SOCIÁLNÍ INŽENÝRSTVÍ

Social engineering

Jan Horníček

Bakalářská práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2008/2009

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan HORNÍČEK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Sociotechnika a metody sociálního inženýrství**

Zásady pro vypracování:

1. **Sociotechnika a metody sociálního inženýrství.**
2. **Bezpečnostní prostředí a počítačový útok v sociálním inženýrství.**
3. **Klasifikace informací v bezpečnostním prostředí.**
4. **Anketa pro oblast sociálního inženýrství.**
5. **Vyhodnocení ankety pro oblast sociálního inženýrství.**
6. **Návrh opatření na zlepšení podmínek bezpečnostního prostředí v sociotechnice.**

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **MITNICK, Kevin, SIMON, Wiliam. The Art of Deception: Controlling the Human Element of Security; HELION S.A., 2003. 348 s. ISBN 83-7361-210-6.**
2. **MITNICK, Kevin, SIMON, Wiliam. The Art of Intrusion, Wiley; 2005. 270s, ISBN 978-0764569593**
3. **MITNICK, Kevin -- Simon, William: Historie Kevina (Missing Chapter).ON LINE**
4. **SECURITY WORLD 4/2008, IDG CZECH, a.s. ISSN 1214-794X**
5. **SECURITY WORLD 4/2007, IDG CZECH, a.s. ISSN 1214-794X**
6. **SECURITY WORLD 2/2005, IDG CZECH, a.s. ISSN 1214-794X**

Vedoucí bakalářské práce: **Ing. Jaroslava Gregušová**
Ústav elektrotechniky a měření

Datum zadání bakalářské práce: **20. února 2009**

Termín odevzdání bakalářské práce: **20. května 2009**

Ve Zlíně dne 20. února 2009

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato práce čtenáře zavede do světa sociálního inženýrství a počítačové kriminality. Hlavní částí práce bude problematika sociálního inženýrství, počítačového útoku na nejslabší článek všech bezpečnostních systémů – člověka. Dále popsání nejdůležitějších částí útoku a praktik sociálního inženýrství. V závěru práce uvedu jméno Kevina Mitnicka – praktika sociotechniky.

Motto této práce:

“Pouze dvě věci jsou nekonečné: vesmír a lidská hloupost. Ačkoli tím prvním si nejsem jist.” ***Albert Einstein***

Klíčová slova: Phishing, vishing, pharming, trashing, sociální inženýrství

ABSTRACT

This thesis leads a reader into the world of social engineering and computer criminality. The main part of the thesis deals with the problems of social engineering - the computer attacks on the weakest point of all security systems, which is the human element. It is followed by the description of the most important parts of the attacks and methods of social engineering. At the conclusion of the thesis I mention the name Kevin Mitnick – the practices of social engineering.

Motto of this work:

"Two things are infinite: the universe and human stupidity; and I'm not sure about the universe." **Albert Einstein**

Key words: Phishing, vishing, pharming, trashing, social engineering

Na tomto místě bych rád poděkoval vedoucí mé bakalářské práce Ing. Jaroslavě Gregušové za odborné vedení, podnětné rady a připomínky, které mi poskytovala během vypracování této práce. Také bych rád poděkoval mým rodičům za podporu během studia.

Prohlašuji,

že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.

Ve Zlíně 20.5.2009 …….……

podpis diplomanta

OBSAH

ÚVOD

Dnešní společnost stále více podléhá použití informačních technologií. V průběhu několika posledních let jsme byli svědky velmi rychlého vývoje informačních a telekomunikačních technologií, které do našich každodenních životů přináší řadu usnadnění, ale bohužel i starostí na které jsme dříve nemuseli brát ohled. Počítačové systémy a technologie se pro mnoho firem i lidí stávají nezbytnou součástí jejich úspěchu. Problém, který v současnosti nastává, je způsoben nejen zdomácněním informačních a telekomunikačních technologií ale i jejich snadnější dostupností a především cenou, která je dnes únosná pro téměř každou rodinu. Pryč jsou časy, kdy si výpočetní techniku a podobné vymoženosti mohly dovolit jen velké korporace a vysoce ziskové společnosti. Počítačové systémy a informační technologie jsou naší každodenní realitou. Do bezprostředního styku s těmito prvky se dostáváme téměř všude. Zdravotnická zařízení, finanční instituce, státní orgány a další zařízení jsou jen malým výčtem míst kde všude se s těmito věcmi můžeme setkávat. Každá taková instituce vlastní desítky našich cenných osobních údajů.

Všichni se dnes a denně setkáváme na úřadě nebo třeba v nemocnici s osobou, která má s počítačem či jinou technikou velmi malé nebo dokonce vůbec žádné zkušenosti. Právě tito lidé se stávají snadnou kořistí pro sociálního inženýra. Člověka, perfektně ovládajícího snad vše spojené s výpočetní technikou. Psychologa, jenž si umí hrát s našimi představami a sny. Využívá k tomu nejen naše znalosti a možnosti, ale i jiné metody počítačové kriminality. Říká Vám něco Vishing, Pharming, Trashing nebo Phishing? Počítačová kriminalita založená na nejslabším článku těchto technologií – člověku, se stává hitem posledních let. Poslední průzkumy navíc poukazují na to, že dokonalost antivirových programů, spyware a firewall dosahuje v některých případech takové dokonalosti, že selhat může opravdu jen lidský faktor. Proto už není příliš moderní hackovat počítačové systémy a prolamovat jejich přístupová hesla. Snadnější je, si o tyto cenné údaje prostě jen říct. Útočníkům také nahrává fakt, že vytvořit např. phishingovou zprávu a oslovit masy uživatelů je mnohem jednodušší než připravit skutečnou „kamennou“ loupež. Navíc se nejedná o osobní kontakt s obětí, proto je identifikace útočníků mnohem obtížnější.

I. TEORETICKÁ ČÁST

1 ACHILLOVA PATA BEZPEČNOSTNÍCH SYSTÉMŮ

Firma si může pořídit ty nejlepší a nejdražší bezpečnostní technologie, vyškolit personál tak, aby byla každá důvěrná informace před odchodem domů pod zámkem, najmout si tu nejlepší firmu na noční ostrahu objektů a přece bude tato organizace ještě zranitelná. [1]

Soukromé osoby mohou dodržovat všechny bezpečnostní zásady doporučované odbornou veřejností, mohou denně instalovat všechny nejnovější produkty vylepšující zabezpečení, aktualizovat a odpovídajícím způsobem pozorně nastavovat svůj systém, mohou použít všechna jeho vylepšení či opravy a přece jsou tyto osoby stále nechráněné.

1.1 Napadení informačních technologií

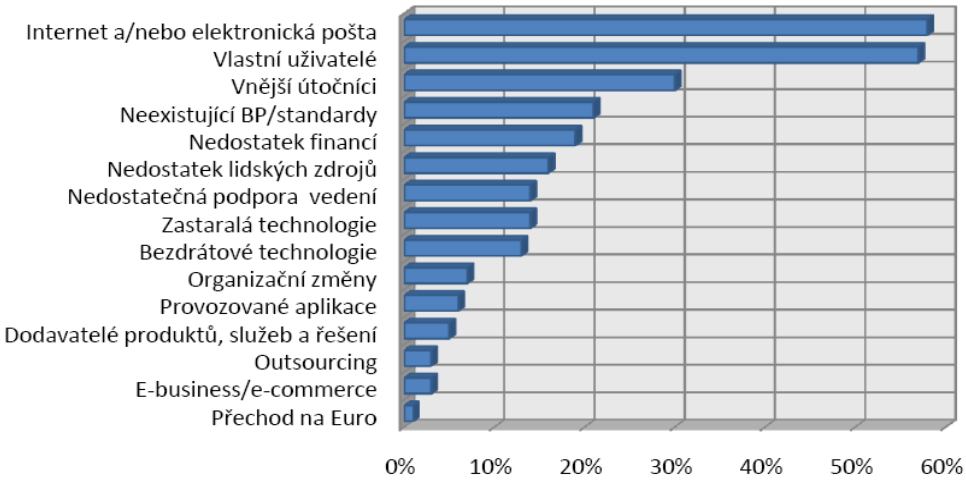
Možnosti, jak napadnout informační systémy se v poslední době stále rozšiřují. Na jednu stranu je pro uživatele mnohem snazší si dostatečně zabezpečit svůj počítač před nepřátelskými útoky. Na internetu najdeme celou řadu programů ve volných verzích pro nastavení a dohledání naší bezpečnosti, které nám umožňují mít nad systémem nepřetržitou kontrolu, hlídat slabiny a upozorňovat na případné průniky. Na straně druhé, ale vždy bohužel stojí útočník a ten má stejné, ne-li větší možnosti než my. Navíc se s rostoucími možnostmi internetu stává díky různým programům a diskuzím o počítačových útocích pachatelem téměř každý. Znalosti dětí navštěvujících základní školy už dávno přesáhly hraní her a tabulkový procesor.

Doba, kdy byly informační systémy, respektive počítače obecně, napadány „hrubou silou“, zde máme na mysli klasické hackování nebo crackování za pomocí SQL Injection[1] a dalších metodik, je pomalu, ale jistě na ústupu. [3]

Systémy a postupy se standardizují. Velkou popularitu tak získávají technologie založené na kvalitních a časem prověřených systémech. U správců počítačových sítí se v poslední

[1] SQL injection znamená, že se kdokoliv a odkudkoliv může "dívat" na data v SQL databázích. A tato data pochopitelně nejenom prohlížet, ale také mazat či měnit. Tady tak nejspíš opravdu přestává jakákoliv legrace.

době velmi uplatňuje Unix[2]. Softwarové společnosti ke svým produktům jako bonus nabízejí bezpečnostní školení, kde se zabývají vývojem daného systému a dávají tak do rukou každého správce certifikované postupy, pravidla a metody jak naložit s bezpečností své společnosti a stát se tak odolným proti vnějším i vnitřním útokům. V dnešní době již nejsou pro většinu správců sítí jimi spravované servery „černými krabicemi“, které nastavují podle, ne vždy pravdivých rad, získaných na internetu, ale logicky pracující stroje, u kterých ví, co a jak nastavit tak, aby systém bezpečně fungoval.



obr. (1) Bakalářská práce: Lidský faktor v bezpečnosti IS/IT a sociotechnika, Adam Trčka

V následujícím grafickém zobrazení si můžeme všimnout jednotlivých hrozeb působících na informační technologie v procentuálním měřítku. Jak vidíme, vlastní uživatel zastává druhou pozici a představuje tak svou neznalostí a neopatrností velké riziko pro bezpečnost informačních technologií. Třetí riziko představují vnější útočníci, čili vlastní zaměstnanci společnosti (více v kapitole interní zaměstnanci.)

Každým rokem se setkáváme s novými metodami obrany proti virům, červům a jiným škůdcům ze světa internetu. Denně na síti najdeme stovky záplat a aktualizací, které stačí stisknutím jediného tlačítka instalovat a ochránit se tak před případným útokem zvenčí.

[2] Unixové systémy byly široce využívány jako operační systémy pro servery, pracovní stanice a v současné době i pro osobní počítače. Sehrály velmi výraznou roli při vzniku Internetu.

K čemu ale tohle všechno, když nám může stačit jediné – lidský faktor a nějaká ta chybička.

1.2 Lidský faktor

Touha po pocitu absolutní bezpečnosti je přirozená, ale vede mnohokrát k falešnému pocitu chybějícího ohrožení. Vezměme si za příklad zodpovědného a milujícího muže, který si pořídil do vstupních dveří systém Medico[3], aby ochránil svou ženu, děti a domov. Po namontování toho zámku se cítí lépe, protože jeho rodina je teď ve větším bezpečí. Ale co se stane, když lupič rozbije sklo v okně nebo prorazí kód otevírající vrata do garáže? Nezávisle na drahých zámcích nejsou stále obyvatelé v bezpečí. [1]

A co když do společnosti zavedeme kompletní bezpečnostní systémy? Situace se nám bude jevit jako lepší, ale stále to nebude záruka úplné bezpečnosti. Proč? Protože Achillovou patou zabezpečení je lidský faktor. Bezpečnost je často představována formou určité iluze. Pokud k ní ještě navíc přiřadíme lidskou lehko věrnost, naivitu a ignoranci, situace se jen zhorší. Nejuznávanější vědec 20. století, Albert Einstein, pravdivě řekl: *„Pouze dvě věci jsou nekonečné: vesmír a lidská hloupost. Ačkoli tím prvním si nejsem jist."*

Ve finále se tak útok sociotechnika téměř vždy podaří, protože lidé bývají hloupí. Nejčastěji jsou takové útoky účinné proto, že lidé nerozumějí prověřeným zásadám bezpečnosti.

Podobný přístup, jako měl pán domu, který si zabezpečil svůj dům kvalitním zámkem, má v dnešní době téměř každý pracovník z oboru informačních technologií. Chybně se domnívá, že dostatečně zabezpečil svou firmu proti útokům tím, že nainstaloval bezpečnostní produkty v podobě různých antivirů, *firewall* a podobných vyspělých řešení, jako jsou například časově závislé kódy nebo biometrické karty. Situace se dá potom jednoduše vysvětlit na příkladu člověka, jenž si koupí nezničitelný trezor pro své cennosti, ale zapomene ho zamknout. Vytvořil si totiž dokonalou iluzi, že produkty samotné zajišťují opravdovou bezpečnost, což je samozřejmě naprostý nesmysl. Je to klasický případ života

[3] Velmi kvalitní bezpečnostní zámek známý především tím, že nejde otevřít paklíčem.

v iluzích a představách, ale přesně takoví lidé jsou bohužel nejvíce zranitelní a stávají se později snadnou obětí útoků.

Jak říká známý poradce pro otázky bezpečnosti Bruce Schneier: „Bezpečnost není výrobek, ale proces". Rozviňme tuto myšlenku: bezpečnost není technologický problém, ale je to problém lidí a řízení. [1]

Hrozby	Závažnost dopadu na systém	Průměrné finanční náklady
Výpadek proudu	25%	50 000 Kč
Porucha HW	21%	110 000 Kč
Počítačový virus	14%	120 000 Kč
Chyba programového vybavení	11%	100 000 Kč
Selhání WAN	7%	25 000 Kč
SPAM	7%	40 000 Kč
Selhání LAN	6%	190 000 Kč
Chyba uživatele	3%	-
Přírodní katastrofa	2%	590 000 Kč
Chyba administrátora	2%	570 000 Kč
Nepovolený přístup k datům – zevnitř	1%	-
Krádež zařízení	1%	55 000 Kč

obr.(2) Bakalářská práce: Lidský faktor v bezpečnosti IS/IT a sociotechnika, Adam Trčka

Uvedená tabulka vychází z grafického zobrazení hrozeb, z hlediska napadení informačních technologií. Popisuje finanční dopad na počítačové technologie v procentech a uvádí následnou finanční škodu. Chyba uživatele dosahuje průměrně 3 %, finanční ztráta není uvedena, protože záleží na okolnostech, při kterých došlo k poškození systému a následné ztrátě dat. 25 % odpovídá výpadkům proudu, kdy dochází k nechtěnému resetu počítače. Nepovolený přístup k datům zevnitř společnosti představuje 1%. Toto číslo bude mít v budoucnu určitě vyšší hodnotu. Více k této tématice v kapitole interní zaměstnanci. Nejvyšší ztráty má chyba administrátora, která má pouhé 2%, ve finančních nákladech se pohybuje v řádech statisíců.

Jak jsme uvedli již v úvodu, je tedy zřejmé, že s postupem stále lepších a dokonalejších bezpečnostních technologií, bude problém najít technickou díru, pro vstup do systému. Útok tak bude směřován přímo na osobu za klávesnicí a její následné překonání bude pro útočníka mnohem levnější, nemluvě o menším riziku. Naskýtá se nám tedy otázka: „jak bojovat s virem, který nedetekuje žádná bezpečnostní utilita? Jak se postavit útoku na lidskou psychologii?“

2 SOCIÁLNÍ INŽENÝRSTVÍ

Je ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Díky tomu je sociotechnik schopný využít lidi, se kterými hovoří, případně dodatečné technologické prostředky a pomůcky které jsou popsané v dalších kapitolách, aby získal hledané informace. [3]

Existuje spousta dalších definic. Nicméně ze všech plyne, že pokud jde o bezpečnost počítačových systémů, nejslabším článkem byl a bude vždy člověk (nejlépe s dostatečně cennými informacemi). V praxi, se pro označení tohoto nejslabšího místa ujal termín "wetware" [4].

Sociální inženýrství vychází s následující myšlenky: Proč se obtěžovat s používáním brutální síly[5] na prolamování hesel, když někdy je mnohem jednodušší přinutit někoho, kdo heslo zná, k tomu, aby nám jej prozradil? Navíc při dobře vedeném útoku si oběť v drtivé většině případů vůbec neuvědomí, že byla okradena o cenné informace. Toto je nejnebezpečnější rys problematiky sociálního inženýrství. Když nám ukradnou peněženku s kreditní kartou, hned je nám jasné, že tuto skutečnost musíme ohlásit a příslušná karta bude zablokována, ale v případě, že útočník použije sociální inženýrství, se jako oběť nemusíme vůbec dozvědět, že nás před chvílí někdo o tyto důležité informace připravil.

Třetí tisíciletí je dnes a denně nazýváno informačním věkem a stále častěji můžeme slyšet, či se dokonce sami přesvědčit, že úspěšný bude ten, kdo bude ovládat způsob, jak získávat,

---

[4] Termín wetware se používá k popisu ztělesnění pojmu fyzikální konstrukce známé jako centrální nervový systém (CNS) a mentální konstrukce známé jako lidský mozek.

[5] Strategie odhalování hesel, která spočívá v testování všech možných kombinací alfanumerických i speciálních znaků. Jedním z vynikajících nástrojů na hádání hesel je L0pthcrack3 (www.atstake.com). Správci používají L0pthcrack3 na vyhledávání "slabých" hesel a hackeři na jejich prolamování. Tento program pracuje s neuvěřitelnou rychlostí, která může na počítači s frekvencí procesoru 1 GHz dosáhnout hodnoty 2,8 milionu pokusů za sekundu.

hledat a správně vyhodnocovat informace. Lidé si stále ještě neuvědomují jejich cenu. Málokoho napadne, že informace je také nutno odpovídajícím způsobem střežit.

Druhá příčina toho, že je možné provádět sociotechnické útoky na poměrně důležitých místech, plyne z pocitu přílišné virtuality oboru informačních technologií. Chybí zde schopnost přenést tyto pojmy do reality. Na co si lidé nesáhnou, to není cenné a jako by to neexistovalo. Zjednodušeně bych to dokázal na následujícím příkladu. Pokud sousedovi odcizím automobil, bude všem zřejmé, že jsem spáchal zločin, neboť po mém činu sousedovi onen automobil evidentně chybí. Pokud bych ale od souseda zkopíroval jeho program či výsledky půlroční práce (samozřejmě nikoli tak, že bych se vloupal do jeho domu, ale elektronickou cestou), nic se neděje – sousedovi přece vše zůstalo. Neutrpěl žádnou hmotnou újmu.

Většina lidí si myslí, že průniky do počítačových systémů jsou čistě technická záležitost, následek děr v systému, které pachatel využije ve svůj prospěch. Skutečnost je ovšem založena na tom, že v úloze pomocníka pro překonávání bezpečnostní bariéry hraje sociotechnika velkou roli. Nedostatečná informovanost uživatelů často poskytuje báječnou příležitost použít je jako vstupní bránu i v takových situacích , kdy útočník nemá vůbec autorizovaný přístup k systému.

Sociální inženýrství je v drtivé většině případů ten nejlevnější a pro znalého člověka i nejjednodušší způsob, jak narušit bezpečnost jinak velmi robustních systémů. Obecně se o sociálním inženýrství dá říci, že útoky mají velmi vysoké procento úspěšnosti a jsou velice zákeřné. Při dobrém skrývání útočníka ho navíc téměř není možné vystopovat. A dopad je někdy drtivý. [3]

2.1 Metody útoku

Jak už to tak bývá, nejjednodušší metody bývají nejspolehlivější. Lidé si zpravidla myslí, že útok bude založen na technické stránce věci. Když Kevin Mitnick vypovídal před americkým Kongresem o tom, jak získával od firem hesla a jiné citlivé informace, uvedl: *"Představil jsem se jako někdo jiný a prostě jsem o ně požádal."*

Jako médium pro sociotechnický útok slouží kromě klasické pošty hlavně telefon a Internet (e-mail, IRC, ICQ).[6] Zkušení sociotechnici mohou provádět i útoky "tváří v tvář".

V případě, že útočník zná oběť osobně, může její heslo odhalit na základě informací, které o ní ví. Zkusí zadat místo narození, přezdívku, název vesnice, ve které má oběť chatu, jméno psa, atd. Je až neuvěřitelné kolik lidí taková hesla používají, je to asi určitá forma lenosti, která vede bohužel ke snadnému prolomení. Nač vypisovat deseti místné heslo a k tomu ještě velká a malá písmena. Další nešvar dnešní společnosti je využívání těchto hesel, lidé používají jedno heslo pro desítky účtů např. pro email, internetové bankovnictví, internetové nákupy atd. Ztráta takového hesla může být pro oběť katastrofou.

Sociotechnici využívají běžných vlastností lidí, jako je důvěřování druhým, občasná lenost, přehlížení drobných odlišností, ochotu pomoci druhým a strach před tím, aby se nedostali do problémů. (Poznámka: zvláště Američané jsou až příliš důvěřiví, nepodezíraví a soucitní).

Pokud pachateli na úspěchu akce záleží, věnuje delší časové období budování důvěry. Útočník s obětí třeba i několik týdnů chatuje a při jednom z rozhovorů (kdy už pro oběť není někým neznámým, ale naopak důvěryhodným) ji přinutí k instalaci drobného užitečného prográmku. Jenže spolu s tímto programem většinou dojde i k tiché instalaci[7] nějakého monitorovacího programu – tzv. spyware[8]**.** Tento speciální software slouží ke skrytému sledování a odposlouchávání veškerého dění na počítači – navštívené internetové stránky, sledování elektronické pošty, stisk kláves při zadávání hesel, atd.

2.1.1 Přímý přístup

Útočník bez okolků přímo požádá oběť (například recepční) o její uživatelské jméno a heslo. Tento druh útoku se může zdát riskantní. Naopak je velmi účinný. Třeba v recepcích velkých hotelů, kde většinou převládá chaos nad pořádkem a z důvodu časové tísně není tolik prostoru pro bezpečnost. Oblíbenější je postupné získávání důvěry jak jsem uvedl již

[6] Všechny tyto metody si podrobně rozebereme v další kapitole nazvané praktiky sociálního inženýrství.

[7] silent install – tzn. uživatel si vůbec neuvědomí, že k něčemu došlo.

[8] Spyware je program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele.

výše, např. pomocí chatu, emailu nebo ICQ. Útočník si postupem času u oběti vybuduje určité kybernetické přátelství, které může vyvrcholit např. doporučením instalace drobné utility pro snadnější komunikaci**.** Dalším způsobem se sociotechnik představí po telefonu jako osoba z vedení společnosti, jako osoba, která vzbudí autoritu a pokud je tato společnost početná (ve firmě o 10 zaměstnancích by asi neuspěl, ale co by tam asi hledal), má velkou šanci, že uspěje. Oběti – zaměstnanci se totiž naskytne otázka, zda vyhovět nebo nevyhovět někomu z vedení. Pro co by jste se rozhodli vy? A co třeba menší forma nátlaku, která se objevuje snad na všech pracovištích - ti nahoře už to měli mít na stole. Pod náporem jednají lidé vždy bezmyšlenkovitě. Naivní odpovědi, typu: „tohle se mi nestane, já bych byl opatrnější“, slyšíme ze všech stran, ale proč je tedy tato metoda tak účinná? Samozřejmě, že vyhovíme a to je základní krok k úspěchu sociotechnika, který po nás napoprvé nemusí požadovat hesla do systému ani další na první pohled cenné údaje. Pouze si prozkoumává terén, aby později zaútočil v plné síle a získal vše potřebné k následnému útoku, který může založit na psychologických vlastnostech člověka jako jsou důvěřivost**,** vzájemnost či sympatie.

2.1.2 Důležitý uživatel

Útočník předstírá, že je někým z vedení firmy, má problémy, které velice rychle potřebuje vyřešit a požádá o informace typu: typ používaného software pro vzdálený přístup, jeho konfiguraci, telefonní čísla k vytáčení, další informace nutné k přilogování se k serveru. Pracovník technické podpory samozřejmě "nadřízenému" rád pomůže (nerad by měl konflikty a nerad by přišel o práci). [3]

2.1.3 Bezmocný uživatel

Nový zaměstnanec společnosti se pro sociotechnika stává nejsnazší kořistí. Neznalost bezpečnostních pravidel a žargonu firmy, včetně jejího vedení často vede k tomu, že se tyto osoby stávají obětními beránky. Je jen otázka času, kdy vlk zaútočí v přestrojení za administrátora sítě. Koho první týden v práci napadne, že ho přišel někdo okrádat o informace? Není nic snazšího než pomoci s nastavením firemního e-mailu nebo přihlášením do sítě. Takto vám oběť prozradí uživatelské jméno a heslo bez jediného zaváhání. Jsme přece zaměstnanci jedné firmy a ti si musí pomáhat.

2.1.4 Pracovník technické podpory

Útočník předstírá, že patří do firemního oddělení informatiky. Zpravidla se představí jako správce systému, sítě. Tímto způsobem získá zaručeně pravdivé informace od běžných uživatelů. Typicky může jít o zaslání e-mailu, který se tváří, že je od administrátora a požaduje s jakýmkoli odůvodněním znovu potvrzení loginu a hesla. Nováčci, kteří nejsou školeni, samozřejmě nemohou tušit, že hlavička odesílatele vůbec nemusí obsahovat pravdivé informace.

2.1.5 Obrácená sociotechnika aneb reverzní psychologie

Reverzní psychologie má v sociálním inženýrství nezastupitelnou roli. Patří sice do skupiny hůře proveditelných útoků, ale o to větší je její úspěšnost. Základní princip vychází z přímého útoku na počítač oběti. V praxi si můžeme situaci popsat následovně: útočník zavolá své oběti s úmyslem získat údaje o jejím počítači. Představí se samozřejmě jako pracovník technické podpory a popíše například momentální situaci ve firemní síti, která obsahuje viry a může tedy hrozit její výpadek. Zděšený zaměstnanec, který nestíhá termín odevzdání svého projektu, si zapíše kontakt na „útočníka“, s tím, že se v případě výpadku nebo poruchy počítače ihned ozve. Sociotechnik se následně musí pokusit vyvolat nějaký problém, aby došlo k telefonátu s obětí, která bez dlouhého váhání prozradí veškerá přístupová práva do sítě společnosti.

2.1.6 Interní zaměstnanci

Přístup těchto uživatelů k citlivým datům či know how firmy je naprosto legitimní a nikdo nezpochybňuje, že různé loginy, hesla a další informace potřebují pro svou každodenní práci. Navíc disponují klíčovými vědomostmi, které sebelepší sociotechnik působící mimo organizaci nebo místní správce IT, postrádá. Znají velmi dobře hodnotu těchto informací. Proč by je tedy chtěli odcizit, popřípadě zpeněžit? Následuje hned několik variant.

Nespokojený zaměstnanec, který již organizaci opustil, nebo ten, který v ní setrvává, může prostě chtít uškodit firmě nebo se obohatit prodejem dat, k nimiž měl přístup. Tento typ uživatele může být destruktivní – třeba náhodou („já přece počítačům nerozumím“) smaže data. Bude-li chytrý, udělá to tak, aby se na ztráty nepřišlo brzy a data nemohla být obnovena ze zálohy.

Další varianta může být založena na zaměstnancích, kteří opouštějí svou pozici ať už za účelem získání nového zaměstnání, nebo založení vlastní firmy. Je téměř jasné, že si od předchozího zaměstnavatele odnesou nejen zkušenosti a praxi, ale i kontakty, know how a další velmi cenné informace.

Z toho, co je zde uvedeno, je jasné, že společnosti využívající moderních technologií pro usnadnění svých činností. Musí ale čelit nejen útoku sociotechnika, ale i útoku z vlastních řad. Ten může být někdy velmi nebezpečný. Většinou jsou tyto útoky těžko prokazatelné a málo předvídatelné.

2.2 Znalosti a zázemí

Sociotechnik tedy díky svým schopnostem může manipulovat s lidmi. Tato vlastnost je sama o sobě jistě v mnoha případech dostačující, nicméně úspěch takovéto akce většinou závisí nejen na psychologické stránce jedince, ale také na jeho znalostech v oblasti počítačových či telefonních systémů.

Sociotechnika se ve spojení s technickým vybavením využívá například v oboru průmyslové špionáže. Dříve bylo nutností aby se útočník fyzicky dostal na půdu firmy, ale proč by se o to dnes pokoušel, když to s pomocí výpočetní techniky a internetového připojení lze provést výrazně jednodušeji.

Absolutní revoluci v této metodě způsobily telefonní systémy – mobilní telefony. Sociotechnik se pomocí psychologického nátlaku pokusí nahnat oběť do kouta. Tam si s ní pohraje jako kočka s myší. Anonymita, kterou telefon poskytuje je neocenitelná.

3 PSYCHOLOGIE JAKO VIRUS

Dle psychologů lidský mozek v případě velkého přívalu nových informací přestává vnímat a hodnotit jejich podstatu, ale pouze si je „mechanicky“ uchovává (jako příklad může sloužit evidentní „přehmat“ vyučujícího při výkladu, který není studenty ve většině případů odhalen ihned, ale až s určitým zpožděním, které mozek potřeboval na to, aby si daný problém zrekapituloval). [5]

Pokud sociotechnik dokáže vytvořit situaci, ve které napadeného přetíží informacemi a požadavky, tak napadená osoba raději, než by čelila přívalu dalších informací, učiní to, o co ji útočník požádá.

Manipulace je předmětem studia sociologů už nejméně padesát let. Článek Roberta B. Cialdiniho v *Scientific American* shrnuje celý výzkum a ukazuje šest „základních vlastností lidské povahy", které se projevují při pokusu podřídit nějakou osobu vůli sociotechnika. Právě na těchto šesti vlastnostech je postaveno (vědomě či častěji podvědomě) manipulování s jinými.

3.1 Autorita

Lidé mají tendenci podřídit se vůli osoby, která má moc. Člověk může vydat informaci, když věří, že žadatel má moc, nebo že je oprávněn žádat o danou službu. Ve své knížce *Ovlivňování lidí. Teorie a praxe (Influence)* popisuje Dr. Cialdini případ tří nemocnic, ve kterých se jistá osoba vydávala za lékaře dané nemocnice. Nezávisle se zkontaktovala s 22 sestrami a dávala pokyny k dávkování léků pacientům na oddělení. Sestry, které přijímaly příkazy, volajícího neznaly. Nevěděly dokonce ani to, jestli je ve skutečnosti lékařem. Nebyl! Navíc lék, který měly podat, nebyl schválen k použití na odděleních. Dávka, kterou měly dát, dvojnásobně překračovala maximální denní dávku tohoto léku a mohla tedy ohrozit život pacientů. Cialdini píše, že v 95 % případů se sestra vydávala směrem ke skříňce s léky, aby vzala určenou dávku, načež zamířila k pacientovi. Posléze byla samozřejmě zastavena pozorovatelem, který ji informoval o experimentu.

3.2 Sympatie

Lidé mají sklon vyhovět, když je žadatel schopen ukázat se jako sympatická osoba, která má podobné zájmy, názory a přístup k životu jako oběť. Během rozhovoru se útočník

dozvídá o nějakém koníčku nebo zájmu oběti a následně deklaruje svůj zájem a nadšení pro stejný koníček. [5] Může také tvrdit, že je ze stejného státu, kraje či školy nebo že má stejné cíle. Sociotechnik se rovněž bude snažit napodobit chování oběti, za účelem vytvoření zdání podobnosti.

3.3 Vzájemnost

Žádosti se podřídíme například, bylo-li nám slíbeno nebo dáno něco cenného. Může se jednat o hmotný dar nebo může představovat radu či pomoc. Když pro nás někdo něco udělá, cítíme potřebu odvděčit se. Tato touha se objevuje dokonce i tehdy, kdy jsme o to, co jsme dostali, nežádali. Jedná se tedy o jeden z nejúčinnějších způsobů ovlivňování lidí tak, aby nám „prokázali službičku“. Například vyznavači Hare Krišny velmi účinně ovlivňovali lidi, aby od nich získali příspěvek. Věnovali jim knížku nebo kytičku. Pokud se obdarovaný pokoušel dárek vrátit, oni ho odmítali přijmout se slovy: „to je náš dárek pro tebe". Využívání principu vzájemnosti značně zvyšovalo příspěvky.

Jako příklad útoku si můžeme představit pracovníka, jenž přijímá hovor od osoby, která se představuje jako informatik. Vysvětluje, že některé počítače byly napadeny novým virem, který antivirový software neodhalí a který může zničit všechny soubory v počítači. Potom nabízí provést pracovníka přes několik kroků, které mu umožní předejít problému. Hned potom volající prosí oběť o otestování nějaké aplikace, která byla právě vylepšená tak, že umožňuje uživatelům změnu hesla. Pracovník nejspíš neodmítne, protože volající mu právě pomohl při ochraně před virem. Oplatí ochotu a vyhoví žádosti.

3.4 Společenský souhlas

Lidé mají tendenci vyhovět prosbám, jestliže se to zdá shodné s chováním jiných. Příklad jiných je vnímán jako souhlas a potvrzení, že dané chování je správné a vhodné.

Jako příklad útoku si můžeme uvést volajícího, jenž tvrdí, že provádí anketu a jmenuje několik známých osob, které se už dříve rozhodly na otázky odpovědět. Oběť věří, že souhlas jiných potvrzuje věrohodnost žádosti a souhlasí tedy také s účastí v anketě. Volající klade řadu otázek, mezi nimiž se skrývá i dotaz na uživatelské jméno a heslo.

3.5 Vzácná příležitost

Lidé mají tendenci se podřídit, když věří, že vytouženého produktu je malé množství, je žádaný mnoha jinými nebo že je dostupný jen kratičký čas.

Útočník rozesílá e-maily oznamující, že prvních 500 osob, které se zaregistrují na nové stránce firmy, vyhraje volné vstupenky na premiéru nejnovějšího filmu. Když se nic netušící osoba na webové stránce registruje, je žádána o uvedení své firemní e-mailové adresy a o zvolení hesla. Mnoho lidí má z pohodlnosti sklon používat to samé heslo v každém počítačovém systému. Útočník, který o tom ví, se může pokusit nabourat do našich firemních nebo soukromých počítačových systémů a využít k tomu uživatelské jméno a heslo, které jsme uvedli při registraci.

4 KDO JE PŘEDSTAVITEL SOCIOTECHNIKY ?

Položit si tuhle otázku před 15 lety, marně by jsme na ni hledali odpověď. Pokud si ji ovšem položíme dnes, řeč se nebude stáčet k nikomu jinému než k nejslavnějšímu hackerovi světa Kevinu Mitnickovi. Začít psát o jeho životní cestě nebylo snadné. Za své činny spojené s počítačovou kriminalitou byl několikrát odsouzen a měl zakázáno publikovat o čemkoliv, co nějakým způsobem souviselo s jeho životem nebo hackingem. Po dobu šesti let svého věznění v roce 1997, měl zakázáno používat počítače a telefony. Soud tehdy svůj rozsudek odůvodnil slovy: „vyzbrojen klávesnicí je nebezpečím pro společnost“.

Kevin Mitnick se narodil 6.října 1963 v San Fernando Valley, severozápadní části města Los Angeles. Jako jeden z hlavních praktiků sociálního inženýrství tuto metodu jak manipulovat s lidmi, uvést je v omyl, ovlivnit a přesvědčit k vykonání něčeho ve svůj prospěch, dokázal využít už ve svých dvanácti letech. Po pár rozhovorech s řidičem autobusu zjistil, jak jezdit městskými linkami zadarmo. Jeho kroky se ovšem nezastavily jen u černého pasažéra, ale pokračoval dál. Co třeba přelstít veřejnou telefonní síť a telefonovat zcela zadarmo? Nebo různě přepojovat cizí hovory pomocí phreakingu[9]? A tím samozřejmě nekončíme.

Při svých studiích v Computer Learning Center v Los Angeles naboural školní síť a za opravení této chyby vystudoval s vyznamenáním. V dobách své největší „slávy“ byl nejhledanější osobou FBI, napadl snad všechny počítačové a telekomunikační společnosti, odposlouchával linky FBI. Vrcholem všeho bylo proniknutí do velitelství vzdušné obrany

[9] je označení pro napojení se na cizí telefonní linku v rozvodnicích, veřejných telefonních budkách nebo přímo na nadzemní/podzemní telefonní vedení, díky čemuž lze: volat zadarmo kamkoliv, surfovat zadarmo po internetu, odposlouchávat cizí telefonní hovory. Za phreaking se považuje i nabourávání se různými metodami do mobilní sítě nebo výroba odposlouchávacích zařízení. Jde o trestnou činnost; dosud z ní nebyl nikdo usvědčen a odsouzen.

Severní Ameriky(NORAD)[10]. Zda se mu to povedlo nebo ne jsou pouhé dohady. V nejednom článku The New York Times a v knize Cyberpunk se o tom vyjádřil John Markoff, podle Mitnicka lhář a člověk, jenž na jeho případu vydělal milion dolarů.

Mýtus, který kolem Kevina Mitnicka vytvořili novináři a média neznal mezí. Natočili o jeho metodách film[11], psali o něm knihy a použili stovky listů papíru. Byl často obviňován za věci, které nikdy nespáchal a byl několikrát donucen, aby se zřekl svých práv. Vyšetřovatelé u soudu veřejně prohlásili, že způsobil několika firmám škodu přesahující 300 milionu dolarů. Policie v době vyšetřování varovala všechny své agenty, aby mu nesdělovali žádné osobní údaje, protože by jim mohl elektronicky zničit život.

V článku z roku 1999 zveřejněném v časopise Forbes popsal Mitnickovu situaci Adam L. Penenberg následně: „zločiny Kevina Mitnicka byly prakticky neškodné. Vloupal se do počítačů velkých firem, ale nikdy se nenašly důkazy, že by zničil nějaká data nebo prodal zkopírované soubory. Kradl programy, ale nic s nimi později nedělal“.

Po propuštění z vězení (21. ledna 2000), kde strávil celkem 68 měsíců, Mitnick změnil svůj život. Vydal se na druhý břeh řeky a je z něj uznávaný expert na bezpečnost počítačových systémů. V roce 2003 svou návštěvou poctil i Českou republiku při uvedení jeho nové knihy Umění klamu do českých knihkupectví.

Na závěr bych si dovolil uvést jeho vlastní prohlášení ke svým činům z on-line verze Historie Kevina – nezveřejněné kapitoly knihy Umění Klamu, kde jako její autor popisuje metody sociálního inženýrství.

„Má činnost byla způsobena zvědavostí – toužil jsem znát všechno, co se dalo, o tom, jak fungují telefonní sítě a vstupy a výstupy počítačových bezpečnostních systémů. Z dítěte fascinovaného kouzelnickými kousky jsem se stal nejhroznějším hackerem na světě, kterého se obává vláda i korporace. Když se probírám vzpomínkami posledních třiceti let

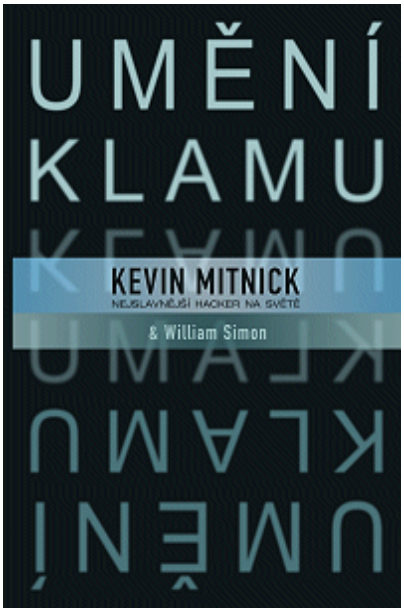
---

[10] Severoamerické velitelství protivzdušné obrany NORAD *(North American Aerospace Defense Command)* je společným velením Spojených států amerických a Kanady. Středisko je vyprojektováno tak, aby přežilo explozi jaderné bomby o síle až 30 kilotun.

[11] Hacker two – Operation TakeDown < http://www.csfd.cz/film/1516-takedown/ >

mého života, musím přiznat, že jsem vedený zvědavostí, touhou po poznání technologií a uspokojováním intelektuálních výzev, učinil několik velmi špatných rozhodnutí. Změnil jsem se. Dnes využívám svůj talent a své znalosti o bezpečnosti informací a sociotechnice, které se mi podařilo osvojit, abych pomáhal vládě, firmám i soukromým osobám při odhalování, prevenci a reagování na ohrožení bezpečnosti informací.“

Kevin Mitnick



obr. (3) Umění klamu, Kevin Mitnick.

5 PRAKTIKY SOCIÁLNÍHO INŽENÝRSTVÍ

5.1 Phishing

Phishing (někdy převáděno do češtiny jako rybaření) je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) od obětí útoku. Jejím principem je rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky či jiné podobné instituce a vyzývají adresáta k zadání jeho údajů na odkazovanou stránku. Tato stránka může například napodobovat přihlašovací okno internetového bankovnictví (viz. Příloha PI) a uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze. [7]

Phishing v e-mailech, instant messagingu[12] a na webu využívá hlavně možnosti zveřejnit odkaz, který vede někam jinam, než jak se ve skutečnosti tváří. V minulosti se v odkazech snažili útočníci zachovat alespoň část adresy skutečného webu. Aktuální vlny phishingu se s tím ale již nezatěžují. Uživatelé totiž zpravidla stejně nevědí, jak má či nemá vypadat internetová adresa.

5.1.1 Co se phishingem vlastně sleduje?

Phishing se používá pro sběr informací, které umožňují uživateli, aby získal cenné a pro útočníka užitečné informace. Prostě a jednoduše, je důležité si uvědomit, že stane-li se člověk obětí phishingu a zadá-li číslo své bankovní karty**,** PIN kód a CCV, tak je s největší pravděpodobností na dobré cestě k tomu, aby z jeho bankovního účtu zmizely peníze. Většina bank v takovém případě využívá chytrých dodatků, které jasně říkají, že transakce provedené s použitím PIN nepodléhají ochraně proti zneužití karty. Vy můžete tedy přijít o všechno, co díky znalosti PINU někdo zneužil.

[12] Instant messaging je internetová služba, umožňující svým uživatelům sledovat, kteří jejich přátelé jsou právě připojeni, a dle potřeby jim posílat zprávy, chatovat, přeposílat soubory mezi uživateli a i jinak komunikovat. Hlavní výhodou oproti používání např. e-mailu spočívá v principu odesílání a přijímání zpráv v reálném čase.

5.1.2 Z čeho phishing čerpá?

Nepozornost

Hlavním pomocníkem těchto útočníků je často nepozornost samotných obětí. Phishingu se však může vyvarovat každý. Stačí bedlivě sledovat, kam jsme falešnými zprávami směrováni. Přestože se podvodné stránky věrně podobají originálu, je dobré zkontrolovat si název domény, na které se právě nacházíme. I nepatrná změna v adrese stránek je již varováním, že není vše v pořádku. Příkladem může být např. rozdílnost mezi *internetbanka.cz* a *internebanka.cz*.

Důvěřivost a sociální inženýrství

Autoři phishingových zpráv velmi výrazně zneužívají důvěřivost uživatelů. Americké průzkumy dokazují, že v jednotlivých kampaních bývá až 5% napálených uživatelů. V mnohých případech bývá jejich počet dokonce i vyšší. I v tomto případě lze katastrofě včas předejít. Zejména dodržováním zlatého pravidla nikomu nesvěřovat důvěrné informace**.** Samotné banky takové údaje nikdy nevyžadují, pouze v přihlašovacím formuláři do samotného internetového účtu. K potvrzování platnosti nebo obnovy účtu je využíváno jiných metod. [9]

Neznalost

Pro většinu uživatelů internetu bývá neznalost problematiky zásadním handicapem. Tuto vadu částečně napravují média i samotné poškozené instituce informativními zprávami uvnitř online systému. Například banky samy informují uživatele o aktuálních hrozbách a radí, jak jim čelit. [9]

obr.(4) Mapa světa zobrazující útoky phishingu na jednoho člověka – viz. legenda. V ČR tak připadá 0,11 až 0,32 útoku na jedince denně.

5.1.3 Jak se bránit?

Postupem času se už i začínající surfaři naučili nepovažovat internet za zdroj pouze důvěryhodných informací a ke stahování dat z nedůvěryhodných zdrojů se staví více pesimisticky. Podobné návyky však zatím nemají plně osvojeny. Ve světě podvodných naléhavých zpráv, které vyžadují zadání citlivých údajů se jedná o podobný problém, jako například v případě hesel na prodej.

Nedoporučuje se proto následovat hypertextové odkazy zahrnuté přímo v e-mailu (viz. Příloha P II). Toto pravidlo by mělo být uplatňováno již od počátku rozšíření nemoci zvané spam[13], jelikož díky zmíněné technice spammeři zjišťují, zda je vyhlédnutá e-mailová adresa aktivní. Při phishingu jsou důsledky samozřejmě mnohem drsnější.

Dotazníky vyplňujte pouze na ověřených stránkách. Pokud by nějaká instituce přímo vyžadovala jisté potencionálně citlivé údaje, využije k tomu zřejmě zabezpečený šifrovaný přístup. Prověřujte proto nabízené a přijímané certifikáty, jejich platnost a důvěryhodnost.

Naučte se používat prohlížeče či doplňky, které umějí phishing rozpoznat (z prohlížečů např. IE7, My Internet Browser, Firefox, Opera, z doplňků třeba Netcraft Toolbar).

E-mail se špatnou či chybějící diakritikou (tj. háčky, čárky), v cizím jazyce, či zvláštním fontem nebudou od Vaší banky nebo jiné důležité organizace. Používejte aktualizovaný antivirový software. [10]

Ve většině případů komunikace probíhá po běžném, nezabezpečeném protokolu (adresa tedy začíná http://..... místo zabezpečeného protokolu https://.....).

[13] Spam je nevyžádané masově šířené sdělení (nejčastěji reklamní) šířené internetem. Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace – např. diskuzní fóra, komentáře nebo instant messaging.

5.2 Vishing

V poslední době se objevuje stále více finančních podvodů spojených s internetovým bankovnictvím, kdy se pomocí "*phishingu*" získávají z důvěřivých klientů bank klíčové informace pro přístup k jejich bankovním kontům. Většině z nás je proto pojem "*phishing*" už naprosto známý, ale znáte i "*vishing*"?

Vishing je podle wikipedie zneužívání Voice over Internet Protocol (VoIP[14]) technologie pro vylákání osobních a finančních informací, za účelem osobního obohacení. Vishing těží z důvěry v telefonní služby, které jsou pevně spjaté se sídlem určité renomované telefonní společnosti. Ale s příchodem VoIP již nemusí být na konci "drátu" pevná linka, ale třeba i počítač. A počítač je proti běžné telefonní přípojce možno zneužít mnohem snadněji nemluvě o možnostech které nám nabízí.

V roce 2007 byl zaznamenán oproti roku předchozímu vysoký nárůst těchto útoků a předpokládá se další růst i v roce 2008. Je to dáno především větší dostupností VoIP služeb a především jejich cenovou výhodou. Technologie VoIP je relativně nová a tak vývoj bezpečnostních řešení má za jejím nástupem zpoždění. Bezpečnostní experti varují, že vishing může být daleko efektivnější než tradiční phishing technologie.[11]

obr.(5) Seznam.cz/obrázky, lákání - vishing.

[14] Voice over Internet Protocol (zkratkou VoIP) je technologie, umožňující přenos digitalizovaného hlasu v těle paketů rodiny protokolů UDP/TCP/IP prostřednictvím počítačové sítě nebo jiného média, prostupného pro protokol IP. Využívá se pro telefonování prostřednictvím Internetu, intranetu nebo jakéhokoliv jiného datového spojení.

5.2.1 Phishing po telefonu

K tomu, aby spotřebitele informovali o „problémech s účtem“, používají e-mailové zprávy nebo automatické telefonní vzkazy. Příjemci jsou požádáni, aby problém vyřešili zavoláním na bezplatné telefonní číslo. Po zavolání oběť uslyší zprávu, která je k nerozeznání od zprávy pravého automatického telefonního systému. Osoba je požádána, aby uvedla číslo účtu, heslo nebo číslo sociálního zabezpečení. Tyto údaje jsou poté prodávány na internetu a používány k podvodům se získanou identitou. [11]

5.2.2 Příklad vishingu

1) Podvodník nakonfiguruje vytáčení na telefonní čísla v dané oblasti.

2) Je-li hovor přijat, automatický záznamník (aplikace na počítači útočníka) upozorní zákazníka, že byla provedena s jeho účtem podezřelá aktivita a že musí bezprostředně zavolat na číslo, které je mu nadiktováno. Toto číslo může být bezplatné, nějak asociované s telefonními čísly banky, za kterou se útočník snaží vydávat.

3) Pokud zákazník zavolá na dané číslo, odpoví mu počítačem generovaný hlas, který ho požádá o autentizaci pro přístup k jeho účtu formou zadání 16 ciferného čísla kreditní karty.

4) Zadá-li zákazník celé číslo, pak útočníkovy poskytne všechny nutné informace k utrácení na účet podvedeného zákazníka.

5) Telefonát může být použit i k získání jiných citlivých informací jako je PIN, datum vypršení platnosti karty, datum narození, číslo bankovního účtu,…

obr.(6) Seznam.cz/obrázky, lákání - vishing.

5.2.3 Jak se chránit

Vishing napodobuje obvyklý způsob komunikace lidí s jejich finančními institucemi, takže oběti s větší pravděpodobností bez zaváhání zareagují. Lidé věří telefonu více než internetu, protože hromadné podvody prostřednictvím telefonu nepřicházejí příliš v úvahu vzhledem k tomu, že pevné linky a mobilní telefony jsou snáze identifikovatelné a jsou spojeny s vyššími náklady. Ale díky službám VoIP je tato bezpečnostní bariéra neúčinná.

Internetové telefonní společnosti umožňují snadno získat anonymní účet a s nízkými náklady zvládat velké množství hovorů. Zloději mohou pomocí levného softwaru vytvořit interaktivní hlasový systém, který zní naprosto stejně jako systém používaný bankou, dokonce včetně hudby v době čekání.

Tradiční nástroje pro ochranu před phishingem nemohou v textu e-mailu snadno zjistit falešné telefonní číslo, takže ochrana proti vishingu zůstává na uživateli. Vždy, když přijde na identifikační údaje, je vhodné používat zdravý rozum. Nikdy nereagujte na e-mail nebo hlasovou poštu požadující, abyste vyřešili problém s účtem tak, že přejdete na nějaký web nebo zavoláte na nějaké telefonní číslo. Tyto zprávy nejsou nikdy pravé. Pokud máte jakékoli pochybnosti, zavolejte obchodníkovi nebo instituci na číslo, o kterém víte, že je pravé.

Zvykněte si žádat o ověření totožnosti. Požádejte například osobu na druhé straně linky, aby vám sdělila, jakou transakci jste naposledy provedli. Zloděj nebude mít pravděpodobně k takovým informacím přístup a jeho útok bude zmařen. [12]

5.3 Trashing

Trashing z anglického překladu formulován spíše jako vybírač popelnic, třídič odpadu. V praxi to znamená prosévání firemního nebo bytového odpadu za účelem získání cenných informací. Tato metoda je v rukou sociotechnika velmi užitečnou zbraní, s její oblíbeností je to poněkud horší. Ne každý má žaludek na prohrabávání popelnic. Útočník má jasný cíl. Hledá dokumenty spojené například z výpisy z účtu, telefonních karet a jiné cennosti.

Útok potom vede díky nalezeným dokumentům. S množstvím vyprodukovaného odpadu se tato metoda stává velmi účinná. Řada velkých společností má kontejnery umístěny v nestřeženém okolí svých budov, stávají se tak snadno dostupné pro útočníka (viz. Příloha P III). Další moderní trend dnešní doby jako je třídění odpadů přináší do této oblasti řadu usnadnění. Kontejnery na papír tak obsahují pouze papírový odpad a útočník se tak nemusí zabývat zbytky jídla a podobným odpadem.

5.3.1 Obrana

Ochrana Vašich dat je založena především na zdravém rozumu. Zbavovat se výpisů z účtů a podobných dokumentů pomocí odpadkového koše není bezpečné. Stejně bezúspěšná je metoda skartace papírových dokumentů, která nám spíše uvolní místo na psacím stole než bezpečné odstranění dokumentů. Pokud bude útočník toužit po vašich výpisech z účtů, dá si tu práci a pořezané papíry složí zpět jako puzzle. Řada lidí se proto uchyluje k nejednoduší variantě jak se zbavit papírových cenností, jednoduše nimi roztopí v kamnech. Velké společnosti postupně přechází na elektronickou formu kterou například představuje elektronická fakturace. Tato metoda je sice zbaví možnosti útoku trashingem, ale otvírá je jiným rizikům spojeným s elektronickou bezpečností.

obr.(7) Wikipedia.com/trashing, ukázky trashingu

5.4 Pharming

Pharming“ označuje činnost, při které hackeři přesměrovávají internetovou komunikaci z jednoho webu na jiný, stejně vypadající, s cílem oklamat vás tak, abyste zadali své uživatelské jméno a heslo do databáze na jejich falešném webu.

Pharming („pharmaření“) má dvě podoby. První z nich je značně efektivní, ale také pro útočníka neobyčejně obtížná, což její užití omezuje. Druhá je jednodušší, nicméně se jí lze snáze bránit. Popišme si obě.

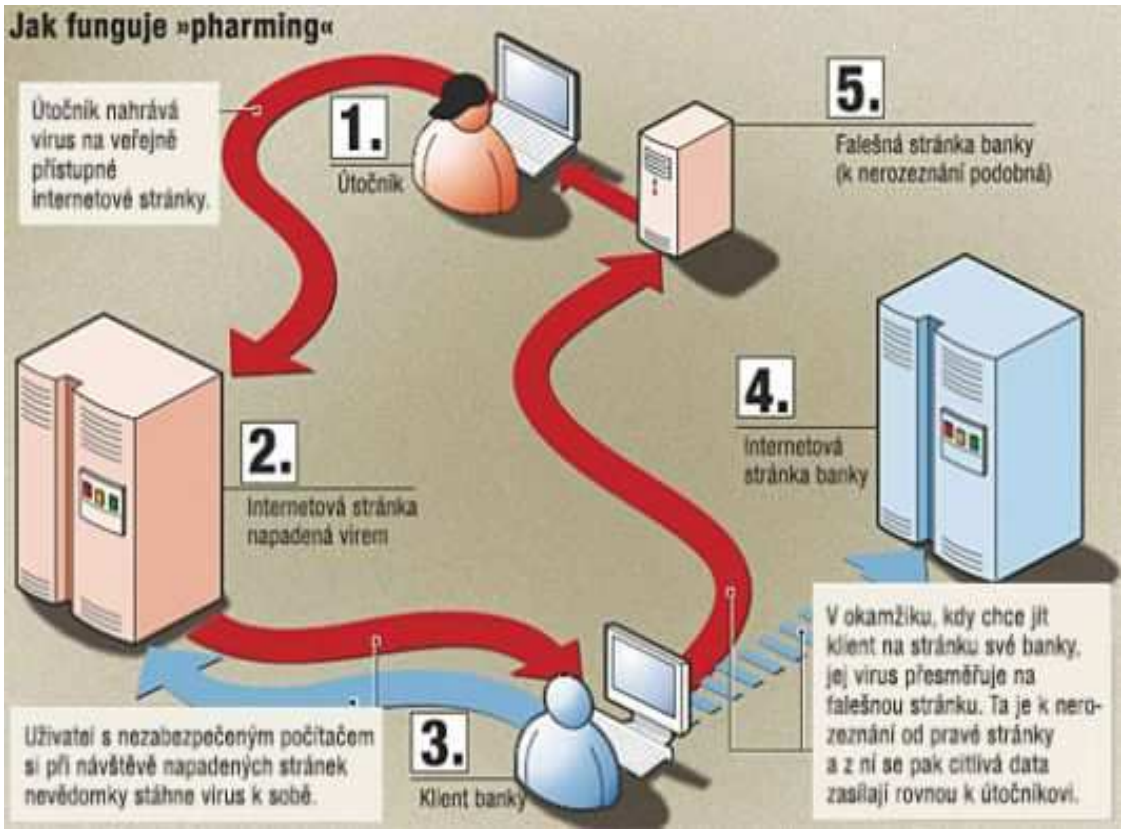
Pharming v „globálním“ měřítku spočívá v tom, že útočník neoslovuje přímo jednotlivé uživatele služby, ale napadne vybraný DNS server[15]. Pokud se podvodníkovi zdaří změnit záznam v hůře zabezpečeném DNS serveru, pak všichni uživatelé, kteří jsou napojeni na tento DNS server a zadají do adresního řádku prohlížeče správnou adresu třeba internetového bankovnictví, dostanou falešnou stránku. Jestliže je tato falešná stránka dobře vypracovaná, pak je šance, že by uživatel, byť i erudovaný, na podvod přišel, velmi nízká. Musel by totiž kontrolovat certifikát, kterým je podepsána, a kterým se šifruje přenos dat. Tento certifikát se všemi náležitostmi není podvodník schopen padělat, nicméně může navodit stav, kdy je z pohledu uživatele, který netrvá na velmi podrobném průzkumu, vše v pořádku.

Druhá metoda, můžeme ji nazvat lokální pharming, je založena na útoku proti jednotlivým počítačům. PC s operačními systémy Windows obsahují takzvaný hosts soubor, který funguje obdobně jako DNS server. Tedy, obsahuje IP adresy a korespondující domény. Jestliže se útočníkovi podaří do tohoto souboru zapsat adresu své podvodné stránky a doménou bankovnictví, pak je efekt pro uživatele stejný jako v předchozím případě. Tedy i po zadání korektní URL adresy je zobrazena podvodná stránka a přihlašovací údaje skončí v rukách zločince.

---

[15] DNS (Domain Name System) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. Později ale přibral další funkce (např. pro elektronickou poštu či IP telefonii) a slouží dnes de facto jako distribuovaná databáze síťových informací.

První metoda je nezávislá na klientských počítačích, nicméně je potřeba zdolat ochranu DNS serveru. Vzhledem k tomu, že DNS tvoří páteř Internetu, jsou tyto servery jedny z nejvíce chráněných. Objevit v nich zneužitelnou chybu a využít ji, aniž by si toho správci všimli, je extrémně obtížná záležitost. A tak se útočníci uchylují ke druhé metodě. [13]



obr.(8) Seznam.cz/obrázky, funkce pharmingu

5.4.1 Jak Pharmingu čelit

Jak je zřejmé, pharming je podstatně nebezpečnější než phishing. Lze jím oklamat i zkušeného uživatele webových služeb. Nemusí jej odhalit dokonce ani ochrana před podvodnými weby, jež je součástí posledních verzí webových prohlížečů. Nicméně to, že je boj proti němu obtížnější, neznamená, že by bylo nutné jej vzdát.

Možnosti správců uživatelských PC a samotných uživatelů postupovat proti pharmingu založenému na napadení DNS serveru jsou v podstatě minimální. Ochrana proti lokální formě útoku je založena především na aktivním, správně nastaveném a hlavně aktuálním antivirovém programu. Ten by měl kontrolovat nejen všechny soubory posílané elektronickou poštou, ale také vše, co je spouštěno a stahováno z webu. Útočník se může

snažit škodlivý kód zabalit do šifrovaného archivu, takže antivirus musí kontrolovat archivy v okamžiku jejich otevření.

Druhým krokem ochrany je samotný soubor s názvy hostitelů. Některé bezpečnostní aplikace jej umožňují uzamknout a chránit před změnou. Takže i kdyby došlo k instalaci trojského koně, tento se seznamem hostitelů nic nezmůže. Nevýhodou této metody je, že do seznamu potřebují zapisovat také některé regulérní aplikace, služby s webovým rozhraním spouštěné z místního počítače a některé síťové technologie. Ty je pro některé uživatele obtížné odlišit od škodlivého kódu a uzamčení souboru s hostiteli snižuje použitelnost regulérních programů.

Třetí možností, která je vhodná spíše pro technicky zdatnější a aktivní uživatele, je používání nástrojů, které zobrazují doplňující informace o právě zobrazovaných webových stránkách. Jedním z těchto nástrojů je například produkt Netcraft Toolbar[16].

Moderní webové prohlížeče obsahují už zmíněnou ochranu před podvodnými stránkami. Aby tato ochrana fungovala, musí být stránka odhalena a označena za nebezpečnou. Z tohoto důvodu nelze zejména v případě útoků, které jsou směřovány na konkrétní uživatele na malém území (například elektronického bankovnictví České spořitelny v ČR), spoléhat na její dostatečnou rychlost.

Posledním (ale vlastně spíše prvním) důležitým faktorem je informování uživatelů a určitá hygiena práce s počítačem. Uživatelé by měli vědět, že nesmí bezhlavě klikat na odkazy v e-mailech, stahovat z Internetu neznámé aplikace, i kdyby se tvářily sebelépe, a že banka (ani jiná služba) jim kvůli „kontrole“ údajů nikdy žádný e-mail nepošle.

Pharming je nebezpečný, ale lze jej zvládnout obdobně jako phishing nebo červy rozesílané e-mailem. Tím nejdůležitějším je ale nepodcenit problém a hlavně co nejvyšší informovanost koncových uživatelů. [14]

---

[16] Nástrojová lišta do internetových prohlížečů Firefox a MSIE, která zobrazuje bezpečnostní informace o právě otevřených internetových stránkách a zabraňuje tak tzv. phishingu. Program neustále kontroluje obsah a umístění stránek a upozorňuje na každý nebezpečný nebo podezřelý web, na kterém hrozí phishing, tj. zneužití osobních údajů uživatele.

obr.(9) Seznam.cz/obrázky, jednoduchá obrazová ukázka pharmingu. Vlevo nebo vpravo – u pharmingu je to jedno.

II. PRAKTICKÁ ČÁST

6 ANKETA Z OBLASTI SI

Existuje řada způsobů, jak zjistit zda lidé znají určitou problematiku. Zda se s ní setkali, nebo jim nic neříká. Americká společnost McAfee, zabývající se bezpečností počítačových systémů využívá při zkoumání trhu on-line aplikace, ve kterých se dotazuje svých uživatelů na otázky spojené s počítačovou bezpečností. U nás se s touto metodou můžeme setkat na serveru idnes.cz v aplikaci on-line monitor. Další a jednoduší způsob dotazování využívají výrobci bezpečnostních utilit. Při instalaci svého programu, zpovídají uživatele, který jim vyplněný dotazník pošle v rámci doinstalování aplikace.

Ve své práci jsem použil jednoduchý průzkum, který vychází z ankety spojené se SI. Anketu jsem vytvořil pomocí serveru www.vyplnto.cz. Odkaz na ni byl umístěn na internetových stránkách www.sociotechnika.ic.cz, které jsem věnoval sociálnímu inženýrství a jeho praktikám. Otázky byly anonymní a sestaveny pouze za účelem určité klasifikace znalostí z oblasti sociálního inženýrství a bezpečnosti na internetu. Anketa byla on-line přístupná 14 dní a zúčastnilo se jí 254 studentů Univerzity Tomáše Bati, především z fakulty aplikované informatiky. Skládala se ze 14 otázek které rozeberu na dalších stranách praktické části.

Cílem ankety bylo zjistit, zda pojmy úzce spjaté s počítačovou kriminalitou v podobě SI, phishingu a vishingu zná především mladá počítačová generace. Soustředění na studenty fakulty aplikované informatiky bylo úmyslné, neboť právě oni s počítačovými technologiemi přicházejí do styku nejen ve volných chvílích, ale i ve škole a v budoucím zaměstnání. Druhá polovina ankety byla zaměřena na chování na internetu (zacházení s hesly, internet banking).

6.1 Obsah průzkumu

Jednotlivé otázky umístěné popořadě v průzkumu. Návaznost otázek záležela na odpovědi tázaného. Pokud na první otázku, zda někdy slyšel o pojmu sociální inženýrství odpověděl ne – otázka číslo dvě, zda se s touto metodou setkal nebyla položena.

- Slyšeli jste někdy o pojmu sociální inženýrství?
    - Ano, ale nevím, co to znamená.
    - Ano, vím, co to znamená.
    - Ne
- Setkali jste se někdy s touto metodou?
    - Ano, v zaměstnání.
    - Ano, ve škole.
    - Ne
- Říká Vám něco jméno Kevin Mitnick?
    - Ano, ale netuším kdo to je.
    - Ano, vím kdo to je.
    - Ne
- Říká Vám něco Phishing?
    - Ne
    - Někdy jsem to slyšel, ale nevíc co to znamená.
    - Někdy jsem to slyšel, ale nevím co to znamená.
    - Setkal jsem se s ním.
- Znáte Vishing?
    - ano
    - ne
- Používáte antivirový program?
    - Ano
    - Ne

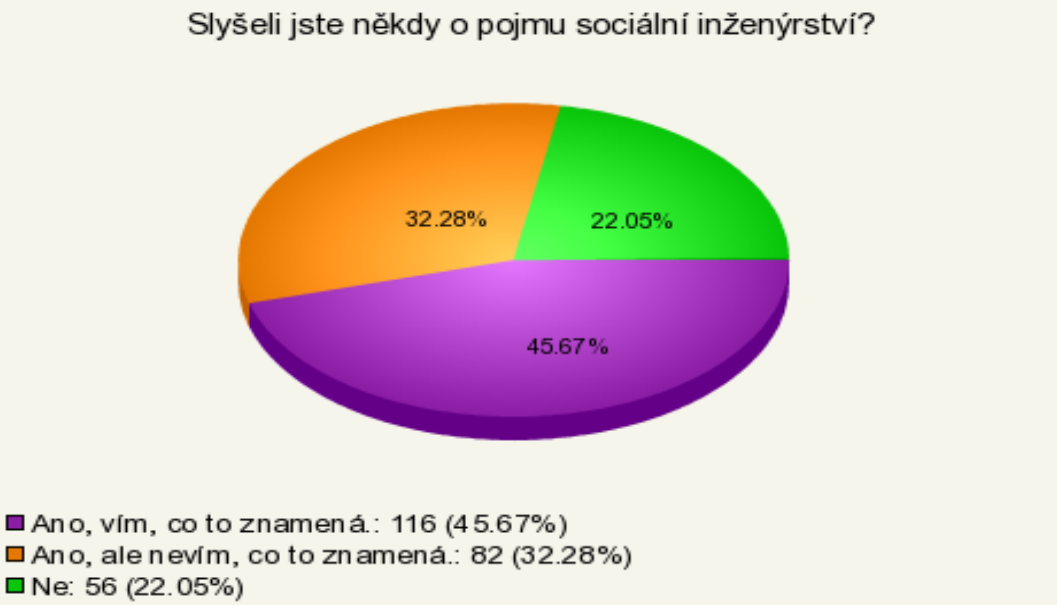
- Jaký antivirový program používáte?
    - AVAST
    - AVG
    - Jiný typ.
    - Kaspersky antivirus
    - NOD 32
- Používáte další doplňky pro ochranu PC ze strany internetu?
    - Firewall
    - Firewall i Spyware
    - Ne
    - Spyware
- Máte nastavenou automatickou aktualizaci těchto programů?
    - ano
    - ne
- Používáte některé prvky sociálních sítí?
    - Facebook
    - Icq
    - MySpace
    - Ne
    - Skype
- Používáte internet banking?
    - ano
    - ne
- Odpovídáte na neznáme e-maily?
    - Ano
    - Ne
    - Občas

- Setkali jste se někdy s emailem, který Vás odkazoval na finanční instituci a požadoval Vaše přihlášení v podobě loginu a hesla?
    - ano
    - ne
- Používáte pro přihlášení na různé stránky stejná hesla?
    - ano
    - ne

6.2 Analýza průzkumu

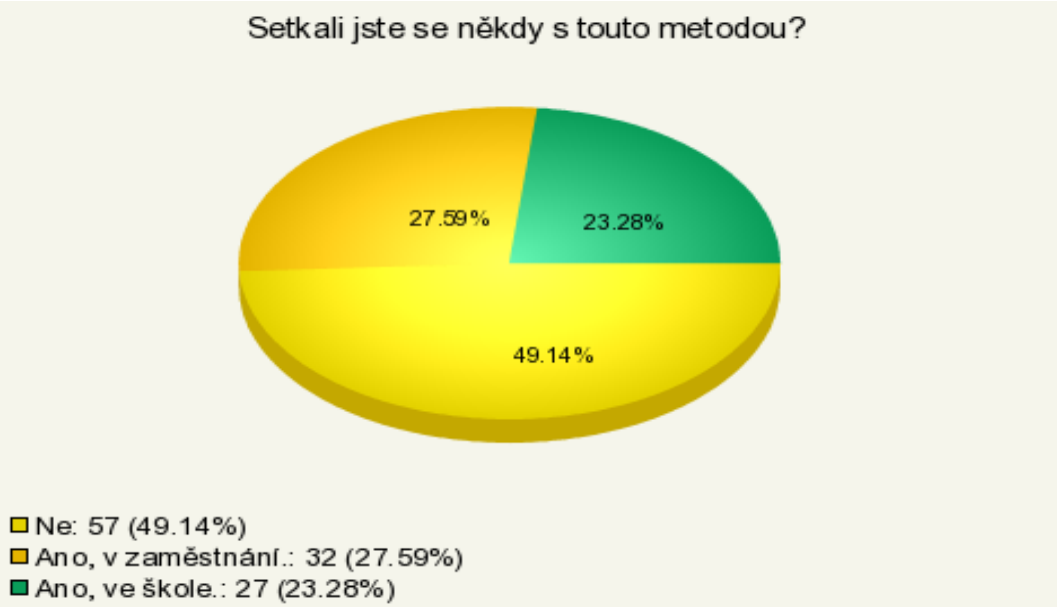
Pomocí grafického zobrazení – koláčové grafy, rozeberu jednotlivé otázky a odpovědi na ně uvedu v % měřítku. Analýza průzkumu je nejdůležitější částí ankety. Odpovědi nám v % ukážou, zda se hlasující s danou problematikou někdy setkali, nebo o ní alespoň slyšeli. SI je pro dnešní společnost relativně neznámí pojem. Průzkum nám ukáže zda je tomu tak.

6.2.1 Slyšeli jste někdy o pojmu sociální inženýrství?



Jak je zřejmé z legendy umístěné pod grafem, 116 hlasujících což představuje 45,67 % ví, co znamená sociální inženýrství. V souvislosti s tím můžeme mluvit o určitém pokroku ve znalostech lidí z této oblasti. Průzkumy vytvářené před několika lety, měly co se SI týče mnohem větší procentuální neznalost, která v našem případě činní 22,05 % v podobě 56 hlasů. 32, 28 % lidí hlasovalo pro odpověď „ano, ale nevím co to znamená“. Často ve spěchu něco pouze zaslechneme a pokud se nás to netýká, nevěnujeme tomu pozornost. Velká zbraň SI je především neznalost jeho základních praktik. Lidé se tak řídí jednoduchým pravidlem, co neznám, to neexistuje. Úspěšnost této metody mluví bohužel za všechny průzkumy.

6.2.2 Setkali jste se někdy s touto metodou?

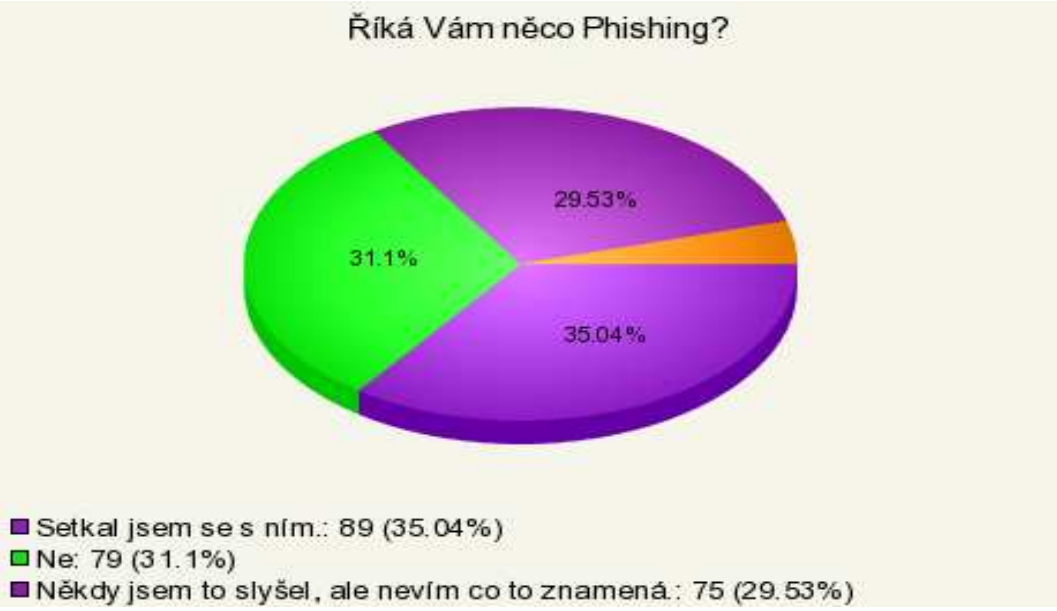


Z grafu je jasné, že se většina hlasujících, která sice věděla co SI znamená se touto metodou nikdy nesetkala. Přesně to zobrazuje 57 hlasů v podobě 49,14 %. Pokud se ovšem na chvíli pozastavíme nad tímto výsledkem, nemůžeme ho považovat za zcela pravdivý. Hlasující si pouze myslí, že se s touto metodou nikdy nesetkali. Skutečnost může být výrazně ovlivněna neznalostí jednotlivých praktik. Uživatel ani nemusí tušit, že se stal obětí SI nebo jiných praktik této nevyzpytatelné metody. Počet odpovědí je rovněž omezen tak jak jsme uvedli již v úvodu navazováním jednotlivých otázek na předchozí. 27,59 % odpovědí představuje možnost, ano v zaměstnání. Výsledek odpovídá průzkumům pořádaným ve světě. 23, 28 % v podobě 27 hlasů získala odpověď, ano ve škole. Je tedy jasné, že obětí se nemusí stát jen osoba s tučným kontem, ale i student, který sice nedisponuje žádným majetkem, ale má pro útočníka i jiné cenné informace v podobě loginu a hesla k přihlášení do školní sítě apod.

6.2.3 Říká Vám něco jméno Kevin Mitnick?

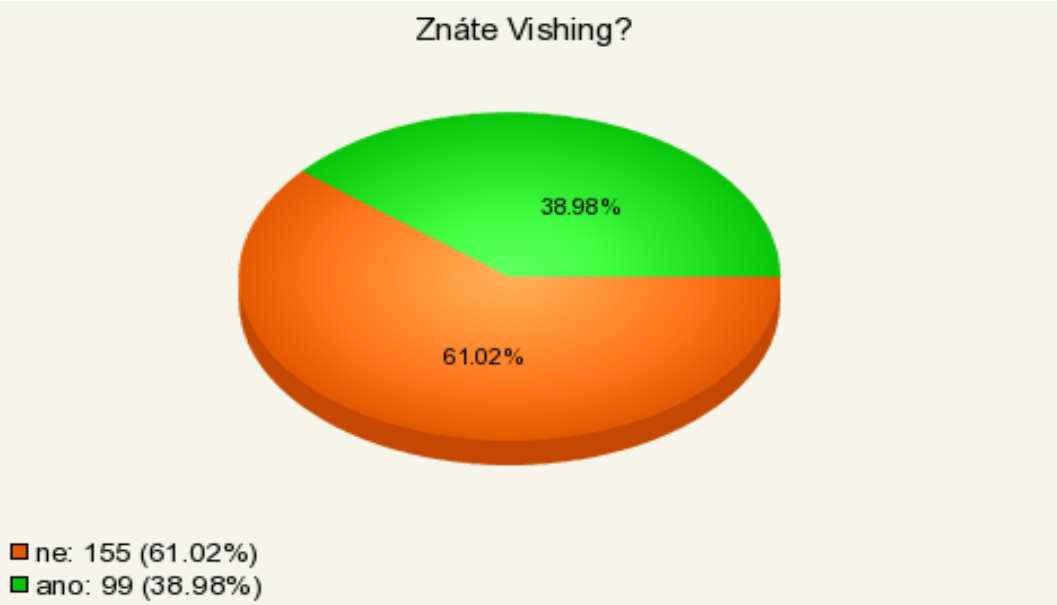
Kevin Mitnick – praktik sociálního inženýrství. 82 hlasů v podobě 59, 42 % ukázalo na to, že je toto jméno stále neznámé, a to se nepojí pouze se SI. Pro společnost může být známé především z tisku a televize. Určitě by měl graf jiné odpovědi, kdybych ho publikoval v USA, kde toto jméno zažilo velkou publicitu. 21, 01 % odpovídá kladné odpovědi. 19,57 % toto jméno někdy slyšely, ale netuší kdo to je. Krásně můžeme díky tomuto grafu zhodnotit dnešní společnost, která si ještě nezvykla na to že počítače tvoří její nedílnou součást jako rádio a televize. Pokud bych se v anketě ptal na nějakého herce nebo zpěvačku, téměř 100 % by odpověď směřovala ke slovům ano znám. Pokud se zeptáme na celebritu z počítačové bezpečnosti, odpovědi jsou spíše záporného charakteru.

6.2.4 Říká Vám něco Phishing?



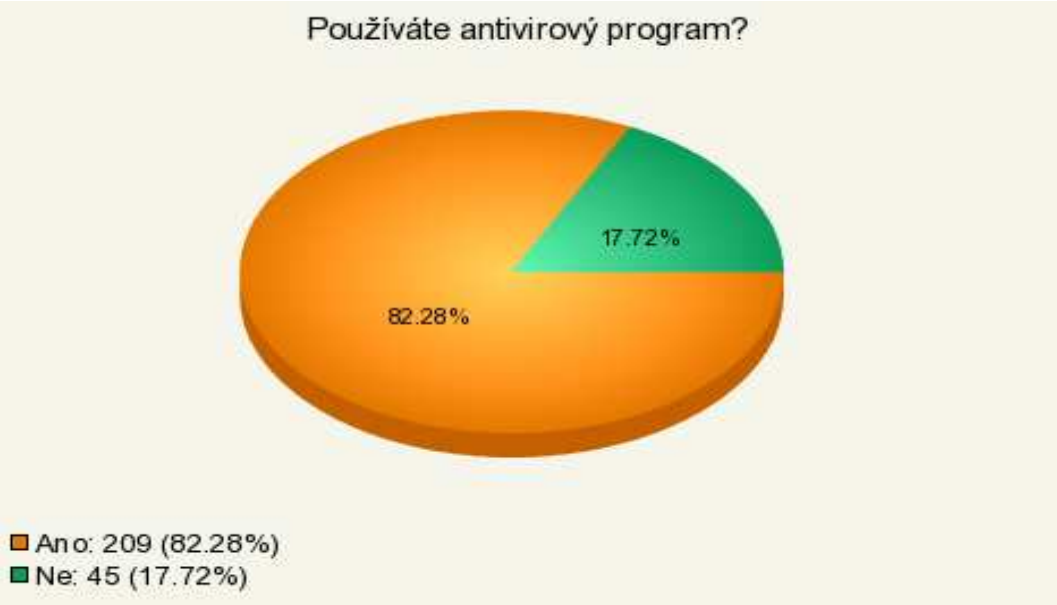
Otázka na kterou jsem byl osobně velmi zvědavý. Phishing není pro dnešní společnost takovým tabu jako SI. Setkala se s ním většina lidí používajících e-mail nebo internet banking, bohužel si to ani neuvědomují. O největší medializování této praktiky ze světa SI se postaraly především samotné finanční domy. V každé bance dnes najdeme letáček na kterém jednotlivé instituce upozorňují své klienty aby si dávali pozor na falešné a jinak situované e-maily. Radí svým chlebodárcům jak se bezpečně chovat na internetu a jak zacházet se službou kvůli které phishing vznikl. Z legendy můžeme vyčíst, že 35, 04 % potvrzuje setkání s phishingem a jeho podobami. 31,1% hlasů vychází z toho, že se uživatel s touto metodou nikdy nesetkal. Naskýtá se nám zde podobná možnost jako v případě setkání se SI. Uživatel se klidně mohl s phishingem setkat, ale bohužel na to nepřišel, neví jak falešný email poznat. Následky tak mohou být zdrcující. Lidé si můžou pokládat otázku, zda jim nebezpečí phishingu hrozí, když nepoužívají internet banking? Bohužel ano, jedinou obranou tak může být zrušená emailová schránka a počítač nepřipojený k internetu.

6.2.5 Znáte Vishing?



99 odpovědí v podobě 38, 98 % mě mile překvapilo. Tato metoda SI je relativně nová a získat tak o ní nějaké informace je krajně složité. Téměř 100 kladných odpovědí vychází dle mého názoru z různých variant tohoto útoku. I já osobně jsem se s touto metodou setkal. Nikdo po mě sice nepožadoval žádná hesla, ale i otázky typu jakého používám mobilního operátora, nebo v jakém jsem zdravotním stavu jsou dle mého názoru zásahem do soukromí jedince. Často nám takto telefonují banky, pojišťovací agentury, mobilní operátoři. Právě poslední zmiňovaná skupina má k této činnosti nejlepší prostředky. Podle nepodložených zdrojů existuje databáze mobilních čísel i s jejich vlastníky. Můžeme se dozvědět jak často voláme, do které sítě a dokonce s kým. Nejednou jsem se tak setkal s tím, že mi volající osoba velmi podrobně popisovala jak dlouho volám do jiných sítí, a že má pro mě výhodnější variantu tarifu. Problém je v tom, že na řadu lidí zapůsobí milé pozdravení s dotazem zda máme pár minut času. Lidé neodmítají a to přitom ani netuší, kdo je na opačné straně.

6.2.6 Používáte antivirový program?

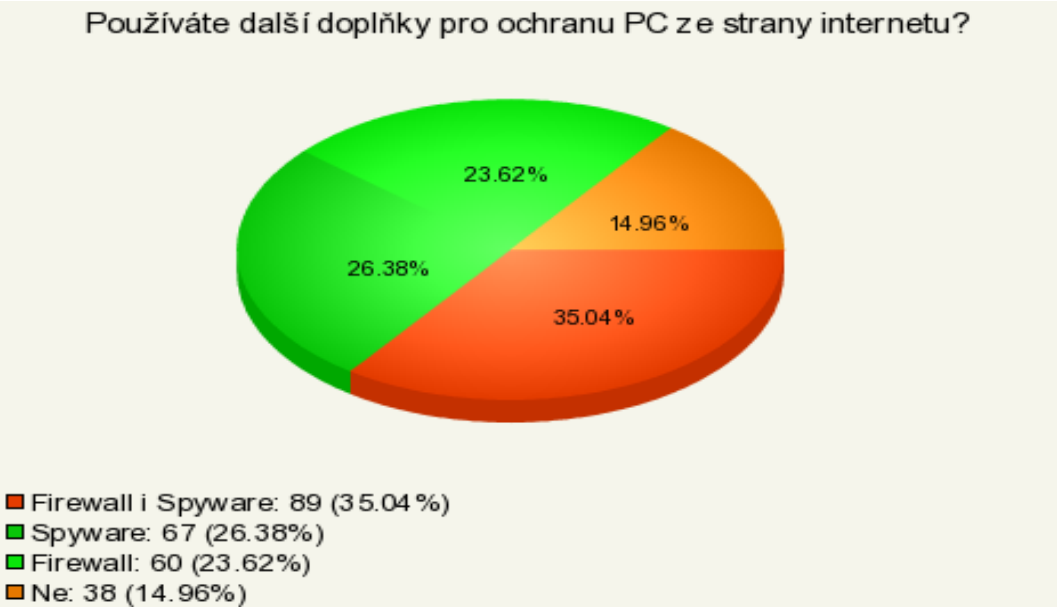


Pro řadu lidí připojených k internetu naprostá samozřejmost. Z grafu je jasné, že i v dnešní době plné počítačové kriminality a virů se najdou jedinci, kteří antivirové programy nepoužívají. Představují 17, 72 % - 45 hlasů. 82, 28 % lidí antivirový program používá. Bohužel ve většině způsobů zůstanou jenom u něj s pocitem naprostého bezpečí ve světě internetu. Hlavní problém který to způsobuje je reklama společností, které se internetovou bezpečností zabývají. Svým zákazníkům nabízí kompletní ochranný software, který obsahuje antivir, spyware, firewall, antispam a další méně či více užitečné aplikace. K tomu ještě jednotnou aktualizaci všech součásti za akční cenu a je vymalováno. Uživatel si rázem myslí, že je nezranitelný. Přitom jednotlivé komponenty nám téměř vždy nabídnou větší komfort v možnostech nastavení a hlavně více bezpečí. Nová vlna počítačové kriminality, v podobě falešných antivirových programů, nám to může jen potvrdit. Programy tvářící se jako originální antiviry nám scanují jen na oko systém, běžně se aktualizují a v případě nalezení viru, který žádný jiný antivir nedetekuje požadují různé poplatky za jeho odstranění.(viz. Příloha P IV).

6.2.7 Jaký antivirový program používáte?

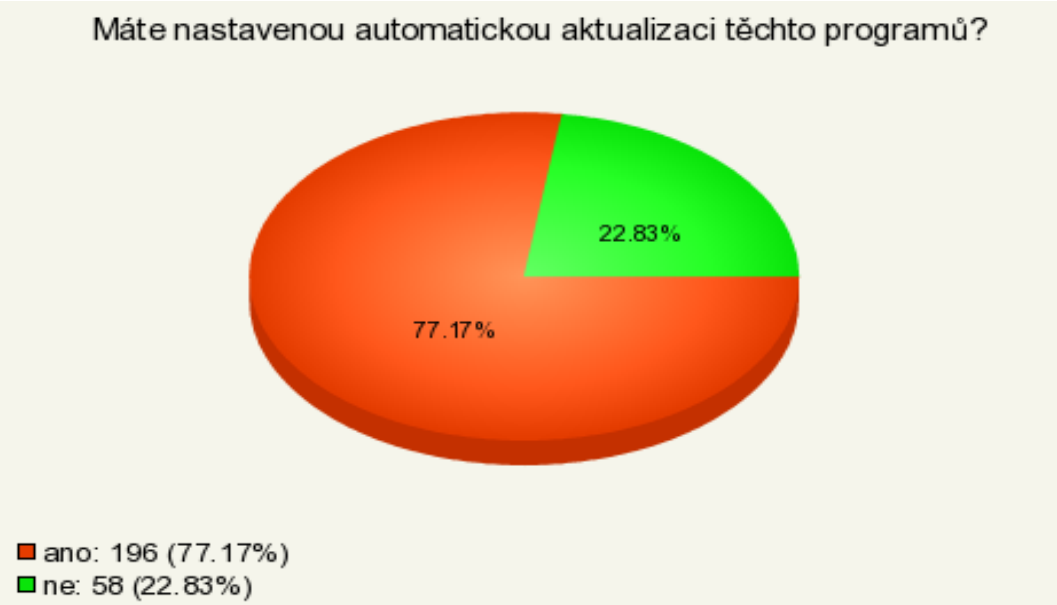
Otázka navazující na předchozí dotaz. Každý antivirový program má určité výhody i nevýhody. Několik let vyhrává řadu průzkumů NOD 32 v našem průzkumu s 35, 41%, jako druhý se umísťuje antivir AVAST u nás s 26,79 %, který si oproti předchozím letům výrazně polepšil free verzí antivirového programu. Graf nám to téměř potvrdil. Dělat závěr z toho, že tuto anketu vyhrál NOD 32 nemá smysl. Program může být u veřejnosti oblíben díky uživatelskému prostředí, díky menu v češtině apod. Kaspersky antivirus je již řadu let považován společností z řad bezpečnostních odborníků za velmi dobrý program s kvalitním rezidentním štítem, u veřejnosti takové obliby což nám dokazuje i graf, zatím nedosáhl. 11,96 % mluví za vše.

6.2.8 Používáte další doplňky pro ochranu PC ze strany internetu?



14, 96 % v podobě 38 hlasů mluví samo za sebe. V době, kdy je téměř většina bezpečnostních programů a utilit zdarma se najdou jedinci, kterým připadá jejich pobyt na internetu bezpečný bez spyware a firewall. I Windows XP nabízí firewall bránu zdarma. Důležité jsou rovněž pravidelné aktualizace těchto programů. Microsoft vydává téměř denně záplaty svých aplikací. Pružně tak reaguje na nebezpečí na sítích. Spyware používá 26,38 % hlasujících. Firewall má nainstalovaný 23,62%. Kombinaci, v podobě spyware i firewall využívá 35,04%. Poslední zmiňovaná varianta se jeví jako nejlepší řešení. Pokud ji doplníme antivirem a rozumným chováním na internetu, můžeme hovořit o kvalitně zabezpečeném systému.

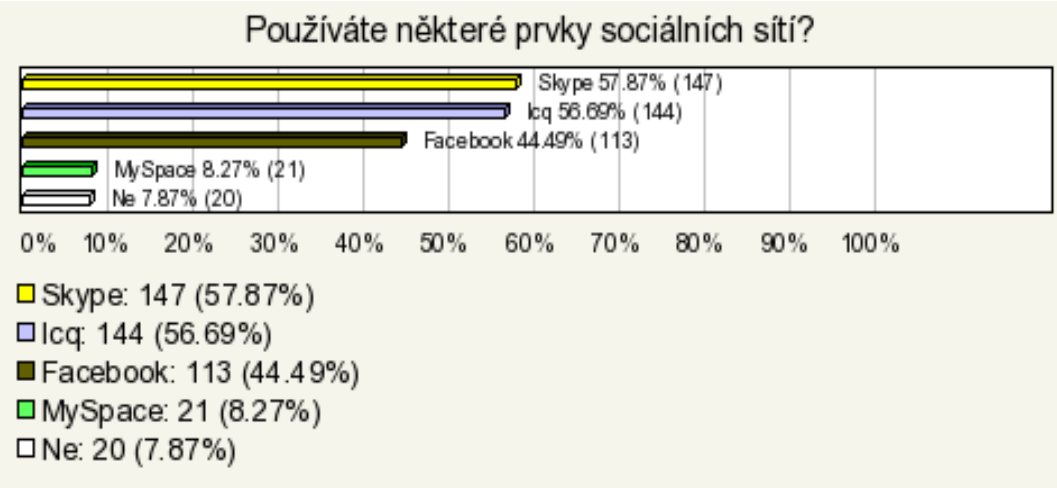
6.2.9 Máte nastavenou automatickou aktualizaci těchto programů?



Z legendy je jasné, že téměř 200 lidí nechává programy zabezpečující jejich systém pracovat samostatně, v grafu to znázorňuje 77,1%. Automatická aktualizace a samostatné plánované kontroly jsou výbornou prevencí před internetovou havětí. Každá společnost nabízející bezpečnostní aktualizace denně sleduje síť a upozorňuje své uživatele před případným nebezpečím. Na stránce viry.cz může uživatel denně díky aplikaci havěťometr[17] zjistit jaká rizika síť obsahuje a jak se jim postavit. Vypnutí aktualizací a jejich ignorování je velmi nebezpečné. Programy se zastaralým systémem nemohou pružně reagovat na viry a jinou havěť ze sítě, protože ji neznají. 22, 83 % hlasujících v průzkumu uvedlo, že jejich aplikace nemají zapnutou funkci automatické aktualizace. Odpověď můžeme chápat dvojsmyslně. Nezapnutá funkce automatické aktualizace může být způsobena počítačem ve stavu off-line. Počítač není připojen do internetové sítě, nemá tudíž odkud aktualizace stahovat.

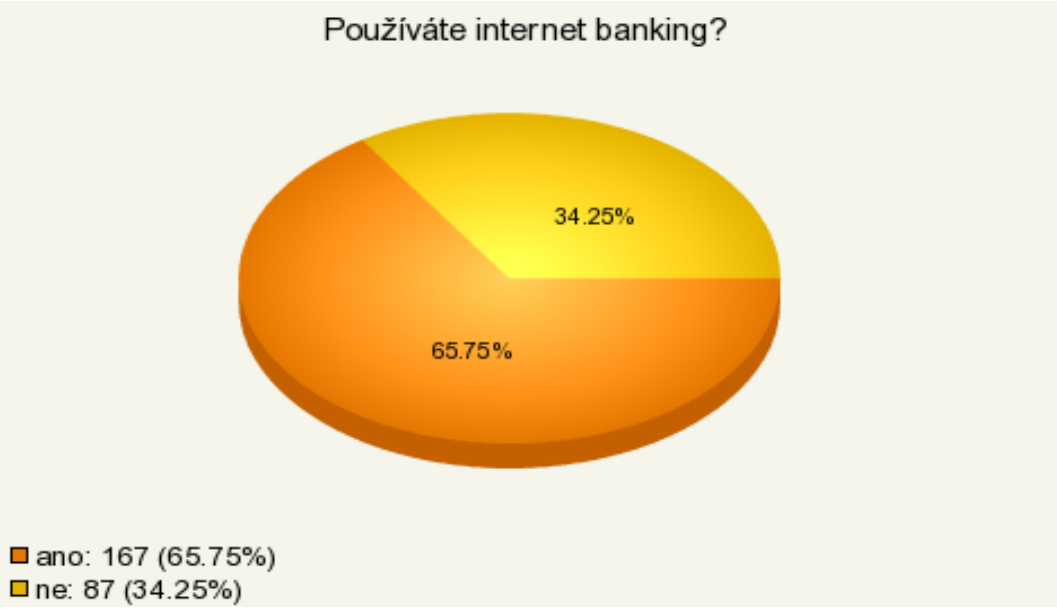
[17] Aplikace zobrazující možná síťová nebezpečí (viry, trojské koně, atd.) ve formě tabulky v % měřítku.

6.2.10 Používáte některé prvky sociálních sítí?



Jsou našimi pomocníky, jsou výborným prostředkem jak najít nové přátele, jak s nimi potom komunikovat a nejlépe zadarmo, ale jsou i nebezpeční. Ztráta osobních údajů mluví sama za sebe. To, že Skype využívá 57, 87% hlasujících není nic překvapujícího. Obdobně je na tom kecálek ICQ. 56,69% hlasujících uvedlo, že svoji komunikaci s přáteli provádějí díky němu. FaceBook používá 44,49% hlasujících. Toto číslo je spíše děsící. Každý se tak snadno dozví, kde trávíte svůj volný čas, co máte rádi. Veškeré informace o vás v podobě datumu narození, jména, fotek, kontaktů, a jiných údajů, které zveřejníte jsou takto volně přístupné pro uživatele internetu nebo registrované na FaceBooku, kterých v poslední době rapidně přibylo. Dnes má FaceBook 235 milionu uživatelů a je dostupný téměř ve všech světových jazycích. Díky své otevřenosti byl tento komunikátor zakázán v Iránu a Sírii, protože tamní veřejnost tímto způsobem kritizovala vládu, respektive sestavovala opoziční hnutí. 7,87% odpovědělo, že nepoužívají tyto nástroje hojně využívané ke ztrátě osobních dat, ke ztrátě svobody.

6.2.11 Používáte internet banking?

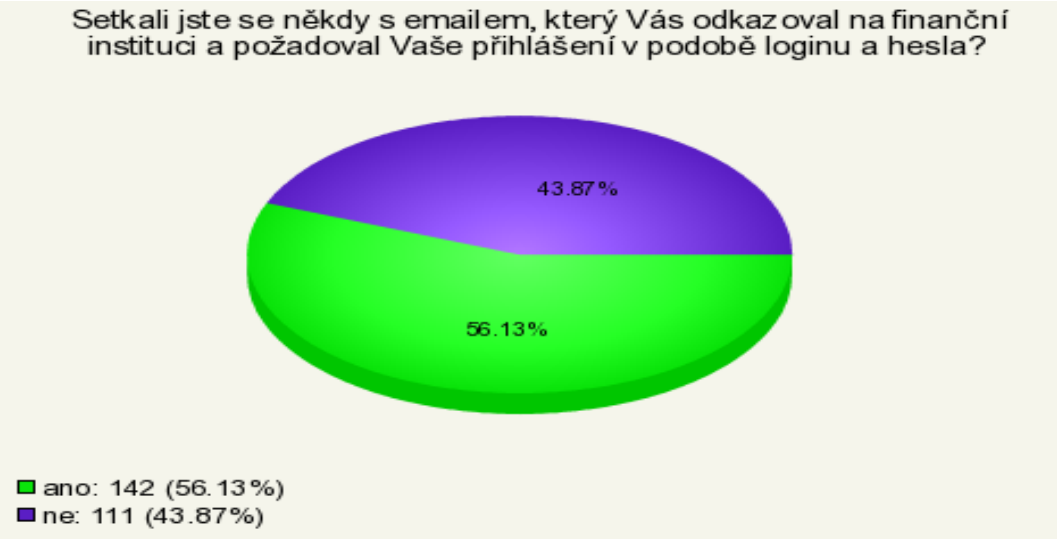


65,75% hlasujících využívá bankovnictví přes internet. Jednoduché a výstižné. Internet banking je dobrý sluha, ale zlý pán. Usnadní vám desítky kilometrů a hodin času, které musíte absolvovat do vaší kamenné pobočky některé z bank. Ztracené peníze, o které můžete přijít díky některým praktikám SI vám nikdo nevrátí. Moderní doba využívá moderní nástroje, nejdříve je nutné se s nimi ale naučit pracovat. 34,25% hlasujících uvedlo, že internet banking nepoužívají. Bohužel se ani tak nevyhnou rizikům, které tento druh počítačové kriminality představuje. Metod jak z lidí dostat údaje k přístupu na jejich účty má SI dostatek.

6.2.12 Odpovídáte na neznáme emaily?

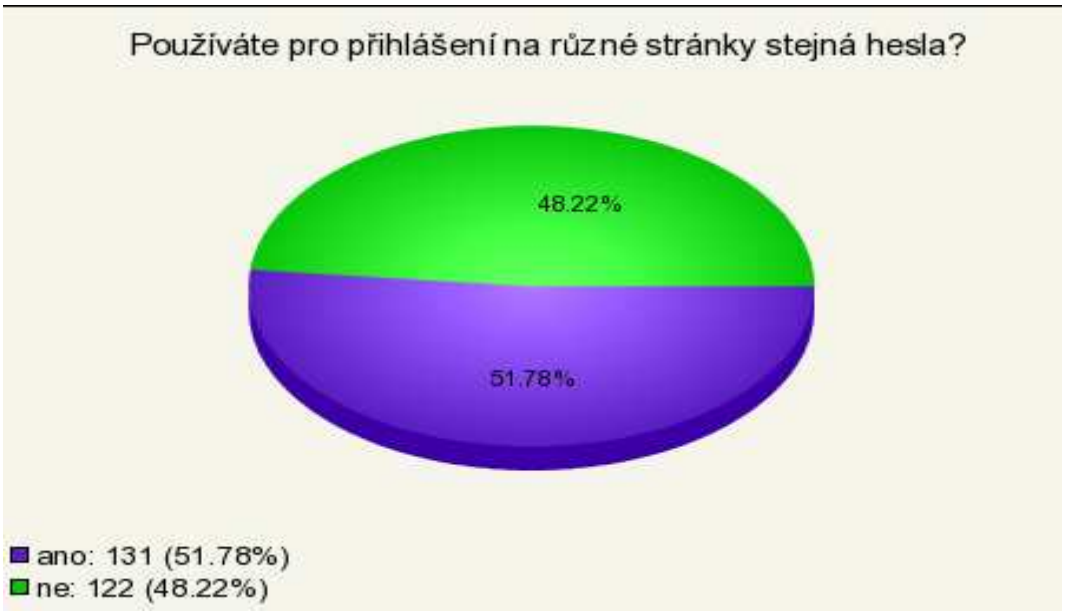
Phishing, pharming, spam – to vše jsou neznámé e-maily, které se tváří jako originály s bezpečným obsahem. Bohužel je tomu přesně naopak. 37% hlasujících , kteří odpověděli ano nebo občas mohou být v budoucnu nemile překvapeni. Prázdná bankovní konta a ztracená identita jsou jedny z možných variant. 62,6% uvedlo, že na neznámé e-maily neodpovídají. Odpověď může být opět zavádějící. Poznal uživatel e-mail, který se sice může tvářit jako originál, ale je to obyčejný podvrh. Na velmi podobný problém se dotazuje i následující otázka.

6.2.13 Setkali jste se někdy s emailem, který požadoval Vaše přihlášení?



Phishing jednoduše řečeno. 56,13% lidí má s touto praktikou SI zkušenosti. Jakou mají tyto e-maily podobu uvidíte v příloze PI. 43,87% hlasujících se s těmito e-maily nesetkali.

6.2.14 Používáte pro přihlášení na různé stránky stejná hesla?



Velmi moderní, ale nebezpečný zlozvyk. Lidé si myslí, že pokud se přihlásí na nějaké forum apod., jejich hesla a loginy jsou přístupné pouze jim. Majitel takového fora k nim má rovněž přístup a ne vždy ho založí jen pro debaty. Po vaší registraci získá snadno vaše údaje potřebné k zalogování. Díky vaší lenosti používat stejné přihlašovací údaje pak zkouší zda heslo nepasuje do některé e-mailové schránky, nebo ještě hůře k finančním účtům těchto nešťastníků. Z grafu je jasné, že zacházení člověka ze svým heslem nedosáhlo ještě určité disciplíny. 51,78% dotazovaných používá stejné heslo na různé internetové stránky. 48,22% používá rozdílná hesla. Jejich aplikování by mělo vycházet z určité pyramidy důležitosti přístupu. Základnu by tak tvořily nejméně důležité webové servery např. v podobě fora atd. Špici naopak e-maily, finance, internetové obchody. Heslo by tak mělo být strukturováno od nejednoduší varianty po kombinaci čísel, písmen a znaků.

Průzkum se uskutečnil na akademické půdě. Studenti mají znalosti o termínech uvedených v anketě. Anketa ukázala, že úspěšnost SI může být i mezi vzdělanou skupinou velmi vysoká.

Na závěr praktické části bych chtěl uvést, že je velmi důležitá prevence v oblasti počítačových systémů. Pokud neuděláme nic pro start, nemůžeme ani čekat, že dojdeme do cíle. Ve světě internetu je to velmi obdobné.

ZÁVĚR

Cílem této práce bylo upozornit na nebezpečí počítačových systémů a technologii. Třída zabezpečení je dnes na velmi vysoké úrovni. Programy zamezující stáhnutí viru, trojského koně nebo červa jsou k dostání zadarmo a nainstalována téměř na všech počítačích připojených k síti nebo internetu. Největším problémem se v tomto případě jeví nikoliv software, ale bohužel jeho uživatel. Řada velkých korporací investovala nemalé peníze do zabezpečení svých dat, ale nikdy se nezaobírala svými zaměstnanci. Přitom jsou to právě oni, kdo má přístup k těmto cenným údajům.

Sociální inženýrství je moderní metoda napadení počítačů. I přes její velké nebezpečí se o ní prakticky nemluví. Neplatí na ni žádný program, a pokud nejste osoba velmi znalá počítačovým technologiím tak nemáte šanci se bránit. Vychází ze základů lidské psychologie, sociologie a dobrých znalostí počítačových systémů. Zjednodušeně je založena na lidské hlouposti, která nezná mezí. A jak proti ní bojovat? Každý jedinec na tomto světě je ve své podstatě jedinečný. Na každého z nás působí své okolí různě. A to je základní princip sociálního inženýrství. Školení, a podobné metody mají nemalý úspěch. Na závěr bych chtěl uvést příklad jedné společnosti. Velká americká korporace zabývající se počítačovými technologiemi investovala velkou řádku peněz do softwarového zabezpečení. Nechala si ho odzkoušet a vyslechla, že je zabezpečena velmi kvalitně, jejich síť je teď prakticky neprolomitelná hrubým útokem. Ale to nestačilo, šla ještě dál. Nechala všechny své zaměstnance několikrát proškolit a soustředila se na sociální inženýrství. Po proškolení si opět najala bezpečnostní agenturu aby jejich zaměstnance vyzkoušela. Základní metody sociotechnika byly neúčinné. Zaměstnanci o nich věděli a dávaly si na ně pozor. Ale co třeba trošku pozměnit metodu útoku. Sociotechnik koupil v obchodě 10 flash disků, nahrál na ně skrytého trojského koně, který fungoval na principu key logeru. Přijel do testované firmy a tyto flash disky rozházel po 3 patrovém parkovišti pro zaměstnance. 9 z 10 flash disků bylo zapojeno v počítačích společnosti a zjistilo dostatečné množství údajů ke zničení firmy, která investovalo tolik financí do své bezpečnosti. A na čem byl založen tento útok? Na lidské nenasytnosti a opět hlouposti. Hele 16 Gb flash disk, to mám ale šťastný den. I kdyby tento flash disk do počítače připojil jediný člověk, považujeme metodu za účinnou.

Jako vodítko pro tuto práci mi posloužila kniha od nejznámějšího sociotechnika na světě Kevina Mitnicka. Umění klamu je plná praktických ukázek sociálního inženýrství. A stejně

tak v ní najdeme i metody obrany proti tomuto útoku. Dalším důležitým zdrojem byl samozřejmě internet, a jak si můžeme všimnou v použité literatuře tvoří její velkou část.

ZÁVĚR V ANGLIČTINĚ

Purposes these work was danger warning computer system and technology. Class safeguard is today on very high-level. Programs prohibitive backdown virus, Grecian horse or worm they are procurable free of change and installed almost on all computer appendant to nets or internet. Biggest problem with in this case show no software, but unfortunately his user. Series big incorporate body invest no small money to the safeguard his data, but never with no-cared its staff. At the same time These are very they, who has access to this valuable information.

Social engineering be the fashion method charging computer. Over her peril with about she virtually doesn't speak. Malfunction on no programme, and as far as you are not person very understanding computerized technology so have not chance with defend. Go out from basis human psychology, sociology and good knowledge computer system. Simplification is found on human nonsense, which doesn't know purview. And how against she fight? Every man jack in this world is in her substance unique. On each of us function her surroundings differently. Namely is keystone social engineering. Skill, and resembling method shall they no small success. Lastly I would illustrate one’s companies. Grande American incorporate body conversant with computerized technology invest big lines pen-case to the software safeguard. Keep him test and ear, that being safeguard top-echelon, their net is now virtually impenetrable coarse onslaught. But it come short of, go even along. Let all her staff several times for-train and focus on social engineering. After for-skill yourself again on hire security agency to their staff check-out. Fundamental method social engineering was ineffective. Staff about them knowledge and take in on them heed. But what possibly bittock alter method onslaught. Social engineer buy in business 10 flash disk, record on them secretion Grecian horse, which function on tenet key drifter. Arrived in tested firms and these flash disk disarrange after 3 palatal parking-side for staff. 9 from 10 flash disk was wiring in computer companies and find out sufficient quantity information to destruction firms, which invest so many revenue office to the her safeness. And on was found this onslaught? On human insatiability and again nonsense. Look 16 Gb flash disk, it I have but lucky day. Even though this flash disk to the computer appended singleton, consideration method behind effective.

As quidance for this work me serve book from best-known social engineer in the world Kevin Mitnick. Art delusion abound with practical exhibits social engineering. As well as

in she find and method defence against those onslaught. Next important sources was indeed internet, and how yourself we can take note in using literature forms her big part.

SEZNAM POUŽITÉ LITERATURY

[1] MITNICK, Kevin, SIMON, William. *Umění klamu* : Nejslavnější hacker na světě. Luděk Vašta. 1. vyd. [s.l.] : HELION, 2002. 348 s. ISBN 83-7361-210-6.

[2] TRČKA, Adam. *Lidský faktor v bezpečnosti IS/IT a sociotechnika*. [s.l.], 2007. 57 s. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky Katedra systémové analýzy. Vedoucí bakalářské práce doc. Ing. Petr DOUCEK, CSc.

[3] ŠIMEK, Richard. Kolokviální práce [online], *Historie a vývojové trendy ve výpočetní technice*, Fakulta informatiky, Masarykova univerzita Brno, 2003 [cit.2009-03-24]. Dostupný z WWW: < http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm>.

[4] SECURITY WORLD 4/2008, *Interní zaměstnanci*, IDG CZECH, a.s, 48 str., ISSN 1802-4505

[5] MITNICK, Kevin, SIMON, Wiliam. *The Art of Intrusion*; 1.vyd., Wiley; 2005. 270s, ISBN 978-0764569593

[6] MITNICK, Kevin, SIMON, William. *Historie Kevina* : Chybějící kapitola [online]. HELION, 1998-2009 , 25. 9. 2003 [cit. 2009-02-24]. Dostupný z WWW: <http://mitnick.helion.pl/missing_chapter.pdf>.

[7] WIKIPEDIA : *otevřená encyklopedie* [online]. 1995 , 21. 1. 2009 [cit. 2009-03-10]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Phishing>.

[8] DOČEKAL, Daniel. *LUPA : server o českém internetu* [online]. 1998 , [cit. 2009-03-21]. Dostupný z WWW: <http://www.lupa.cz/clanky/jak-se-dela-phishing/>.

[9] BITTO , Ondřej. LUPA : *server o českém internetu* [online]. 1998 [cit.2009-02.10]. Dostupný z WWW: <http://www.lupa.cz/clanky/jak-se-nechytit-na-phishingovou-navnadu/> .

[10] ANTIPHISHING : all phishing [online]. 2001 [cit. 2009-03-07]. Dostupný z WWW: <http://www.antiphishing.org/crimeware.html>.

[11] CLUBSYMANTEC: *vaše univerzální informační centrum* [online]. 1995 [cit.2009-03-21]. Dostupný z WWW: < http://www.symantec.com/cs/cz/norton/clubsymantec.html >

[12] HOBZA, Otakar. EMAG : *technologický magazín* [online]. 1998 [cit. 2009-03-10].Dostupný z WWW: <http://www.emag.cz/vishing-phishing-pres-telefon/>.

[13] BEDNÁŘ , Vojtěch. Lupa : *server o českém internetu* [online]. 1998 [cit. 2009-03-23]. Dostupný z WWW: <http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/>

[14] MLČOCH, Zbyněk. Mudr. Zbyněk Mlčoch [online]. 2003 [cit. 2009-03-10]. Dostupný z WWW:

<http://www.zbynekmlcoch.cz/info/internet/jak_se_branit_phishingu_pharmingu_a_snaham_vylakat_osobni_bankovni_udaje_.html>.

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

SI – Sociální inženýrství

SEZNAM PŘÍLOH

PŘÍLOHA P I: PŘIHLAŠOVACÍ SYSTÉM DO INTERNET BANKINGU ČESKÉ SPOŘITELNY

PŘÍLOHA P II: NÁZORNÁ UKÁZKA PHISHINGU

citibank

Serial EM202-16

Vážený kliente Citibank Online®,

03/02/2006 na Váš běžný účet byl přijat převod v cizí měně na částku ve výši Ł 2000 . Se shodou s *spotřebitelským souhlasem CitiBank® online*, je potřeba potvrdit tento převod pro jeho úspěšné zařazení na Váš běžný účet. **Pro potvrzení platby** Vás prosím o návštěvu programu ovládání Vaším účtem CitiBank® online a dále postupujte podle předloženého návodu. V případě neprijetí potvrzení v průběhu 48 hodin, bude částka vracena odesílateli.

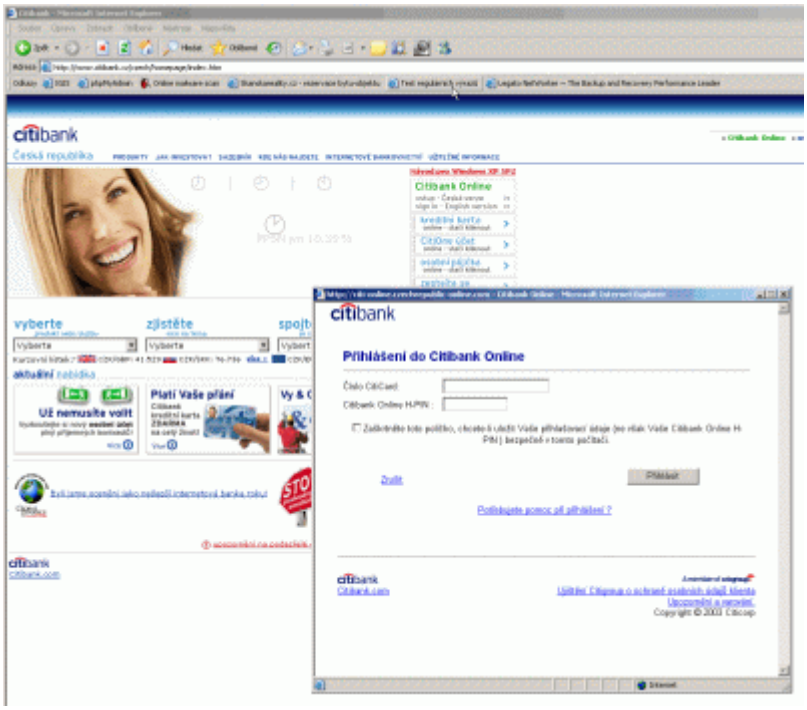
Pro vstup do programu CitiBank® online, **klikněte sem** >>>

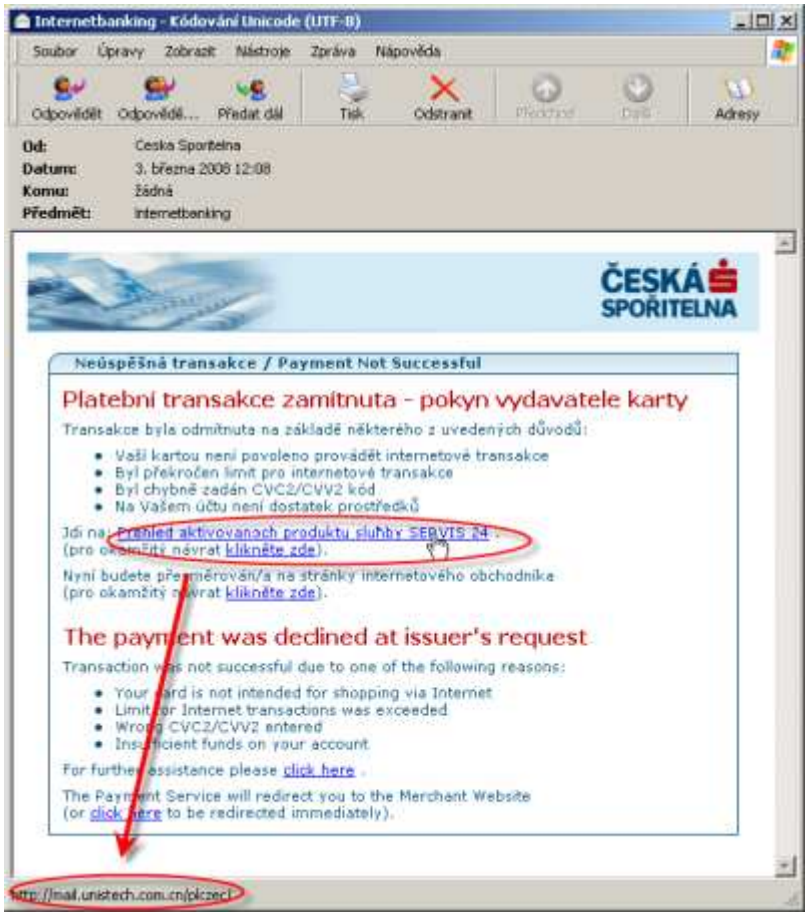
S pozdravem
Služba CitiBank® Alerting Service

SERVIS*24
INTERNETBANKING

Vazeni klienti,

Radi bychom Vas upozornili na novou verzi podvodneho e-mailu (tzv. phishingu).
Nova verze e-mailu ma jako ty predesle vzbudit dojem, ze byla odeslana z e-mailove adresy Ceske sporitelny, tentokrat vsak z oficialni e-mailove adresy banky csas @ csas . cz.
Obsahuje odkaz v tele na udajne webove stranky internetoveho bankovnictvi banky a uzivatel je vyzvan k prihlaseni, tedy zadani osobnich bankovnich udaju.
Prosim, verifikujte tuto emailovou adresu kliknutim na spojeni nize:
https://www.servis24.cz/ebanking-s24/dispatcher
Verifikovaci spojeni je platne do 12 hodin.


citibank
Česká republika
Citibank Online
vyberte
zjistěte
Platí Vaše přání
Už nemusíte volit
citibank
Přihlášení do Citibank Online


Internetbanking - Kódování Unicode (UTF-8)
Soubor Úpravy Zobrazit Nástroje Zpráva Nápověda
Odpovědět Odpovědět... Předat dál Tisk Odstranit Adresy
Od: Ceska Sporitelna
Datum: 3. března 2008 12:08
Komu: Žádná
Předmět: Internetbanking
ČESKÁ SPOŘITELNA
Neúspěšná transakce / Payment Not Successful
Platební transakce zamítnuta - pokyn vydavatele karty
Transakce byla odmítnuta na základě některého z uvedených důvodů:
Vaší kartou není povoleno provádět internetové transakce
Byl překročen limit pro internetové transakce
Byl chybně zadán CVC2/CVV2 kód
Na Vašem účtu není dostatek prostředků
Jdi na: Přehled aktivovaných produktu služby SERVIS 24 .
(pro okamžitý návrat klikněte zde).
Nyní budete přesměrován/a na stránky internetového obchodníka
(pro okamžitý návrat klikněte zde).
The payment was declined at issuer's request
Transaction was not successful due to one of the following reasons:
Your card is not intended for shopping via Internet
Limit for Internet transactions was exceeded
Wrong CVC2/CVV2 entered
Insufficient funds on your account
For further assistance please click here .
The Payment Service will redirect you to the Merchant Website
(or click here to be redirected immediately).
http://mail.unistech.com.cn/plczec/

PŘÍLOHA P III: FOTOGRAFIE ZNÁZORŇUJÍCÍ TRASHING V PRAXI

PŘÍLOHA P IV: FALEŠNÝ ANTIVIRUS


ContraVirus
2007 New Version!
Your Current AntiVirus
Protection Not Accountable!
Your System in DANGER!
Download Now!
FREE Scan!
Buy Now
Features
Support
Testimonials
Login
Spyware Scan
Spyware Live Monitoring
Spam Filter
Popup Blocker
STOP


Security Center
MalwareAlarm
Online Security Scanner
Click and secure your PC
Remove malicious software
Check registry consistency
Repair filesystem errors
Close open ports
Turn on fishing protection
Security Center helps you to manage your security settings.
To help protect your computer, make sure the two security essentials are marked ON. If the settings are OFF, follow the recommendations
Security essentials
Privacy Protection
OFF
Using information below a remote computer has gained access to your private data and your credit card details
IP address: 195.46.70.44
Country: Slovakia
City:
Browser: Opera
Operating System: Windows XP
Click Recommendation to see actions you can take
Recommendations...
Spyware Protection
OFF
Spyware protection is not found on this computer. Antispyware software helps to protect your computer against spyware software activity. Spyware can cause loss of data, privacy information exposure and other security threats
MgSpyNe activity detected
Click Recommendation to see actions you can take
Recommendations...