

## 10 Sociální inženýrství

### Obsah hodiny



V této hodině se budeme zabývat ohrožením počítače prostřednictvím sociálního inženýrství a možnostmi ochrany

### Cíl hodiny



Po prostudování budete schopni:

- Vysvětlit jakou hrozbou pro bezpečnost je sociální inženýrství
- Orientovat se v různých sociometodách
- Objasnit možnosti snížení rizika ohrožení pc ze strany člověka

### Klíčová slova



Sociální inženýrství, sociotechnicky, Baiting, Trashing, Phishing, Pharming

Sebelepší bezpečnostní technologie nebudou k ničemu, když nebudeme při zabezpečení počítače brát do úvahy lidský faktor. Největším bezpečnostním rizikem je totiž člověk.

Útočník, který chce napadnout počítač, si musí najít nějakou cestu k němu. Pokud použijeme různé bezpečnostní technologie, bude si hledat informace, které mu umožní přístup do systému, jiným způsobem. Bude se je snažit podvodně vylákat. Existuje celá řada triků a technik, jak toho docílit, jejich zkoumáním se zabývá sociální inženýrství.

### 10.1 Sociální inženýrství

Zabývá se tím, jak podvodně od uživatele získat data umožňující přístup k počítači. Základem je ovlivňování, přesvědčování, manipulace lidí s cílem oklamat je tak, aby uvěřil.

Vychází z klasických podvodů v reálném světě. Cílem všech technik, které sociální inženýrství používá, je vytvořit v člověku nějakým způsobem dojem, že situace je jiná, než ve skutečnosti je:

- člověk nepozná, že mu telefonuje nebo e-mailuje nebo ho jinak oslovuje podvodník,

- na základě některých uměle vytvořených indicií se domnívá, že komunikuje s někým úplně jiným, důvěryhodným.

Je dnou z forem takových to podvodů jsou i jsou webové stránky, na které odkazuje spam (nevyžádané zprávy) nebo se nacházejí na "šedé" zóně Internetu (stránky s tematikou warezu<sup>1</sup>). Přesvědčují uživatele k nainstalování antiviru, kodeku, ke stažení žhavého videa s nějakou nahou celebritou apod. Ve skutečnosti se tak do PC dostane jen další havěť nebo falešné bezpečnostní produkty, které vytváří falešné poplachy<sup>2</sup>, PC označí za infikované bez ohledu na reálnou situaci. Zároveň nabízejí řešení takového neexistujícího problému zakoupením "plné" verze.

Útočníci, kteří se snaží uvedenými způsoby podvést uživatele, využívají různé triky a úskoky.

**Stres** – člověk pod tlakem reaguje jinak než člověk v pohodě, který má čas nad věcmi přemýšlet. Zvláště ve velké firmě platí, že ne každý zná každého. Když zazvoní telefon, že je potřeba něco udělat nebo sdělit nějakou informaci, aby se zabránilo velkému průšvihy (ztráta významného zákazníka apod.), málokdo asi zaváhá.

**Nebezpečí** – nejčastěji je používaná metoda „Vaší peněženice hrozí nebezpečí. Když nechcete, nic nedělejte. Ale kdybyste se přece jen rozhodli něco udělat...”

**Vydávání se za někoho/něco známého** – opravdu je osoba v e-mailu nebo na telefonu skutečně tím, za koho se vydává? Zvláště v armádě se hierarchie hodností dodržuje více než důsledně. Ale i v civilu platí, že když zavolá nová asistentka generálního ředitele, asi jen největší odvážlivec by jí odmítl sdělit požadovanou informace. Přitom třeba v kybernetickém světě není nic jednoduššího, než si změnit identitu.

**Důvěryhodná činnost** – útoky není potřeba provádět pouze vzdáleně. Člověk s brašnou a v montérkách propluje hlavně do objektu velké firmy zpravidla bez větších potíží. A když se předtím ještě třeba telefonicky objednal, má zpravidla dveře otevřené prakticky všude...

**Lákavá činnost** – lidé většinou nejsou složitými osobnostmi, alespoň ne v základních potřebách. A tak není divu, že mnohdy podlehnou možnosti např. podívat se na soubor s lechtivým obsahem, za který se vydává e-mailový červ.

---

<sup>1</sup> nelegální software, slangové označení SW, se kterým je nakládáno nelegálně, v rozporu s autorským právem. Podle druhu bývá někdy warez rozdělován na *gamez* (počítačové hry), *appz* (aplikace), *crackz*(cracky) a také *moviez* (filmy).

<sup>2</sup> Na adrese [www.spywarewarrior.com](http://www.spywarewarrior.com) lze najít seznam falešných (rogue/suspect) antispyware programů.

**Zvědavost – možnost odhalit tajemství** – na chodbě firmy leží CD a na něm nápis „Mzdy třetí kvartál“. Dříve či později ho někdo zvedne a je velká pravděpodobnost (skoro až jistota), že i vloží do počítače. Zvědavost vítězí. Spustí program a zároveň s tím si nevědomky nainstaluje do počítače nějaký nástroj pro útočníka.

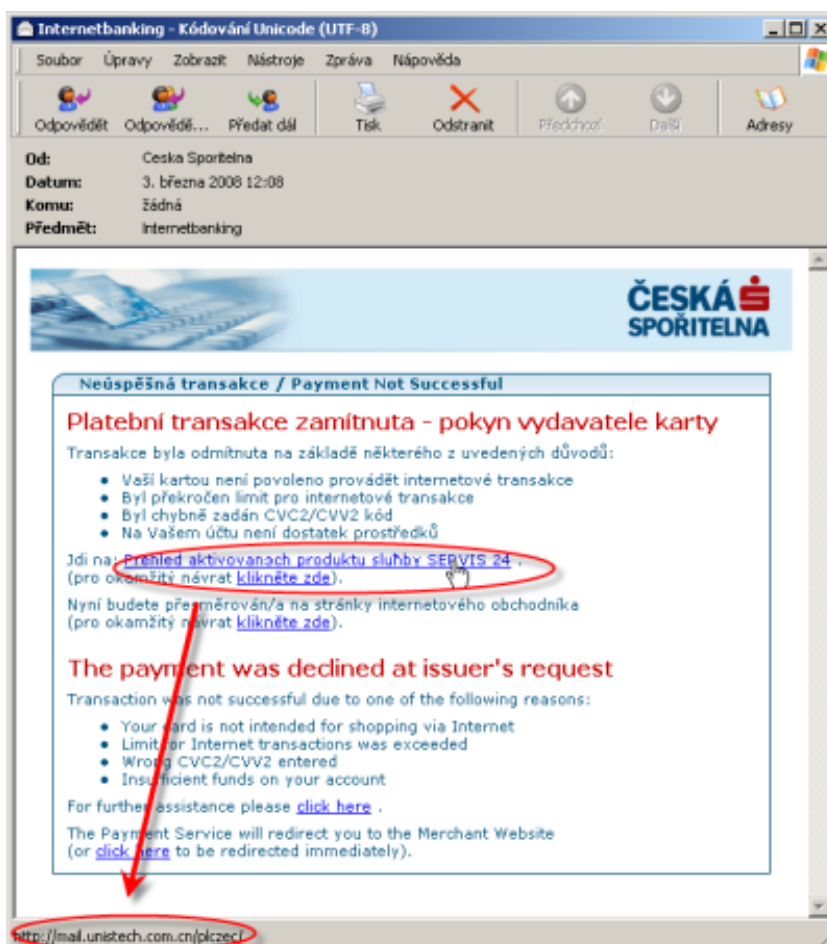
## 10.2 Některé sociotechniky

### Baiting

Útočník nechá infikované CD, flashdisk nebo jiné paměťové médium na místě, kde jej oběť s velkou pravděpodobností nalezne a ze zvědavosti vloží toto médium do svého počítače.

### Phishing

Podstatou je zaslání falešného e-mailu, který na první pohled vypadá jako důvěryhodná zpráva. Na místě odesílatele je uvedena například uživatelská banka, [administrator@inetbanka.com](mailto:administrator@inetbanka.com).



Obrázek 10-1: Rok 2008: cílem phishingu se stali zákazníci České Spořitelny.

V textu e-mailové zprávy se pak nic netušící oběť dočte, že se vyskytly problémy s jeho přihlašovacím heslem, a musí proto vyplnit speciálně pro tento účel vytvořený WWW formulář.

Design, grafika, údaje, text a další informace na stránce s tímto formulářem přesně odpovídají zvykům dané banky.

### **Pharming**

Princip: napadení DNS a přepsání IP adresy, což způsobí přesměrování klienta na falešné stránky InternetBankingu po napsání URL banky do prohlížeče.

Tyto stránky jsou obvykle k nerozeznání od skutečných stránek banky. Ani zkušení uživatelé nemusejí poznat rozdíl.

### **Trashing**

Vybírání košů s cílem najít důležité informace

## **10.3 Jak minimalizovat riziko ohrožení**

Chráníme nejen vlastní počítač, ale i fyzický přístup k němu.

- Zajištění přístupu do budovy, k serveru.
- Prověření zaměstnanců (včetně úklidových pracovníků).

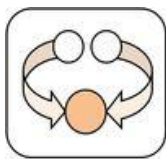
Měly by existovat zásady bezpečnosti a všichni zaměstnanci by s nimi měli být seznámeni, proškoleni. Nestačí pak jen důkladně proškolit zaměstnance, uživatele, aby si byli vědomi všech bezpečnostních rizik, ale je nutné kontrolovat dodržování bezpečnostních pravidel. Důležitá je kvalifikace a odborná způsobilost IT pracovníků.

- Proškolení zaměstnanců.
- Bezpečnostní kontroly.
- Zvyšování kvalifikace a odborné způsobilosti pracovníků. IT.

V rámci bezpečnostních pravidel by mělo být definováno, jakým způsobem se budou bezpečně likvidovat nejen dokumenty (skartace), ale rovněž datové nosiče.

- Pravidla pro archivaci a skartaci dokumentů
- Způsob likvidace odpadu (dokumenty, nosiče dat, ...).

## Shrnutí kapitoly



Sociální inženýrství se zabývá tím, jak podvodně od uživatele získat data umožňující přístup k počítači. Vychází z klasických podvodů v reálném světě. Cílem všech technik, které sociální inženýrství používá, je vytvořit v člověku nějakým způsobem dojem, že situace je jiná, než ve skutečnosti je

Základem je ovlivňování, přesvědčování, manipulace lidí s cílem oklamat je tak, aby uvěřil.

Některé sociotechniky:

- Baiting
- Trashing
- Phishing
- Pharming

Riziko ohrožení lze minimalizovat ochranou počítače a přístupu k němu, vytvořením zásad bezpečnosti (včetně zásad bezpečné likvidace dokumentů, a datových nosičů), proškolením zaměstnanců, bezpečnostními kontrolami.

## Kontrolní otázky a úkoly



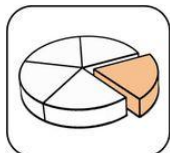
- 1) Čím se zabývá sociální inženýrství?
- 2) Uveďte příklady metod sociálního inženýrství.
- 3) Jaká opatření ve firmě vedou ke snížení rizika ohrožení?

## Otázky k zamyšlení



- 1) Co zneužívají útočníci k oklamání uživatele?

## Použitá literatura a jiné zdroje:



- [1] PŘIBYL, Tomáš. Sociální inženýrství z pohledu útočníka. ICT Security [online]. 08.09. 2009, x, [cit. 2011-11-20]. Dostupný z WWW: <<http://www.ictsecurity.cz/odborne-clanky/socialni-inzenyrstvi-z-pohledu-utocnika.html>>.
- [2] Sociální inženýrství aneb nenechte se oblbnout!. www.viry.cz [online]. [cit. 2011-11-20]. Dostupné z WWW: <<http://www.viry.cz/go.php?p=spyware&t=clanek&id=48>>.

- [3] Sociální inženýrství (bezpečnost). In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-11-20]. Dostupné z WWW:  
<[http://cs.wikipedia.org/wiki/Sociální\\_inženýrství\\_\(bezpečnost\)](http://cs.wikipedia.org/wiki/Sociální_inženýrství_(bezpečnost))>.