného úkonu, nebo na časovou tíseň, tak se oběť nezamyslí ani nad důsledky daného úkonu a spíš bude útok úspěšný.

- už jen poznámku: pokud oběť dělá v malé firmě kde se všichni znají, tak je malá naděje, že sociotechnik uspěje.

Sociologie ve svém (50-ti letém) výzkumu ukazuje šest „základních vlastností lidské povahy“, které se projevují při pokusu podřídit někoho vůli sociotechnika.
**1) Autorita** – jak jsem již psal, lidé mají tendenci se podřídit osobě s vetší funkcí (mocí)
**2) Sympatie** – sociotechnik může získat sympatie oběti několika způsoby: stejné názory, zájmy, sport atd.
**3) Vzájemnost** – je mnohem větší pravděpodobnost, že sociotechnikům oběť vyhoví když pro ní předtím něco udělají. Například vyřeší problém se sítí a pak řeknou ať si nainstaluje program, který bude síť hlídat což přitom může být trojan, keyscan atp.
**4) Důslednost** – lidé mají tendenci se podřídit, jestliže předtím veřejně vyhlásili svou podporu a angažovanost v určité záležitosti.
**5) Společenský souhlas** – sociotechnik zavolá a zeptá se zda-li nemá oběť čas, že by potřeboval vyplnit dotazník, který už všichni ostatní s ním vyplnili. Když to přece udělali ostatní proč ne já, že? Pak už záleží jen na sociotechnikovy co vybere za otázky ;)
**6) Vzácná příležitost** – viz. posílání mailů. Prvních 500 lidí dostane lístek! Zaregistrujte se!

## Závěrem

Kniha je to opravdu zajímavá, poučná a věcná. Sice je plná zajímavých příběhů, ale ty se časem začnou „opakovat“ a pár stránek prospíte, vynahradí to však shrnutí metod a téma obrany proti těmto útokům, které se dočtete v posledních kapitolách. I když nejsem zrovna velkým fanouškem Kevina Mitnicka, tak bych tuto knihu určitě doporučil všem lidem zajímajícím se o bezpečnost.

**URL článku:**
https://security-portal.cz/clanky/soci%C3%A1ln%C3%AD-in%C5%BEen%C3%BDrstv%C3%AD

**Odkazy:**
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/hacking-method
[4] https://security-portal.cz/category/tagy/security
[5] http://www.helion.pl