

Sociální inženýrství

Social engineering

Martin Pomykal

Bakalářská práce
2012



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Martin POMYKAL**
Osobní číslo: **A09599**
Studijní program: **B 3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Sociální inženýrství**

Zásady pro vypracování:

1. Provedte literární rešerši týkající se sociálního inženýrství.
2. Definujte nejčastější sociotechniky používané v současnosti.
3. Uvedte typické ukázky sociálních útoků.
4. V praktické části vypracujte rady a postupy obrany proti sociálnímu inženýrství.
5. Vypracujte a vyhodnoťte anketu, která zjistí povědomí veřejnosti o sociálním inženýrství.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. MITNICK, Kevin. Umění klamu. Vyd. 1. Gliwice: Helion, 2003, 348 s. ISBN 83-736-1210-6.
2. VÍTEK, Miloš a Marcela VÍTKOVÁ. Sociální vědy a inženýrství. Vyd. 1. Hradec Králové: Gaudeamus, 2004, 164 s. ISBN 80-704-1474-X.
3. JAŠEK, Roman. Informační a datová bezpečnost. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 80-731-8456-7.
4. MITNICK, Kevin D a William L SIMON. The art of deception: controlling the human element of security. Indianapolis, Ind.: Wiley, c2002, 352 s. ISBN 07-645-4280-X.
5. TRČKA, Adam. Lidský faktor v bezpečnosti IS/IT a sociotechnika. Praha, 2007. Dostupné z: https://www.vse.cz/vskp/show_evskp.php?evskp_id=2403.
Bakalářská práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky, Katedra systémové analýzy. Vedoucí práce prof. Ing. Petr Doucek, CSc.

Vedoucí bakalářské práce:

Ing. Jiří Vojtěšek, Ph.D.

Ústav řízení procesů

Datum zadání bakalářské práce:

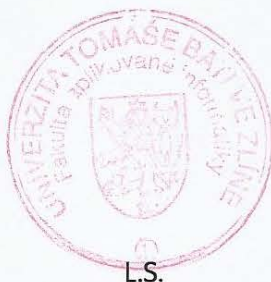
24. února 2012

Termín odevzdání bakalářské práce:

25. května 2012

Ve Zlíně dne 6. února 2012

prof. Ing. Vladimír Vašek, CSc.
děkan



L.S.

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Práce řeší obecný pohled na sociotechniku a její definici. Jsou v ní popsány nejčastější útoky sociálního inženýrství, které se v dnešní době objevují jak v prostředí internetu, tak i ty, které vyžadují fyzický pohyb. V práci jsou uvedeny příklady útoků jak z minulosti, tak i z přítomnosti, což jenom potvrzuje, že sociotechnika není hudbou minulosti, ale je to problém stále aktuální a závažný. Práce obsahuje vyhodnocenou anketu, která se zabývala povědomím lidí o sociálním inženýrství. Součástí je také vypracovaná prezentace pro vedoucí pracovníky, kteří budou seznamovat své zaměstnance s nebezpečím sociálního inženýrství.

Klíčová slova: Phishing, Vishing, Baiting, Pharming, Sociální inženýrství, Mitnick

ABSTRACT

The work solves the common view of the social engineering and its definition. The most frequent social engineering attacks are described in, the ones which appears today in the internet, as those that require physical movement. The work presents examples of attacks from the past and from the present, which only confirms that social engineering isn't the music of the past, but the problem is still actual and serious. The work contains evaluation a poll which looked at people's awareness of social engineering. Also include a presentation prepared for managers who will familiarize their employees with the dangers of social engineering.

Keywords: Phishing, Vishing, Baiting, Pharming, Social engineering, Mitnick

Na tomto místě bych rád poděkoval vedoucímu mé bakalářské práce Ing. Jiřímu Vojtěškovi, Ph.D. za odborné vedení, podmětne rady a připomínky, které mi poskytoval během vypracování této práce. Rád bych také poděkoval mým rodičům, sestře a také přítelkyni, kteří mě během studia podporovali.

Motto:

Kdo chce, hledá způsoby. Kdo nechce, hledá důvody.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD	9
I TEORETICKÁ ČÁST	10
1 OBECNÝ POHLED NA SOCIOTECHNIKU	11
1.1 DEFINICE SOCIOTECHNIKY	11
1.2 SILNÉ STRÁNKY SOCIOTECHNIKY	11
1.3 KEVIN MITNICK	11
2 PRAKTIKY SOCIÁLNÍHO INŽENÝRSTVÍ	13
2.1 PHISHING	13
2.2 VISHING.....	13
2.3 TRASHING.....	13
2.4 PHARMING	14
2.5 CLICKJACKING	14
2.6 TABNABBING.....	14
2.7 BAITING.....	15
2.8 FYZICKÁ SOCIOTECHNIKA.....	15
2.9 PRETEXTING.....	15
3 UKÁZKY ÚTOKŮ SOCIOTECHNIKOU	17
3.1 AVONET.....	17
3.2 KOMERČNÍ BANKA	18
3.3 ČESKÁ SPOŘITELNA	19
3.4 TABNABBING.....	21
3.5 TWITTER.....	22
4 NOVÉ TRENDY V SOCIOTECHNICE.....	23
4.1 FACEBOOK.....	23
4.2 TWITTER.....	25
II PRAKTICKÁ ČÁST	27
5 ANKETA	28
5.1 VYHODNOCENÍ ANKETY	28
5.1.1 Co je to sociální inženýrství?	28
5.1.2 Kde jste se setkali se sociálním inženýrstvím?	29
5.1.3 S jakou formou jste se už setkali?	30
5.1.4 Sociotechnika se zabývá?	31
5.1.5 Phishing je?	32
5.1.6 Pro sociotechniku jsou vhodné znalosti?	33
5.1.7 Na útok sociotechnikou je náchylná?	34
5.1.8 Kolik různých hesel používáte pro autentizaci?.....	35
5.1.9 Jaká hesla využíváte pro přístup k serverům využívajících autentizaci?.....	36
5.2 VYHODNOCENÍ SPRÁVNÝCH ODPOVĚDÍ	36
6 OBRANA PŘED ÚTOKY SOCIÁLNÍM INŽENÝRSTVÍM.....	37

6.1	PHISHING	37
6.2	VISHING.....	37
6.3	TRASHING.....	37
6.4	PHARMING	38
6.5	CLICKJACKING	38
6.6	TABNABBING.....	38
6.7	BAITING.....	38
6.8	FYZICKÁ SOCIOTECHNIKA.....	39
6.9	PRETEXTING.....	39
7	NÁVRH ŠKOLENÍ PRO VEDOUCÍ PRACOVNÍKY	40
7.1	PHISHING	40
7.2	VISHING.....	40
7.3	TRASHING.....	40
7.4	PHARMING	41
7.5	CLICKJACKING	41
7.6	TABNABBING.....	41
7.7	BAITING.....	41
7.8	FYZICKÁ SOCIOTECHNIKA.....	41
7.9	PRETEXTING.....	42
	ZÁVĚR	43
	ZÁVĚR V ANGLIČTINĚ.....	44
	SEZNAM POUŽITÉ LITERATURY	45
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	47
	SEZNAM OBRÁZKŮ.....	48
	SEZNAM PŘÍLOH	49

ÚVOD

V současné době se stále setkáváme s nejrůznějšími druhy útoků sociálního inženýrství. Tyto útoky jsou vedeny na získání citlivých informací, což je to co má dnešní době velkou cenu, protože například ukradené “Know-how“ může i velkou firmu zruinovat. Jako příklad si můžeme uvést Coca-Colu, kdy její přesný recept je stále veřejnosti utajen, ovšem pokud by jej někdo získal, tak by mohlo vzniknout spoustu firem, které by vyráběly nápoj podle jejich receptu, ovšem prodávaly by jej za mnohem nižší cenu, čímž by jim odlákaly spoustu zákazníků hlavně těch, co se zaměřují na cenu a kterých je v dnešní době většina.

Mnoho lidí však zná jenom phishing a to protože už se s ním setkalo a uvědomili si, že se o něj jedná a to z důvodu, že se o něm mluví v médiích. Je to avšak pouze jeden z mnoha útoků, které nás v dnešní době ohrožují a chtějí od nás získat důvěrné informace. Tyto útoky nejsou pouze hrozbou dnešní doby, ale jsou tu s námi již mnoho desetiletí.

Dříve neprobíhaly útoky na internetu, protože ten ještě neexistoval a jeho předchůdce propojoval pouze několik málo počítačů na světě, ale lidé se mohli s útočníky setkat osobně. Jako například s mladým Kevinem Mitnickem, kterému před více než 40 lety stačilo pouze chytře formulovat otázky, aby z řidiče autobusu získal informaci, kde si může pořídit stroj na označování lístků a jezdit tak městskou dopravou zadarmo. [1]

S rozvojem internetu se rozšířily jak druhy útoků, tak se i mnohonásobně zvedl počet útočníků, protože ty pro ně nejsou díky internetu tak riskantní, přece jenom jejich oběť se může nacházet na jiném světadílu a tím je riziko například fyzické konfrontace minimální.

Obranou před těmito útoky je jak prevence, tak i samotné seznámení uživatelů s útoky které na ně můžou být vedeny. Protože těžko se brání proti něčemu, co neznám, ovšem když už mám aspoň malý přehled o rizicích, tak se jim již dokáži lépe čelit.

I. TEORETICKÁ ČÁST

1 OBECNÝ POHLED NA SOCIOTECHNIKU

1.1 Definice sociotechniky

Sociální inženýrství, jinak taky zvané sociotechnika, je ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že útočník je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Díky tomu je schopen využít lidi, se kterými hovoří, případně dodatečné technologické prostředky k tomu, aby získal hledané informace. [1]

Sociální inženýrství vychází z myšlenky, že je mnohem jednodušší přinutit někoho, kdo heslo zná, aby nám ho prozradil, než jej prolamovat pomocí útoku hrubou silou (brute force attack)¹. Navíc při dobře vedeném útoku si oběť v drtivém případě vůbec neuvědomí, že byla okradena o cenné informace.

1.2 Silné stránky sociotechniky

Pokud je útočnickovým cílem získání přihlašovacích údajů, tak je pro něj nejvýhodnější pokud uvede oběť to časové tísň. Ta u oběti vyvolá stresovou situaci, kdy se musí během chvíle rozhodnout. Proto je nutné nenechat se rozhodit a nejednat ukvapeně. Z toho důvodu nikdy nezasílat administrátorovi vaše heslo, on jej znát nepotřebuje, v případě potřeby je schopen ho resetovat a nastavit si své heslo, případně k instalaci programů bude v počítači jeho administrátorský účet, který má vyšší oprávnění než uživatel.

1.3 Kevin Mitnick

Je nejznámější a nejmedializovanější osoba, která se zabývala sociotechnikou. Nyní o něm budu citovat pár odstavců z jeho knihy [1]

Kevin Mitnick vyrůstal v San Fernando Valley, poblíž Los Angeles, a již v útlém mládí nacházel zajímavé způsoby, jak dělat věci, které se „normálně nedělají“. Například jezdit městskými autobusy zcela zadarmo, přelstít veřejnou telefonní síť a telefonovat zdarma nebo různě přepojovat cizí hovory. Nebo přišel na způsob, jak proniknout do počítače společnosti DEC. Zajímavé ale je, že k tomu využíval jak svých znalostí a technické dovednosti, tak především schopnosti manipulovat s lidmi; uvést je v omyl, ovlivnit a

¹ Systematické zkoušení všech možných kombinací hesla případně omezené množiny, například pouze čísel.

přesvědčit k vykonání něčeho ve svůj prospěch, co by tito lidé za normálních okolností vůbec neudělali. Například zmiňovaný průnik do počítače firmy DEC provedl mladý Kevin Mitnick tak, že zavolal administrátorovi systému a vydával se za jednoho z hlavních programátorů tak přesvědčivě, že mu uvěřili a poskytli potřebné údaje pro přístup a ještě ho nechali nastavit si vlastní heslo.

S postupem času Kevin Mitnick tuto svou schopnost manipulace s lidmi dále rozvinul a povýšil na svou hlavní zbraň. Začal ji označovat jako „social engineering“ (podle českého překladu knihy: „sociotechnika“) a i dnes se jako červená nit táhne celou jeho knihou. Ostatně, výmluvný je už samotný název knihy, stejně jako hlavní zjištění, které je v knize obsažené: nejslabším článkem v každém bezpečnostním systému jsou lidé. To prý Kevin Mitnick zjistil, už když mu bylo 17 let.

Výčet a popis dalších útoků dospívajícího a dospělého Kevina Mitnicka se většinou liší podle toho, zda je popisuje on sám, nebo bulvárnější či méně bulvární média, případně zda jde o vyšetřování „orgánů činných v trestním řízení“. Měl se například nabourávat do ústředí mezinárodních korporací či dokonce do počítačů Velitelství vzdušné obrany Severní Ameriky (NORAD), které ale vůbec nejsou připojeny k žádné externí veřejné síti. Taktéž měl mít přístup k obchodním tajemstvím v hodnotě milionů dolarů. Také je mu připisováno, že odcizil data týkající se nejnovější generace elektronických zabezpečení a supertajných nástrojů, používaných bezpečnostními orgány.

Svého času byl jednou z nejhledanějších osob v historii FBI. V roce 1995 byl skutečně zatčen a hrozilo mu několik set let odnětí svobody. Ve vazbě strávil čtyři a půl roku, kdy nakonec odešel s pětiletým trestem a pokutou ve výši 4 150 USD. Proč tak velká disproporce? Pravděpodobně proto, že vyšetřující soudní orgány zpočátku nevěděly, jak ohodnotit, co vlastně Kevin Mitnick svými průniky spáchal a jak velkou škodu skutečně natropil.[2]

2 PRAKTIKY SOCIÁLNÍHO INŽENÝRSTVÍ

V této kapitole se zaměřím na seznámení s nejčastějšími druhy sociotechnik a to jak prováděných přes počítač, tak i útoky prováděné přes telefon, případně přímo fyzickému útoku.

2.1 Phishing

Je podvodná technika hojně využívaná na internetu k získání citlivých informací od uživatele. Principem phishingu je typicky rozesílání e-mailových zpráv nebo instant messaging (internetová služba pro zasílání textových zpráv v reálném čase), které často vyžívají adresáta k zadání osobních údajů na falešnou stránku, jejíž podoba je takřka identická s tou oficiální. Stránka může například napodobovat přihlašovací okno internetového bankovníctví. Uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze. [4]

2.2 Vishing

Obdobou phishingu, kdy útočník k útoku využívá navíc ještě telefon či telefonování přes internet (VoIP). V případě takového útoku obdržíte e-mail nebo SMS zprávu s žádostí abyste zavolali na bezplatné telefonní číslo a potvrdili své údaje. Nebo obdržíte nahranou telefonickou zprávu s žádostí o zadání údajů k vašemu bankovnímu účtu. Pokud tyto informace poskytnete, je velká pravděpodobnost, že z účtu budou velmi rychle převedeny všechny prostředky někam do zahraničí a vám zbude pouze prázdné konto.

Pokud Vám tedy někdo bude volat a bude Vás milým a vstřícným hlasem informovat o vzniklém bezpečnostním problému s Vaším bankovním účtem a přesvědčovat Vás, abyste volali například na jejich telefonní číslo z důvodu například reaktivace kreditní nebo platební karty, bude vám hned jasné, že se něco děje.[3]

2.3 Trashing

Je druh útoku, který už je mnohem náročnější než předešlé a to z důvodu, že už je nelze provést z „tepla domova“ ale je nutné vyrazit do terénu. Už sám název napovídá, o co se bude jednat. Trash v angličtině znamená koš. Čili trashing je prohledávání se odpadky ve snaze získat citlivé informace jako například výpisy z účtu, ve kterých útočník zjistí potřebné informace proto, aby byl jeho vishingový útok mnohem důmyslnější. Snaha o

recyklaci a tím i vyhrazené kontejnery pro papír, tento útok mnohem zjednodušuje, jelikož útočník se nemusí prohrabávat množstvím odpadků.

2.4 Pharming

Útok prováděný v prostředí internetu, kdy principem je napadení DNS serveru a přepsání IP adresy na kterou má být proveden překlad doménového jména. Což znamená, že nic netušící oběť se ve snaze dostat na internetové bankovníctví rázem ocitne na úplně jiné stránce, která ale vypadá úplně stejně jako stránka jeho banky, rozdíl je ovšem v tom, že přihlašovací údaje nejsou porovnány s údaji banky, ale jsou uloženy do databáze útočníka, který je využije ke svému obohacení.

2.5 Clickjacking

Je útok vedený na uživatele webových stránek, kdy při běžném prohlížení zdánlivě neškodné stránky spustí akci, kterou nečekali, například kdy při kliknutí na obrázek neklikne na něj, ale na průhledný odkaz, který je umístěn nad ním, ale má průhlednou barvu. Čímž může například uživatel povolit snímání webkamery, zadat k tisku značné množství stránek atd.

Clickjacking je odborně definován v [10]:

Zákeřná stránka na doméně A vytvoří iframe² směřující na doménu B, do které je uživatel aktuálně přihlášen pomocí cookies³. Stránka skryje jinými prvky větší část iframe, až na jedno jediné tlačítko na doméně B, např. „Smazat vše“, „Přidej Boba jako svého přítele“ apod. Může přidat své rozhraní pro oklamání uživatele, který si myslí, že tlačítko patří do domény A klikne na něj. Ačkoliv jsou uvedené příklady naivní, jedná se o jasný problém pro celou řadu moderních aplikací.

2.6 TabNabbing

TabNabbing využívá nepozornosti uživatele, který si při běžném prohlížení otevírá více záložek v prohlížeči. Často má pak uživatel ve zkratkách zmatek, čehož využije útočník,

² Umožňuje na webové stránce vymezit plochu pro vložení jiné webové stránky

³ Malé množství dat, kterými se prohlížeč autentizuje webovému serveru po prvotním přihlášení

kdy pomocí nastrčeného skriptu čeká, až uživatel přepne na jinou záložku, poté skript změni ikonku webu v záložce a také obsah stránky, aby vypadal jako například přihlašovací stránka e-mailu na seznamu. Adresa sice zůstala původní, ale toho si uživatel často nevšimne. A jelikož měl uživatel otevřených mnoho záložek, tak si už nepamatuje, zda mezi nimi byl i e-mail, takže zadá přihlašovací údaje. Tyto údaje putují jak na útočnickův server, tak i uživatele přesměrují na skutečný e-mail, aby nepojal podezření a nezměnil si například heslo, pak by tento útok pozbýval smyslu. [11]

2.7 Baiting

Baiting lze považovat za útok pomocí trojského koně v reálném světě. Útok je vedený přes fyzická média jako jsou CD/DVD nebo USB paměti a tyto média útočník zanechá na místech, kde se vyskytuje mnoho lidí, jako jsou například fast foody, výtahy atd. Poté už stačí pouze zvědavost oběti, která neodolá zvědavosti a nalezené médium strčí do počítače. Čímž dojde k infekci a otevření zadních vrátek pro útočníka. U nepopsaných nosičů mají větší úspěšnost USB paměti, kdy si ji oběť vezme s tím, že ji zformátuje a bude používat. Ovšem atraktivnost DVD lze zvednout pouhým popsáním, kdy například stačí na krabičku napsat „Výplaty leden“ a každý ve firmě bude hořet zvědavostí, aby zjistil jaký plat má jeho kolega. [6]

2.8 Fyzická sociotechnika

Útočník se vydává za nového zaměstnance firmy a využívá toho, že se ve velkých firmách znají, pouze v rámci oddělení či patra a využije důvěřivosti pracovníků firmy k získání tajných dokumentů, informací. Často také dochází ke sblížení útočníka a zaměstnance firmy v osobním životě, ale poté následnému zcizení informací, dokumentů prostřednictvím tohoto zaměstnance.

Útočník se vydává za počítačového odborníka a jde ve firmě odstranit viry z počítače, místo odvirování však naistaluje do počítače škodlivý software, který bez vědomí uživatele odesílá data na e-mail nebo FTP server útočníka.

2.9 Pretexting

Je vytváření a užívání vymyšleného scénáře, jehož cílem je přesvědčit oběť k provedení potřebné akce nebo získání informace. Jde o skloubení lživé informace s informací, která se zakládá na pravdě a byla už získána dříve. Touto informací může být například rodné

číslo, číslo účtu, jméno vedoucího atd. Kdy je cílem přesvědčit oběť o legitimnosti akce, jež je požadována. [7]

U pretextingu se útočník může také vydávat za policejního vyšetřovatele, zaměstnance finančního úřadu nebo jiného úředníka, který by mohl mít právo na dotazování dané oběti. Stačí, pokud je útočník přichystán na možné kontrolní otázky oběti, ovšem někdy stačí pouze seriózní a autoritativní tón hlasu a dostatečně přesvědčivý obsah konverzace. [6]

3 UKÁZKY ÚTOKŮ SOCIOTECHNIKOU

Tato kapitola se zachycuje útoky, které byly provedeny v České republice a to z důvodu, abychom si uvědomili, že útoky sociálním inženýrstvím nejsou doménou pouze Spojených států amerických, ale můžeme se s nimi setkat i v České republice.

3.1 Avonet

V listopadu loňského roku (2011) byly uživatelům e-mailových schránek u společnosti Avonet rozesílány podvodné e-maily, které po uživatelích vyžadovaly doplnění jejich osobních dat a přístupových údajů k e-mailové schránce. Kde pachatelům tohoto phishingového útoku šlo o získání obsahu schránek, hlavně e-mailových adres, které by byly zneužity jakožto adresáti spamu. Odhalení tohoto útoku je velmi snadné v případě, že si oběť zkontroluje odesílatele. A bude mu zřejmé, že podpora společnosti, bude těžko mít e-mail na doméně gmail.com jak vidíme na Obrázek 1

Příklad podvodného e-mailu:

From: Avonet mailovou službou <actualizareaserviciului@gmail.com>
To: undisclosed-recipients:;
Subject: Deaktivace vašeho účtu AVONET Webmail.

Deaktivace vašeho účtu AVONET Webmail.

Vezměte laskavě na vědomí, že jsme v poslední době dělali některé inovace v naší databázi. Během aktualizace došlo k neobvyklé reakci kódu z e-mailovou adresu požadující pro deaktivaci. Zkontrolujte, zda vypnout nebo si e-mailový účet aktivní.

Za účelem ověření / potvrzení vám e-identity, můžete je poskytnout tyto údaje:

Potvrzení vašeho AVONET EMAIL IDENTITY níže:

Křestní jméno : _____
Příjmení : _____
Email jméno : _____
E-mail Heslo : _____
Odebrání: (Aktivujte si prosím upřesněte) _____ (Ano Ne deaktivovat, aby aktivní.)
Důvod Deactivation _____ (pokud ano)

VAROVÁNÍ! Při selhání ověření e-mailový účet na obdržení tohoto oznámení, bude Váš účet automaticky deaktivován

Děkujeme Vám za používání našeho Webmail!

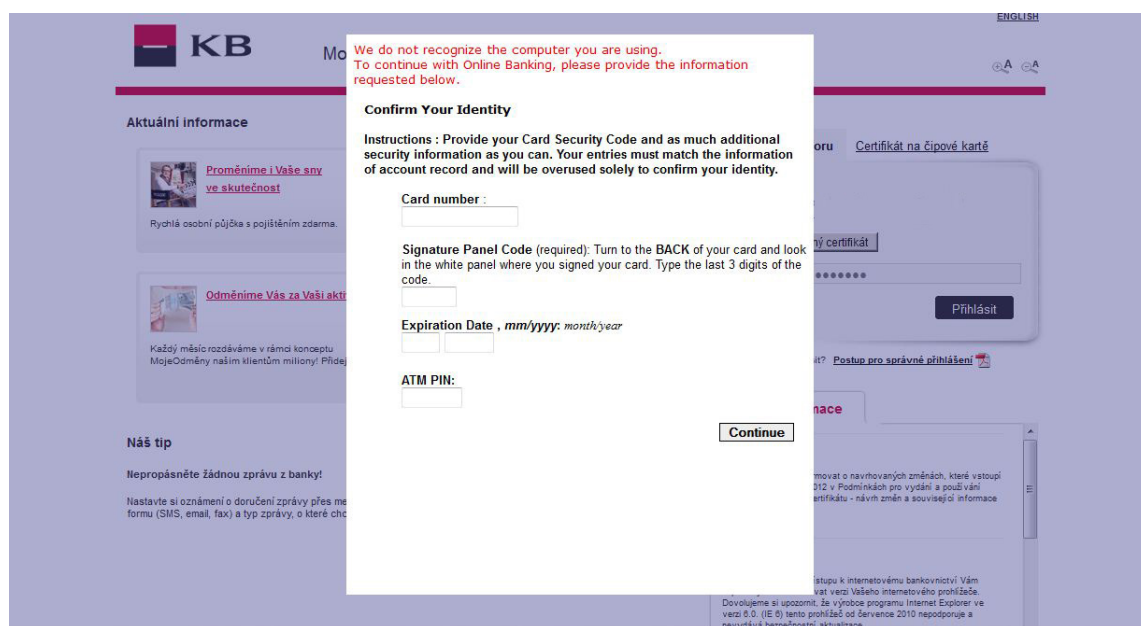
Varování Kód: ASPH8B02AXV

Se srdečným pozdravem,
AVONET Webmail služeb řízení týmu.
ABN 33
Všechna práva vyhrazena

Obrázek 1 Ukázka phishingového útoku Avonet

3.2 Komerční banka

V březnu letošního roku tj. 2012 se stali někteří klienti oběťmi pharmingového útoku, kdy místo na stránku banky, byli přesměrováni na podvržené stránky, které po uživateli chtěli, aby se autentizoval pomocí údajů ze své kreditní karty.



Obrázek 2 Ukázka pharmingového útoku Komerční banka

Ovšem tento útok má dost zásadní slabinu a to tu, že nejsme anglicky mluvící zemí, takže i méně obezřetného uživatele (tedy pokud si vůbec přeloží, co po něm stránka požaduje) musí trefit do očí, že tady je něco špatně, když je internet banking celou dobu česky a najednou mu naskočí okno v angličtině.

3.3 Česká spořitelna

Patrně nejznámější obětí phishingového útoku se stala Česká spořitelna v roce 2006, kdy to byl tento útok náležitě medializován.⁴ Tento útok však obezřetný uživatel zcela jistě odhalil, jelikož když se podíváme na obrázek, tak nám dojde, že žádné „Oddělení Banky pro ochranu před frodem“ neexistuje. Obrana proti tomuto útoku je tudíž snadná.

Dobry den vazeni klienti!

Leto roku 2006 bylo pro Banku nejzavaznejsim z hlediska poctu nelegalnich operaci. Cim dal vice maji podvodnici zajem o duvernou informaci nasich zakazniku. Velke mnozstvi lidi se na nas obraci s zadosti zamezit vzniku nebezpeci ztraty peneznich prostredku z uctu.

S ohledem na soucasny stav vyhlasuje Banka nasledujici mesic za mesic boje s frodem.

Do 1.listopadu musi vsechny nasi klienti aktivovat novy system bezpecnosti vlastnich uctu.

Provedli jsme velkou praci pro zlepzeni bezpecnosti. System byl zkontrolovan uznavanymi odborniky v oboru elektronickych plateb, a vsechny nezavisli experti potvrdili ucinnost systemu proti frodu. Z duvodu nebezpeci mozneho zneuzeni techto udaju podvodniky nejsou tyto data zverejnena v otevrenych zdrojich.

Vy jste byl (a) zvolen (a) jako jeden z ucastniku finalniho stadia testovani systemu.

V soucasne dobe Vam navrhujeme vyuzit odkaz <https://www.servis24.cz/ebanking-s24/> a standardnim zpusobem prihlaseni do Internet bankingu aktivovat novy bezpecnostni system.

V aktualnim stadiu provozu jsou mozne nekteere nesrovnalosti.

Pripoustime jejich existenci, a proto prosim nezasilejte dodatecne popisy vznikajicich potizi, prace na jejich odstraneni jiz probihaji.

Musime Vas informovat o bezpodminecnem pouziti noveho systemu od listopadu, v opacnem pripade budou Vase ucty zablockovany do okamziku uplne identifikace Vasi osoby. Proto doporučujeme v nejkratsi mozne dobe prejit na novy bezpecnostni standard.

S pozdravem, Oddeleni Banky pro ochranu pred frodem

Obrázek 3 Phishingový útok na Českou spořitelnu

⁴ Při zadání slov „phishing Česká spořitelna“ do vyhledávače Google <http://goo.gl/7b1k1> dostaneme přes 9 000 výsledků

Ovšem druhý phishingový útok na Českou spořitelnu v roce 2008 už byl mnohem zákeřnější, jak vidíme na Obrázek 4, tak zde už pravděpodobně mnoho uživatelů naletělo, protože e-mail je psán česky a s diakritikou, odesílatel také vypadá věrohodně. A navíc ještě obsah varuje před phishingovými útoky.

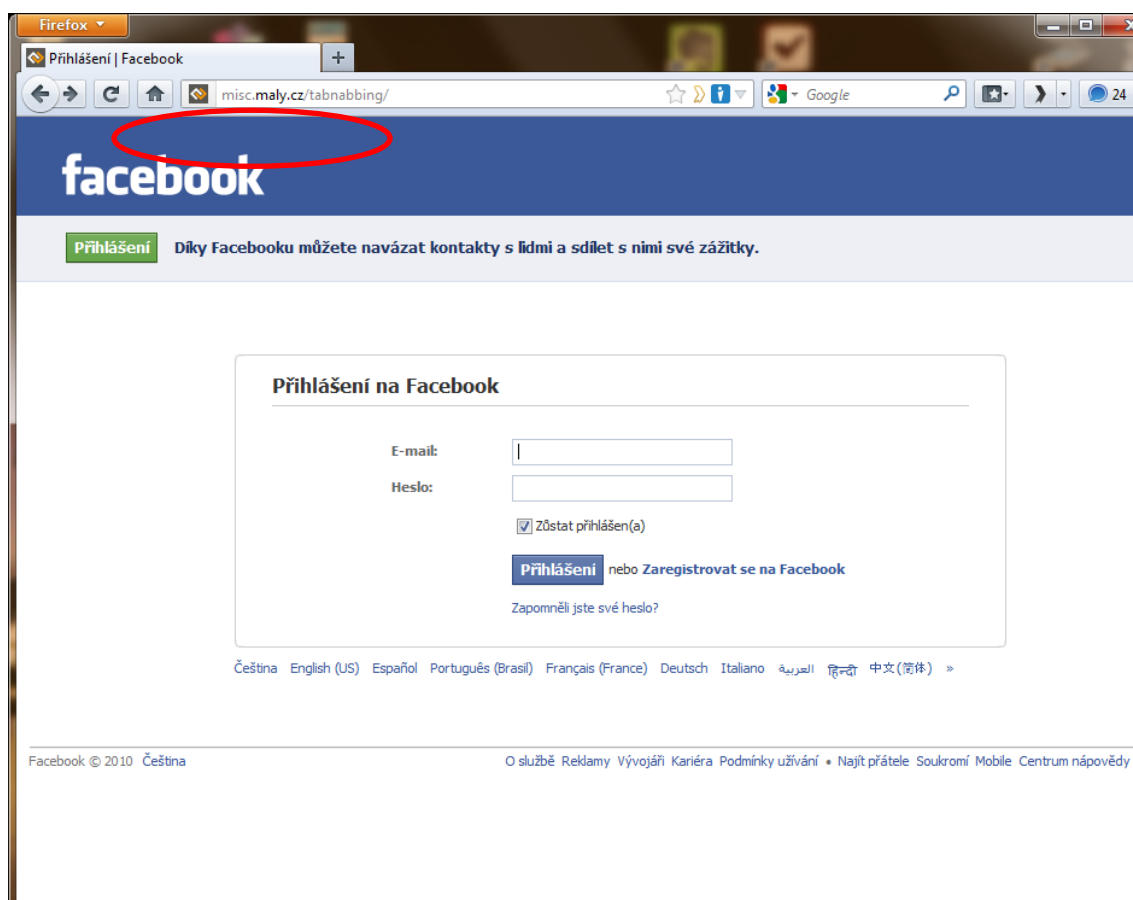
Před tímto útokem ovšem varuje přímo Česká spořitelna na hlavní stránce svého internetového bankovníctví Servis24 (<https://www.servis24.cz>), kde uživatele nabádá, aby nesdělovali své osobní údaje, hesla či kódy PIN formou e-mailu a také že od klientů nebude nikdy údaje touto formou požadovat. [13]



Obrázek 4 Phishingový útok na Českou spořitelnu [13]

3.4 TabNabbing

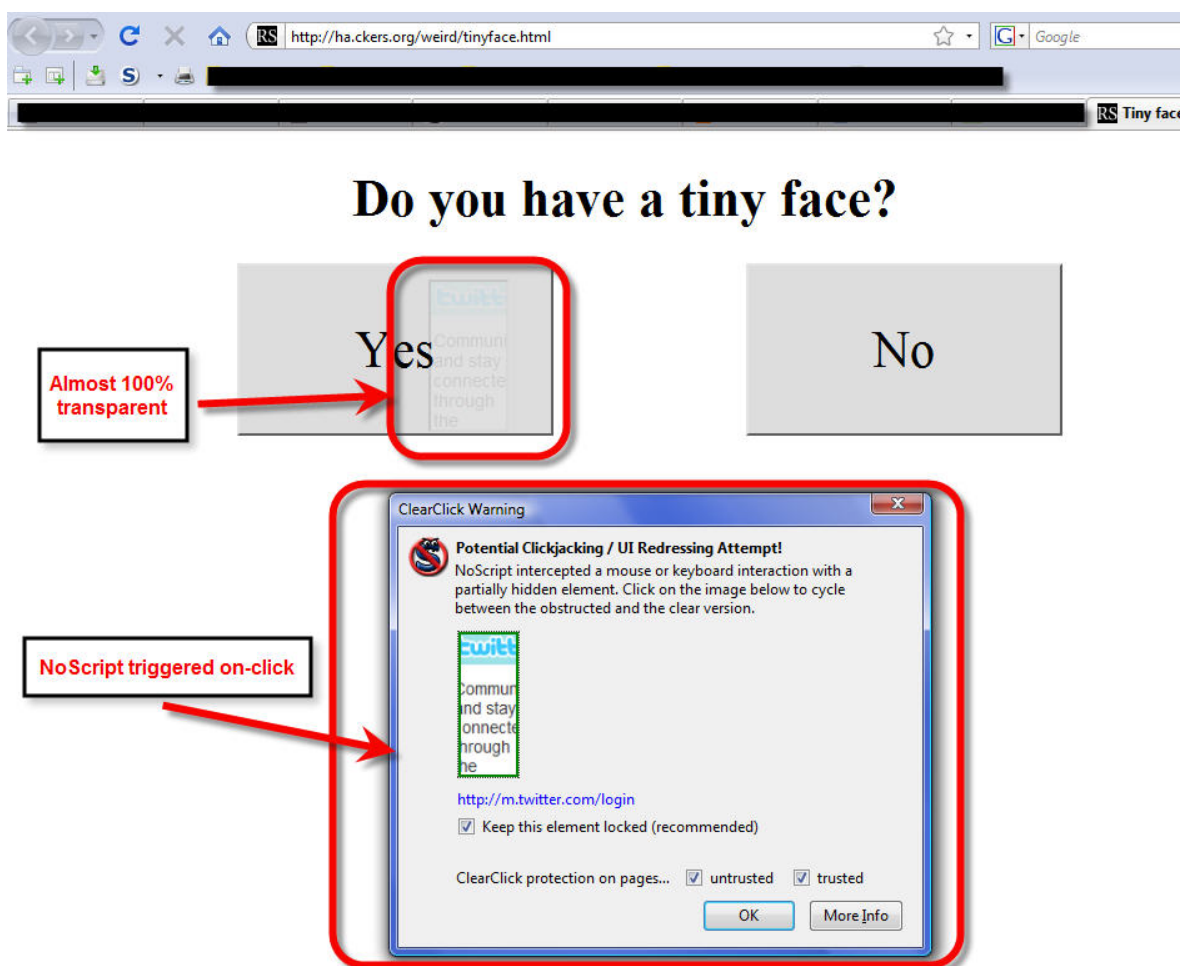
Zde se nejedná přímo o útok, ale ukázkou TabNabbingu v praxi. Kdy pokud si otevřeme v novém panelu webovou adresu <http://misc.maly.cz/tabnabbing/> a pak přepneme na jiný panel, tak se nám za chvíli načte jiná stránka, tak jako vidíme na Obrázek 5. Pokud je uživatel trochu obezřetný, tak si jistě všimne, že webová adresa neodpovídá obsahu. Tudíž panel zavře a neposkytne tak své přihlašovací údaje třetí straně.



Obrázek 5 TabNabbingový útok

3.5 Twitter

Útoky Clickjackingu často směřovaly na uživatele sociálních sítí, kdy vidíme příklad na Obrázek 6. Uživatel si myslí, že odpovídá pouze na neškodnou otázku ovšem místo toho, pokud má účet na Twitteru, tak se současně s odpovědí na otázku se také pod jeho účtem na Twitteru odeslala krátká zpráva se škodlivými odkazy. Díky doplňku NoScript jsme na tento útok upozorněni, často si ale všimneme až posléze, že jsme se stali obětí útočníka. Zkušeným uživatelům ovšem stačí podívat se do zdrojových kódů stránky a hned jim bude jasné, že na stránce je něco jiného než uživatel vidí.



Obrázek 6 Clickjackingový útok na Twitter

4 NOVÉ TRENDY V SOCIOTECHNICE

S rozvojem sociálních sítí se rozvíjí také možnosti sociotechniků, jak získávat cenné informace. Už nejsou odkázáni na e-mail případně instant messengery, ale můžou získávat potřebné informace prostřednictvím těchto sítí.

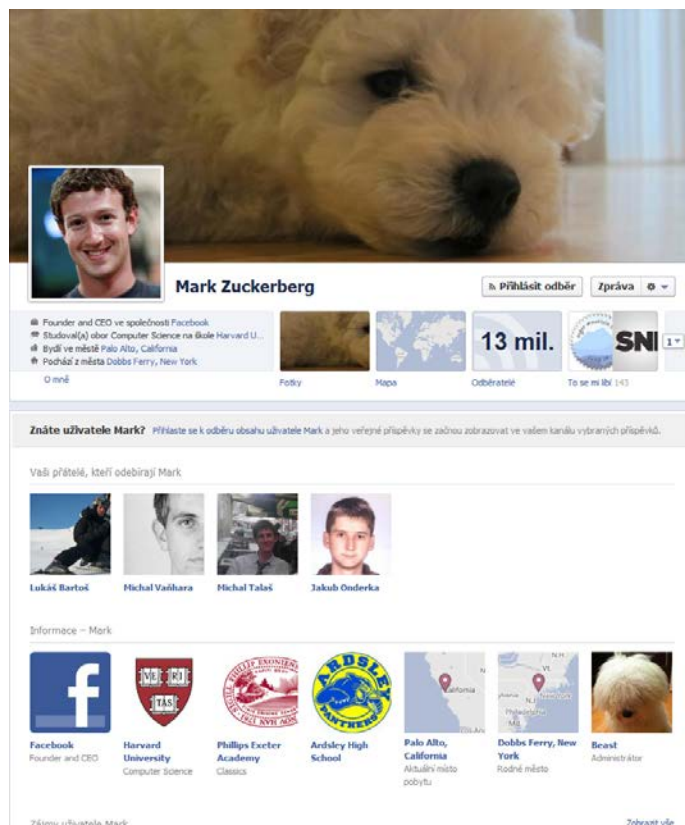
4.1 Facebook

Facebook je služba založená v roce 2004 Markem Zuckerbergem, která si za 8 let vybudovala základnu čítající přes 845 milionů lidí po celém světě. Kdy 80% aktivních uživatelů pochází mimo USA a Kanadu a denně je aktivních více než 483 milionů. [5]

Z těchto dat vidíme, že na Facebooku je ohromné množství uživatelských účtů, z nichž je mnohdy spousta slabě zabezpečených, čímž umožňují naprosto neznámým lidem pohled do svého soukromí. Mnoho lidí si toto nebezpečí vůbec nepřipouští, ale například fotky z rodinné oslavy můžou případnému zloději ukázat vybavení domácnosti a ten si takto může vytipovávat domy k vyloupení. [12]

Na Facebooku není problém vydávat se za někoho jiného a získat důvěru oběti, která si bude myslet, že komunikuje s jemu známou osobou a vůbec jej nenapadne, že se stal obětí útočníka. K tomu abychom se mohli vydávat za někoho jiného, nám stačí jenom jméno a příjmení dané osoby. Pokud uvedeme další údaje, jako je datum narození, bydliště, vzdělání či fotografii, tak nám to jen pomůže k autentičnosti profilu.

Zde na Obrázek 7 vidíme rozdíl mezi profilem, který spravuje přímo Mark Zuckerberg a profilem, kdy se někdo snaží za něj vydávat. Falešný profil většinou odhalíme snadno pohledem, kdy má například málo přátel, žádné osobní fotografie nulová aktivita a jiné. Zde je navíc ještě vidět chyba v příjmení, jelikož jsou v něm dvě g. Známé osobnosti tenhle problém řeší jednoduše tím, že si umístí na své webové stránky odkaz na svůj profil na Facebooku.



Obrázek 7 Pravý profil na Facebooku



Obrázek 8 Falešný profil na Facebooku

4.2 Twitter

Twitter je mikroblog a sociální síť v jednom, která umožňuje uživatelům sdílet krátké zprávy o délce až 140 znaků. V současnosti má 200 milionů uživatelů, kdy aktivních jich je 100 milionů. Každý den se napíše 230 milionů krátkých zpráv tzv. tweetů, což je pro zajímavost zhruba 6 400 tweetů za sekundu. [8]

Z předešlého vidíme, že Twitter je ohromný nástroj, který díky své jednoduchosti, překonává média. Není nic jednoduššího než napsat z mobilu tweet o tom, že v blízkosti hoří byt a jsou zde hasiči a předběhnout tím zpravodajství komerční televize. [9]

Ovšem jeho jednoduchost nahrává i útočníkům, kteří se můžou vydávat za kohokoliv. Na Twitteru najdeme mnoho falešných účtů jako například účet prezidenta Václava Klause, vidíme jej na Obrázek 10. Zde už je odhalení mnohem složitější, jelikož zde lze nastavit pouze přezdívka, fotografie, jméno příjmení a popis osoby. Ovšem pokud si přečteme napsané zprávy, tak nám musí být hned jasné, že takovéto informace by určitě nepsala hlava státu.

O ověření svého účtu mohl ještě v roce 2010 žádat kdokoli, kdo lidem v centrále Twitteru doložil, že uvedený účet je opravdu jeho. Většinou stačilo zaslat odkazy na vlastní webové stránky, které na uvedený účet odkazovaly. V České republice má jako jeden z mála takto ověřen účet Radek Hulán. Verifikovaný účet poznáme podle viditelné značky za jménem uživatele. Tak jako to vidíme na Obrázek 9. Ovšem od prosince roku 2010 není tato verifikace možná, kdy doporučení je, že autenticitu si uživatelé sami nejlépe dokáží odkázáním se z vlastního oficiálního webu. [15]



Obrázek 9 Ověřený účet na Twitteru

The image shows a screenshot of a Twitter profile page for 'Václav Klaus' (@vaclavklaus). The profile is a clone of the real one, featuring a photo of Václav Klaus, his bio 'Vždy jsem chtěl být prezident. A tak jím jsem.', and a link to 'http://www.klaus.cz'. The statistics show 182 tweets, 0 following, and 3,448 followers. The 'Following' button is highlighted in blue. The left sidebar contains navigation links: 'Tweet to Václav Klaus', 'Tweets', 'Following', 'Followers', 'Favorites', 'Lists', and 'Recent images'. Below these are 'Similar to Václav Klaus' suggestions for 'Bc. Onderka, MBA', 'Léko Media Group', and 'TOP 09'. The main content area displays a list of tweets from the account, including references to a photo, a list, and various political statements. The footer contains the Twitter logo and copyright information for 2012.

Home @ Connect # Discover Search

Václav Klaus
@vaclavklaus
Vždy jsem chtěl být prezident. A tak jím jsem.
<http://www.klaus.cz>

Following 182 TWEETS 0 FOLLOWING 3,448 FOLLOWERS

Tweet to Václav Klaus

@vaclavklaus

Tweets

Following

Followers

Favorites

Lists

Recent images

Similar to Václav Klaus

Bc. Onderka, MBA @Onderka_MBA Follow

Léko Media Group @ceskapozice Follow

TOP 09 @TOP09cz Follow

twitter
© 2012 Twitter About Help Terms Privacy
Blog Status Apps Resources Jobs
Advertisers Businesses Media Developers

Tweets

Václav Klaus @vaclavklaus 2 Apr
Toto mne teda opravdu, ale opravdu unika. Jaky je smysl teto fotografie? Nedokazal mne to vysvetlit ani Jakl s Hajkem.
twitpic.com/94eg4j
[View photo](#)

Václav Klaus @vaclavklaus 29 Mar
Byla by nepravda, kdybych řekl, že mně nevadí, že nejsem v seznamu @cermak. Ale jak musí být nasraní takový jako @petmara, @cuketka...

Václav Klaus @vaclavklaus 10 Mar
Nektere tweety jsou jen bzucením filcky v usich mych.

Václav Klaus @vaclavklaus 5 Mar
Drzost podrizenych nezna mezi. Ted si nekdo na chodbe prozpevoval. Putin - in, Klaus - aus... Jeste ne, vazeni, jeste ne!

Václav Klaus @vaclavklaus 17 Feb
Člověk si ani v tom Turecku neodpočine. Opravdu, ale opravdu nechápu, proč někdo řeší mnou udělené milosti. Já si nebudu doma dělat peklo.

Václav Klaus @vaclavklaus 14 Feb
Milý Jaromíre, chtěl bych Vám popřát všechno nejlepší ke kulatým narozeninám! A konečně předběhněte toho Sakica v bodování. #jagr #68 #kona

Václav Klaus @vaclavklaus 3 Feb
Jednou pisi z pocitace a podruhe z telefonu. Jednou s diakritikou, podruhe bez. A dost te kritiky.

Václav Klaus @vaclavklaus 3 Feb
Stop #ACTA! Ale bohužel, opravdu bohužel, si myslím, že na mně nezáleží. ://

Václav Klaus @vaclavklaus 3 Feb
Kdyz se clovek nepripomene, tak si nikdo nevzpomene. #ff #ffc Jen ten Hajek s Jaklem mne prorad pripominaji, jak jsem dobrej. Uz me nudi.

Obrázek 10 Falešný profil na Twitteru

II. PRAKTICKÁ ČÁST

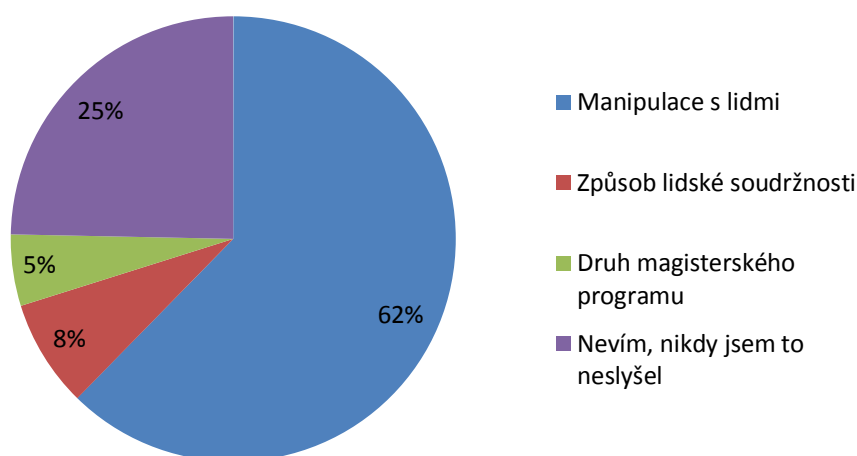
5 ANKETA

K anketě jsem využil služby Google Docs, která oproti specializovaným službám jako je například vyplnto.cz, nemá žádné vstupní podmínky. Pokud bych ji chtěl umístit na vyplnto.cz, tak bych musel před přidáním vlastní vyplnit ankety ostatních. Navíc na Google Docs může být otevřena déle než měsíc, takže je stále přístupná na adrese <http://goo.gl/xdGqy>. Ankety se zúčastnilo přes 70 respondentů a byla umístěna na sociálních sítích Facebook, Twitter a Google+ a taky byla šířena přes e-mail přátelům a známým, kteří nepoužívají uvedené sítě. Nejčastěji odpovídající respondent byl muž, ve věkovém rozpětí 20-25 let se středoškolským vzděláním,

5.1 Vyhodnocení ankety

Anketa je umístěna v příloze kde se nachází, jak otázky které byly respondentům předloženy, tak jsou tam také zobrazeny její výsledky v nezpracované podobě.

5.1.1 Co je to sociální inženýrství?

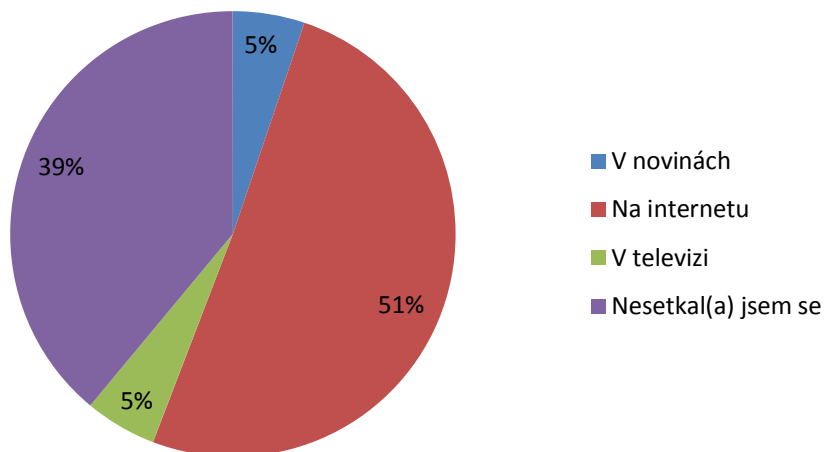


Obrázek 11 Výsledky pro otázku: Co je sociální inženýrství?

První otázkou v anketě bylo cílem zjistit, zda respondent má tušení čeho se budou následující otázky týkat. Překvapilo mě, že čtvrtina uživatelů se s tímto pojmem vůbec neselekala. Což svědčí o tom, že je potřeba uživatele s touto problematikou více seznámit a obeznámit je i se všemi riziky, jež hrozí. Dotazované jež odpověděli na otázku špatně bych

zařadil do kategorie možná, protože buď chtěli na otázku odpovědět a nechtěli přiznat, že pojem neznají, případně tento pojem slyšeli, ale nebyli si jistí kam jej zařadit.

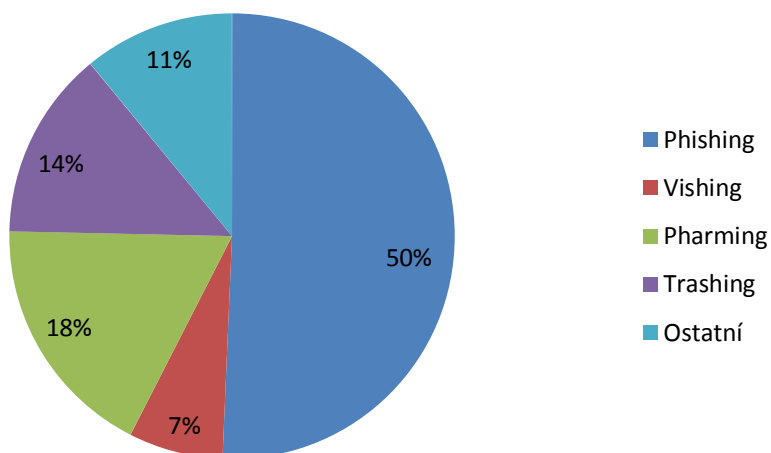
5.1.2 Kde jste se setkali se sociálním inženýrstvím?



Obrázek 12 Výsledky pro otázku: Kde jste se setkali se sociálním inženýrstvím?

Z tohoto grafu vidíme, že polovina respondentů se už se sociálním inženýrstvím setkala. Zarážejících je ovšem 10% odpovědí, které odkazují na noviny a televizi. Tito lidé vůbec netuší, co sociotechnika je, takže se pravděpodobně už s takovýmto útokem setkali, ale jenom o něm neví.

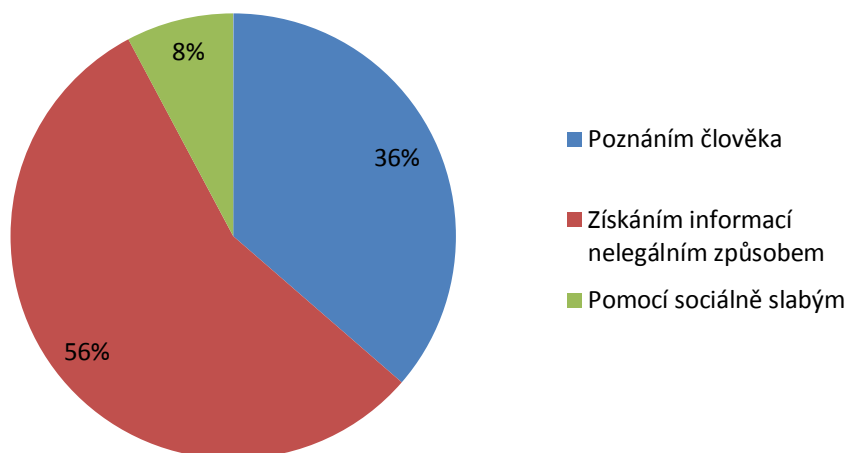
5.1.3 S jakou formou jste se už setkali?



Obrázek 13 Výsledky pro otázku: S jakou formou jste se už setkali?

Z grafu je naprosto jasné, že phishing je stále aktuální téma, když jej zatklo 50% respondentů. V kolonce Ostatní jsou zahrnuty odpovědi, které mohli uživatelé doplnit sami. Objevil se zde dvakrát baiting a také jednou handshaking, který ovšem se sociálním inženýrstvím nemá nic společného, protože se jedná o proces, který je nutný pro uskutečnění komunikace zařízení.

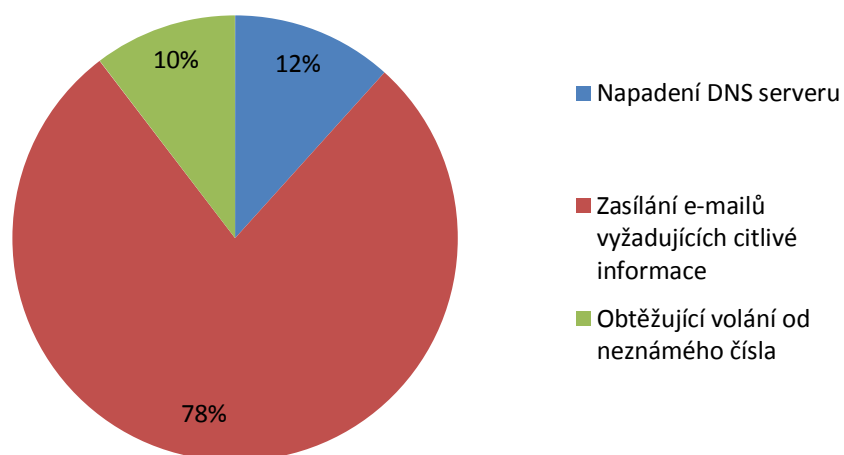
5.1.4 Sociotechnika se zabývá?



Obrázek 14 Výsledky pro otázku: Sociotechnika se zabývá?

Z tohoto grafu jsem potěšen, protože 92% lidí ví, čím se sociotechnika zabývá. Primárně jí sice jde o získání informací, ale v případě fyzické sociotechniky je nutné i poznání oběti, aby byl útok dokonalý a útočník nevzbudil pozornost. Zbýlých 8% přisuzuju tomu, že respondenti naprosto nevěděli, o č se jedná a vzali podobnost socio a sociální a podle toho označili výsledek.

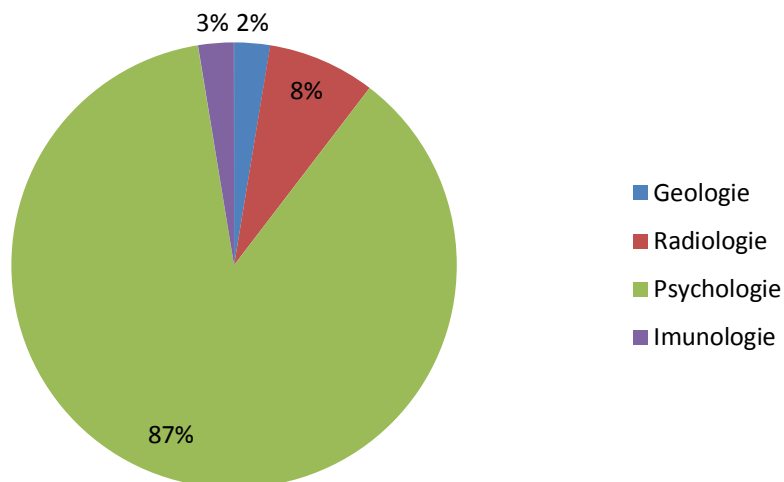
5.1.5 Phishing je?



Obrázek 15 Výsledky pro otázku: Phishing je?

Z výše uvedeného grafu je krásně vidět, že tři čtvrtiny uživatelů vědí, o co se jedná a už i pravděpodobně mají s phishingem zkušenost. Což je to pravděpodobně způsobeno medializovanými útoky na Českou spořitelnu.

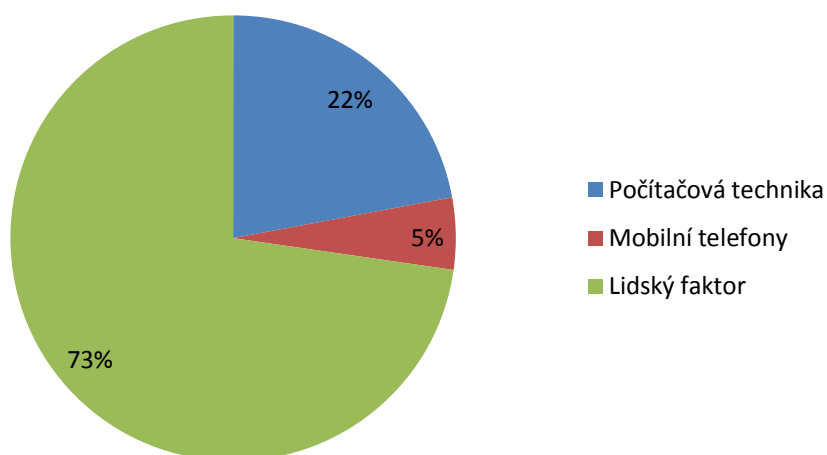
5.1.6 Pro sociotechniku jsou vhodné znalosti?



Obrázek 16 Výsledky pro otázku: Pro sociotechniku jsou vhodné znalosti?

Zde vidíme jasnou převahu správné odpovědi, kterou je psychologie. Třináct procent špatných odpovědí lze přisuzovat neznalosti uživatelů daných profesí, protože například nevím, k čemu by útočníkovi byly dobré znalosti geologie, což je věda, která zkoumá složení, stavbu a historický vývoj Země.

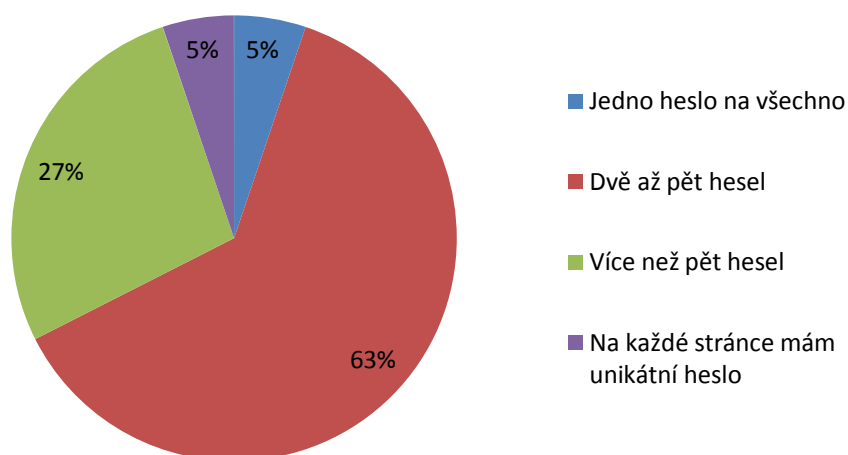
5.1.7 Na útok sociotechnikou je náchylná?



Obrázek 17 Výsledky pro otázku: Na útok sociotechnikou je náchylná?

Že je na sociotechniku náchylný člověk je více méně jasné, ale že by na ni byla náchylná počítačová technika nebo telefon se říct nedá, protože to jsou pouze prostředky využívané útočníky. Ale i tak je 73% potěšujících a to z toho důvodu, že si většina uživatelů uvědomuje, že slabým článkem jsou oni a ne technika.

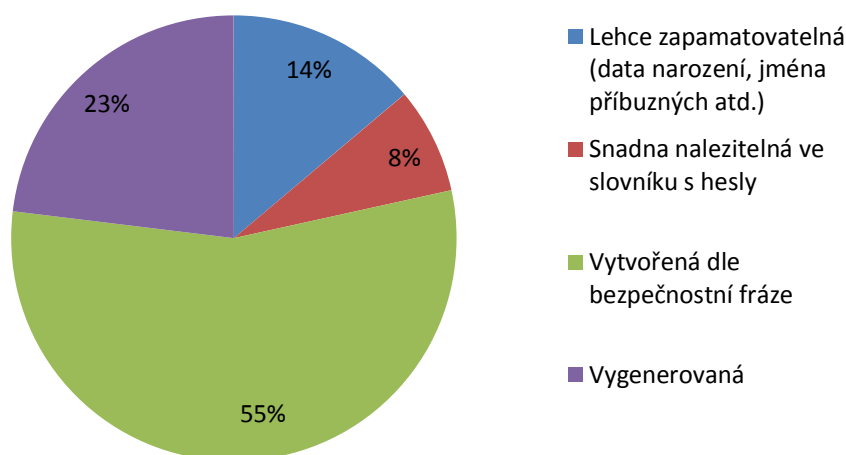
5.1.8 Kolik různých hesel používáte pro autentizaci?



Obrázek 18 Výsledky pro otázku: Kolik různých hesel používáte pro autentizaci?

Tato otázka nám zobrazuje rozsah škod v případě získání hesla útočníkem. Protože pokud uživatel využívá jedno heslo, tak útočnickovi nic nebrání v tom, aby se za něj vydával na všech internetových službách, které daný uživatel využívá a útočník je objevil. Naštěstí těchto uživatelů je jen 5%. Oproti tomu druhým extrémem je dalších 5 % uživatelů, kteří mají na každou stránku jiné heslo, což je v ohledu na bezpečnost ideální stav, ale ovšem klade velké požadavky na paměť uživatele, který si tak musí nejen pamatovat všechna hesla, ale také vědět, které heslo ke které službě patří. Naštěstí se tohle dá obejít například pomocí správce hesel, který je dnes již v každém internetovém prohlížeči.

5.1.9 Jaká hesla využíváte pro přístup k serverům využívajících autentizaci?



Obrázek 19 Výsledky pro otázku: Jaká hesla využíváte pro přístup k serverům využívajících autentizaci?

Tři čtvrtiny uživatelů má dobré heslo, ale u zbytku je velké riziko, že jejich heslo bude odhaleno a to z toho důvodu, že je mnohem rychlejší zkoušet hesla, které už máme v předpřipraveném slovníku či o uživateli známe dostatek informací, takže můžeme zkoušet hesla, která s ním souvisí, například jméno jeho manželky, dítěte, mazlíčka atd., než zkoušet prolomit pomocí hrubé síly heslo "nSmkLs18WsZ,s65K(Z)", které vzniklo z fráze "Na stole mám kloubovou lampu s 18W šetrivou žárovkou, stála 65Kč (žárovka)"

5.2 Vyhodnocení správných odpovědí

Všechny odpovědi správně mělo pouhých 11 respondentů, což je 14% dotazovaných. Převažovali muži v poměru 8:3, ve věku 20-25 let a vysokoškolsky vzdělaní v poměru 6:5 vůči maturantům.

6 OBRANA PŘED ÚTOKY SOCIÁLNÍM INŽENÝRSTVÍM

V této kapitole se budeme věnovat obraně před útoky sociálním inženýrstvím, které jsme si uvedli v kapitole 2. Protože nestačí vědět, jak se který útok jmenuje, mnohem důležitější je vědět, jak se před ním chránit.

6.1 Phishing

I když v dnešní době už poštovní klienti, jako je například Microsoft Outlook, blokuji podezřelé zprávy, tak stále hlavní odpovědnost zůstává na uživateli, který musí používat zdravý rozum při práci s elektronickou poštou. U phishingových zpráv je potřeba si dávat pozor na odesílání citlivých údajů. Nikdo mimo nás tyto údaje nesmí znát. Administrátor naše heslo znát nepotřebuje, jelikož má vyšší oprávnění, což mu umožňuje neomezený přístup do systému. A ani banka po nás tyto údaje chtít nebude, jelikož si je sama vědoma, že by klienty vystavila zbytečnému riziku. Nejlepší prevencí proti útokům touto technikou je školení uživatelů, kdy se jim ukáží vzorové útoky a jejich charakteristické rysy, jako je například adresa odesílatele, jehož e-mail se nachází například na doméně seznam.cz. Čeština má také tu výhodu, že obsahuje mnoho tvarů sloves, takže u strojového překladu z angličtiny je okamžitě každému jasné, že zde není něco v pořádku.

6.2 Vishing

Vishing, jak jsme si uvedli v předešlé kapitole, se týká telefonické konverzace, kdy po nás chce někdo po telefonu zjistit informace například o bankovním účtu, heslu k němu atd. Ochrana před těmito útoky je opět jednoduchá, nic nikomu po telefonu neříkat. Například pokud voláme do banky, tak operátorům nediktujeme celý kód, ale třeba jenom třetí a sedmý znak hesla, což je pro obě strany mnohem bezpečnější, protože ani operátor toho nemůže následně zneužít, neboť pořadí znaků, které chce banka znát se neustále mění a tak nehrozí, že by operátor po směně volal do banky a autentizoval se bance naším heslem.

6.3 Trashing

Trashing vychází ze získávání informací z vyhozené papírové korespondence či jiných důležitých materiálů. Obranou proti tomuto útoku je pořídit do kanceláři skartovačky, které znemožní rekonstrukci materiálu, nutno však pořídit takovou, která papír stříhá na malé kousky a ne takovou, která jej rozřeže na pásy. Skartovačkou můžeme taky likvidovat stará CD či DVD, případně kreditní karty, které by také mohl útočník zneužít.

6.4 Pharming

Záludností pharmingu je jeho obtížná odhalitelnost. Jestliže útočník napadne DNS server, my nemáme mnoho možností, jak se to dozvědět. Naštěstí existuje aplikace Netcraft Toolbar, která se instaluje jako doplněk do prohlížeče a ta nám zobrazuje další informace o stránce, jako je například hodnocení ostatních uživatelů a stát ke kterému je IP adresa stránky přiřazena. To nám může hodně napovědět, protože například weby našich bank jsou zcela jistě umístěny v České republice a to z důvodu dostupnosti. Takže pokud uvidíme, že webová stránka je umístěna například v Izraeli, musí nám být jasné, že stránka není ta, za kterou se vydává.

6.5 Clickjacking

Ochrana před tímto útokem je možná jak u poskytovatele webového obsahu, který znemožní zobrazování své stránky v iframe, tak i u uživatele, jenž musí mít aktualizovaný webový prohlížeč, který některé útoky dokáže rozpoznat. Cílová ochrana u uživatele však nyní velmi slabá.

Z běžně používaných je k dispozici zatím pouze doplněk NoScript pro prohlížeč Firefox, který blokuje většinu útoků ClickJackingu. Což například provádí zakázáním iframe v prohlížeči. [14]

6.6 TabNabbing

Proti tomu útoku jsou odolní jedinci, kteří disponují vynikající pamětí, kterým hned dojde, že se něco děje, protože vědí, že si třeba stránku s e-mailem neotevřeli. Ostatním ovšem stačí, když se vždy při návratu na otevřenou záložku podívají na adresní řádek a porovnají, že adresa koresponduje s obsahem. Taktéž může pomoci funkce doplňování přihlašovacích údajů v prohlížeči. Ta nám na kompromitované stránce nevyplní jméno a heslo, protože zobrazená adresa neodpovídá uložené adrese, ke které jsou přiřazeny údaje.

6.7 Baiting

Je jedna ze zákeřných podob sociotechniky, protože využívá lidské zvědavosti. Pokud ovšem dobře nastavíme bezpečnostní politiku v počítačích ve firmě, tyto útoky nás nemůžou ohrozit. Administrátor pomocí Zásad zabezpečení zakáže uživatelům používat CD mechaniku a USB paměti. V případě, že někteří uživatelé tato rozhraní v rámci své profese potřebují, tak se zakáže automatické spouštění z těchto médií.

6.8 Fyzická sociotechnika

Fyzická sociotechnika se vyskytuje ve velkých firmách, případně ve firmách s mnoha pobočkami. Řešením této situace je tvorba firemních visaček, kde bude uvedeno jméno, příjmení a fotka zaměstnance přes kterou bude holografická nálepka, kterou zabráníme či alespoň ztížíme kopírování. Případně na ni můžeme ještě umístit informace na magnetickém proužku a tím kartu rozšířit o možnost autentizace u přístupových systémů.

6.9 Pretexting

Obrana před pretextingem je nejtěžší ze všech, jelikož útočník má dost informací, tak často útok ani nezjistíme. Ovšem můžeme tomu částečně zabránit tím, že citlivé informace nebudeme sdělovat přes telefon či e-mail, ale pouze osobně nebo je budeme zasílat doporučeně do vlastních rukou na adresu.

7 NÁVRH ŠKOLENÍ PRO VEDOUcí PRACOVNÍKY

Tato kapitola má sloužit jako podklad pro vedoucí pracovníky, kteří budou proškolovat své podřízené, jež seznámí s různými druhy útoků, které by mohli v jejich firmě nastat. V příloze je přiložena osnova školení, v níž je v bodech shrnuta tato kapitola. Součástí je také vypracovaná prezentace.

7.1 Phishing

Vysvětlíme zaměstnancům co to phishing je a kde se s ním můžeme převážně setkat (e-mail, IM). Dále jim zobrazíme ukázky takovýchto případů, jako bylo například napadení České spořitelny. Zde jim ukážeme typické znaky těchto útoků (špatná e-mailová adresa odesílatele, slovníková čeština) a hlavně zdůrazníme, že tyto e-maily budou požadovat citlivé informace. V poslední části necháme prostor pro dotazy

7.2 Vishing

Zaměstnance seznámíme s vishingem a zdůrazníme, kde se s ním můžou setkat (telefon, VoIP). Pro názornost jim také ukážeme, jak takový telefonát může probíhat:

Útočník: Dobrý den, tady Petr Novák z banky Banka. Mluvím s panem Novotným?

Oběť: Ano, mluvíte.

Útočník: Pane Nováku, vyhrál jste v naší soutěži osobní automobil. Potřebuji nyní ověřit, že jste to opravdu Vy, máte u sebe kreditní kartu?

Oběť: Ano, mám.

Útočník: Dobrá, abychom si vaši totožnost ověřili proti naší databázi, tak mi prosím nadiktujte tyto údaje...

Poté je instruujeme, aby po telefonu nesdělovali žádné důvěrné informace.

7.3 Trashing

Podřízeným vysvětlíme co to trashing je a čeho se týká. Uvedeme jim příklady těchto útoků, kdy například z výpisu účtu můžeme získat citlivé údaje jako je jméno, příjmení, adresa, číslo účtu a zůstatek na něm, které útočníkovi můžou posloužit například k vishingu. Proto zaměstnance nabádát k důslednému používání skartovaček a v případě jejich absence, alespoň k trhání dokumentů na co nejmenší kousky.

7.4 Pharming

Vysvětlíme zaměstnancům čeho se pharming týká a instruujeme je k tomu, aby si na počítače nainstalovali Netcraft Toolbar, který dokáže před těmito útoky varovat.

7.5 Clickjacking

Seznámíme je s Clickjackingem, jak funguje a jaká rizika z něj plynou. Doporučíme instalaci doplňku NoScript (pouze pokud používají Firefox) a vyzveme uživatele k obezřetnosti, aby nechodili na nežádoucí stránky, kde se s tímto mohou setkat (warez, pornografie, hry atd.)

7.6 TabNabbing

Zaměstnance seznámíme s TabNabbingem a ukážeme jim názorný příklad tohoto útoku <http://misc.maly.cz/tabnabbing/>. Upozorníme je, aby si vždy kontrolovali adresní řádek, kdy adresa musí odpovídat obsahu. Nemůžeme mít adresu seznam.cz a obsah bude naše internetové bankovníctví.

7.7 Baiting

Vysvětlíme pojem baiting, můžeme i rozvinout diskuzi co kdo udělá s nalezeným DVD či USB pamětí. Zaměstnancům vysvětlíme rizika, která plynou z tohoto útoku (backdoor⁵, ztráta dat atd.) Pokud zaměstnanci ke své práci nepotřebují vyměnitelná média, tak požádáme správce sítě, aby zablokovali přístup k těmto médiím ve firemních počítačích.

7.8 Fyzická sociotechnika

Zaměstnancům vysvětlíme fyzickou sociotechniku. Můžeme například vzít na školení cizí osobu, která všem bude tvrdit, že je nový zaměstnanec, případně že je z jiného oddělení. A po vysvětlení s posluchači diskutovat, zda měli nějaké podezření či obavy z neznámé osoby. Ve firmě proto pořádat akce, kde se kolektiv více pozná a také každého nového zaměstnance představit ostatním.

⁵ Zadní vrátka, která umožňují útočníkovi obejít zabezpečení počítače a využívat pro stahování firemních dat, případně pro nelegální činnost

7.9 Pretexting

Vysvětlíme zaměstnancům pretexting a ukážeme jim vzorový telefonát, který může být stejný jako u vishingu. Upravit politiku firmy tak, aby se citlivé informace sdělovaly pouze osobně nebo zasílaly doporučeně do vlastních rukou na adresu, kterou máme u klienta vedenou v databázi.

ZÁVĚR

V práci jsem čtenáře seznámil s pojmem sociotechnika, kterou do praxe uvedl poprvé Kevin Mitnick na přelomu 70. a 80. let kdy získal potřebné informace od ochotného řidiče autobusu. Dále jsem čtenáři představil nejčastější útoky, které se v dnešní době vyskytují. Jsou to převážně útoky vedené prostřednictvím internetu, jelikož ty jsou nejbezpečnější a nejrozsáhlejší. Protože není problém pro útočníka z USA provést útok na oběť, která se nachází v Evropě, což potvrzují uvedené příklady útoků. Navíc také vidíme, že se útoky netýkají pouze velkých států jako je například USA, ale celého světa, České republiky nevyjímaje. Přestože je jich většina vedena prostřednictvím internetu, tak to neznamená, že fyzické útoky nejsou zákeřné, opak je bohužel pravdou, protože o těchto útocích se nikde nemluví a ani nejsou medializované.

Obranou proti útokům je jediné obezřetnost uživatele, které dosáhneme pouze tím, že se o tomto tématu bude více mluvit, případně firmy budou pro své zaměstnance pořádat školení, které může být ve formě, jak jsem nastínil v praktické části práce. Z vypracované ankety jsme zjistili, že osvěta o těchto útocích není na moc velké úrovni. Uživatelé mají často zkušenost s phishingem, což je ale jenom jedna z možností jak od nich dostat citlivá data.

I když se většina útoků odehrává na internetu a už je pár programů, které se nás snaží před nimi ochránit, tak ale stále zůstává největší odpovědnost na uživateli. Protože sociotechnice odolá každý systém, už ovšem neodolá uživatel, který těmto útokům podlehne a poskytne přístup do systému cizí osobě, případně poskytne požadované informace přes e-mail či webové stránky.

Pro uživatele rozhodně není důležité znát všechny útoky názvem, to po nich nikdo nemůže chtít. Ovšem je důležité, aby uživatelé nezapomínali na zdravý rozum a nepodléhali bláhovému pocitu, že na internetu se jim nemůže nic stát. Ano, fyzicky se jim stát nic nemůže, ale prázdné bankovní konto nepotěší.

Dle mého názoru je cenným výsledkem mé práce vypracovaná anketa vyhodnocující aktuální povědomí lidí o sociálním inženýrství a také příložená prezentace, kterou můžou vedoucí pracovníci použít, pokud budou s těmito útoky seznamovat své podřízené. Já osobně jsem se například seznámil s baitingem o kterém jsem neměl tušení, že něco takového existuje.

ZÁVĚR V ANGLIČTINĚ

At work I familiarized reader with the concept of social engineering which for the first time put into practice Kevin Mitnick in the late 70s and 80s when he got information from a willing bus driver. Next, I introduced readers of the most common attacks that appear today. They are mostly attacks led via the Internet inasmuch as they are the safest and most extensive. Because there is no problem for the attacker from the U.S. to attack the victim, which is located in Europe, which is confirmed by the examples of attacks. In addition, we also see that the attacks don't concern only large states such as the U.S., but all over the world, including the Czech Republic. Although most of them conducted through the Internet, it does not mean that physical attacks are not insidious, the opposite is true, but about these attacks is nowhere talking and they are not even published.

Defense against attacks is the only users caution, that we achieved only when we will be more talk about this subject or companies will organize training for their staff that may will be as I outlined in the practical section. From the developed questionnaire we found that education about these attacks isn't very high level. Users have got often experience with phishing but this is just one of the options how to get from them sensitive data.

Although most attacks take place on the internet and are a few programs that are trying to protect us against them but still remains the greatest responsibility to the user. Because each system resist to social engineering but user don't resist he succumb to these attacks and provide access to foreign person into the system or provide the requested information via e-mail or web page.

For the users is not certainly important to know the name of all the attacks, no one can want it after them. However is important that users don't forget the common sense and do not succumb to unreasonable sense that on the internet nothing can happen to them. Yes, physically nothing can happen to them but an empty bank account is displeasing.

In my opinion is a valuable result of my work developed survey assessing current awareness people about social engineering and also accompanying presentation which can lead employees to use if they will familiar their subordinates with these attacks. I am for example personally acquainted with Baiting about which I had no idea that something like this exists.

SEZNAM POUŽITÉ LITERATURY

- [1] MITNICK, Kevin. Umění klamu. Vyd. 1. Gliwice: Helion, 2003, 348 s. ISBN 83-736-1210-6.
- [2] Kevin Mitnick: Umění klamu. PETERKA, Jiří. Lupa.cz [online]. 25. 9. 2003 [cit. 2012-04-08]. Dostupné z: <http://www.lupa.cz/clanky/kevin-mitnick-umeni-klamu/>
- [3] Vishing - phishing přes telefon. HOBZA, Otakar. EMag.cz [online]. 25. 1. 2008 [cit. 2012-04-08]. Dostupné z: <http://www.emag.cz/vishing-phishing-pres-telefon/>
- [4] Phishing. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-04-12]. Dostupné z: <http://cs.wikipedia.org/wiki/Phishing>
- [5] Facebook's latest news, announcements and media resources - Fact Sheet - Facebook. Facebook [online]. 2012 [cit. 2012-02-19]. Dostupné z: <http://newsroom.fb.com/content/default.aspx?NewsAreaId=22>
- [6] HILLS, Chris. Social engineering in a socially networked world. SecurityInfoWatch.com [online]. 2010 [cit. 2012-03-24]. Dostupné z: <http://www.securityinfowatch.com/blog/10474470/social-engineering-in-a-socially-networked-world>
- [7] Pretexting: Your Personal Information Revealed. In: Federal Trade Commission: Protecting America's Consumers [online]. 2006 [cit. 2012-04-24]. Dostupné z: <http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre10.shtm>
- [8] TAYLOR, Chris. Twitter Has 100 Million Active Users. In: *Mashable* [online]. 2011 [cit. 2012-04-29]. Dostupné z: <http://mashable.com/2011/09/08/twitter-has-100-million-active-users/>
- [9] Věta "V baráku hoří, jsou tu hasiči" dnes vstoupila do historie Twitteru. In: *Futurum* [online]. 2011 [cit. 2012-04-29]. Dostupné z: <http://futurum.cz/clanky/veta-v-baraku-hori-jsou-tu-hasici-dnes-vstoupila-do-historie-twitteru.578/>
- [10] HASSMAN, Martin. Clickjacking: nebezpečí číhající na uživatele webových aplikací. *Zdroják.cz* [online]. 2008 [cit. 2012-04-29]. Dostupné z: <http://www.zdrojak.cz/zpravicky/clickjacking-nebezpeci-pro-uzivatele/>

- [11] MALÝ, Martin. TabNabbing krade přihlašovací údaje nepozorným. *Root.cz* [online]. 2010 [cit. 2012-04-29]. Dostupné z: <http://www.root.cz/clanky/tabnabbing-krade-prihlasovaci-udaje-nepozornym/>
- [12] KASÍK, Pavel. Češi Facebooku nebezpečně věří. Falešné krasavici naletělo 60 procent. *Technet.cz* [online]. 2009 [cit. 2012-04-03]. Dostupné z: http://technet.idnes.cz/cesi-facebooku-nebezpecne-veri-falesne-krasavici-naletelo-60-procent-112-/sw_internet.aspx?c=A091117_171036_sw_internet_pka
- [13] HOLČÍK, Tomáš. Česká spořitelna: phishing na druhou. *Živě.cz* [online]. 2008 [cit. 2012-05-03]. Dostupné z: <http://www.zive.cz/bleskovky/ceska-sporitelna-phishing-na-druhou/sc-4-a-140704/default.aspx>
- [14] MAONE, Giorgio. NoScript - JavaScript/Java/Flash blocker for a safer Firefox experience! - faq - InformAction. *NoScript* [online]. 2012 [cit. 2012-05-03]. Dostupné z: <http://noscript.net/faq>
- [15] DOČEKAL, Daniel. Twitter končí s „verified account“ označením. *JustIT.cz* [online]. 2010 [cit. 2012-05-10]. Dostupné z: <http://www.justit.cz/wordpress/2010/12/01/twitter-konci-s-verified-account-oznaceni/>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DEC	Digital Equipment Corporation
IP	Internet protokol
NORAD	North American Aerospace Defense Command
FBI	Federal Bureau of Investigation
VoIP	Voice over Internet Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
PIN	Personal identification number
IM	Instant messaging

SEZNAM OBRÁZKŮ

Obrázek 1 Ukázka phishingového útoku Avonet	17
Obrázek 2 Ukázka pharmingového útoku Komerční banka	18
Obrázek 3 Phishingový útok na Českou spořitelnu	19
Obrázek 4 Phishingový útok na Českou spořitelnu [13]	20
Obrázek 5 TabNabbingový útok	21
Obrázek 6 Clickjackingový útok na Twitter	22
Obrázek 7 Pravý profil na Facebooku	24
Obrázek 8 Falešný profil na Facebooku	24
Obrázek 9 Ověřený účet na Twitteru	25
Obrázek 10 Falešný profil na Twitteru	26
Obrázek 11 Výsledky pro otázku: Co je sociální inženýrství?	28
Obrázek 12 Výsledky pro otázku: Kde jste se setkali se sociálním inženýrstvím?	29
Obrázek 13 Výsledky pro otázku: S jakou formou jste se už setkali?	30
Obrázek 14 Výsledky pro otázku: Sociotechnika se zabývá?	31
Obrázek 15 Výsledky pro otázku: Phishing je?	32
Obrázek 16 Výsledky pro otázku: Pro sociotechniku jsou vhodné znalosti?	33
Obrázek 17 Výsledky pro otázku: Na útok sociotechnikou je náchylná?	34
Obrázek 18 Výsledky pro otázku: Kolik různých hesel používáte pro autentizaci?	35
Obrázek 19 Výsledky pro otázku: Jaká hesla využíváte pro přístup k serverům využívajících autentizaci?	36

SEZNAM PŘÍLOH

Příloha I: Výsledky ankety

Příloha II: Osnova pro školení

Příloha na CD: Prezentace v PowerPointu

PŘÍLOHA P I: VÝSLEDKY ANKETY

Výsledky ankety, tak jak byly stáhnuty z internetu dne 25. 4. 2012. K tomuto datu se ankety zúčastnilo 77 respondentů.

První číslo značí počet odpovědí, druhé jsou procenta z celkového počtu, u otázek kde je součet přes 100% bylo možno zatrhnout více odpovědí.

1. Sociální inženýrství je?

Manipulace s lidmi	48	62%
Způsob lidské soudržnosti	6	8%
Druh magisterského programu	4	5%
Nevím, nikdy jsem to neslyšel	19	25%

2. Kde jste se setkali se sociálním inženýrstvím?

V novinách	4	5%
Na internetu	39	51%
V televizi	4	5%
Nesetkal(a) jsem se	30	39%

3. S jakou formou jste se už setkali?

Phishing	37	79%
Vishing	5	11%
Pharming	13	28%
Trashing	10	21%
Ostatní	8	17%

4. Sociotechnika se zabývá?

Poznáním člověka	28	36%
Získáním informací nelegálním způsobem	43	56%
Pomocí sociálně slabým	6	8%

5. Pro phreaking potřebujeme?

Mobilní síť	10	13%
Internet	34	44%
Telefonní linku	28	36%
Satelitní přímač	5	6%

6. Kevin Mitnick byl ve své době?

Producentem her	5	6%
Programátorem škodlivého software	15	19%
Útočníkem využívající sociotechniku	57	74%

7. Phishing je?

Napadení DNS serveru	9	12%
Zasílání e-mailů vyžadujících citlivé informace	60	78%
Obtěžující volání od neznámého čísla	8	10%

8. Trashingu se dá zabránit?

Izolepou	10	13%
Sešíváčkou	4	5%
Skartovačkou	60	78%
Kancelářskými sponkami	3	4%

9. Záludností sociotechniky je?

Lehká odhalitelnost	7	9%
Otevřená hrozba	12	16%
Skrytá hrozba	58	75%

10. Pro sociotechniku jsou vhodné znalosti?

Geologie	2	3%
Radiologie	6	8%
Psychologie	67	87%
Imunologie	2	3%

11. "Nejznámější" společností v ČR, jejíž klienti se stali obětmi podvodných e-mailů byla?

Komerční banka	11	14%
Česká spořitelna	46	60%
Vodafone	10	13%
Poštovní spořitelna	10	13%

12. Jak poznáme podvodný e-mail?

Je plný reklamních sdělení s výhodnou cenou Viagry	6	8%
Bude vyžadovat odpověď s doplněnými citlivými údaji	69	90%
Je od neznámé osoby nebo firmy	2	3%

13. Na útok sociotechnikou je náchylná

Počítačová technika	17	22%
Mobilní telefony	4	5%
Lidský faktor	56	73%

14. Jaká hesla používáte pro přístup na servery vyžadující autentizaci?

Lehce zapamatovatelná (data narození, jména příbuzných atd.)	9	12%
Snadna nalezitelná ve slovníku s hesly	5	6%
Vytvořená dle bezpečnostní fráze	36	47%
Vygenerovaná	15	19%

15. Kolik různých hesel používáte pro autentizaci?

Jedno heslo na všechno	4	5%
Dvě až pět hesel	48	62%
Více než pět hesel	21	27%
Na každé stránce mám unikátní heslo	4	5%

16. Vaše pohlaví?

Muž	58	75%
Žena	19	25%

17. Kolik je Vám let?

0-15	2	3%
16-19	1	1%
20-25	58	75%
26-45	10	13%
46-65	5	6%
65-99	1	1%

18. Vaše nejvyšší dosažené vzdělání?

Základní	3	4%
Vyučen	0	0%
Maturita	42	55%
Absolutorium	2	3%
Bakalář	20	26%
Magisterské	7	9%
Doktorské a vyšší	3	4%
Magisterské	7	9%
Doktorské a vyšší	3	4%

PŘÍLOHA II: OSNOVA PRO ŠKOLENÍ

Následující body, slouží jako šablona k prezentaci, která je přiložena na CD. Navrhuju věnovat každému pojmu cca 5 minut.

Phishing

- Vysvětlit co to phishing je
- Ukázat příklady phishingových zpráv
- U příkladů se zaměřit na typické znaky phishingu
- Nechat prostor na dotazy

Vishing

- Vysvětlit vishing
- Vysvětlit zaměstnancům, ať po telefonu nesdělují citlivá data

Trashing

- Vysvětlit co je to trashing
- Uvést příklady využití trashingu (výpis účtu-jméno, příjmení, adresa, číslo účtu, ideální podklady pro Vishing)
- Zavést skartovačky do každé kanceláře, případně oddělení

Pharming

- Vysvětlit pojem Pharming
- Ukázat na příkladu napadení pharmingem
- Nainstalovat Netcraft Toolbar

Clickjacking

- Vysvětlit pojem Clickjacking
- Nainstalovat rozšíření NoScript (pouze v případě, že se ve firmě používá Firefox)
- Vyzvat uživatele k obezřetnosti, aby nechodili na nežádoucí stránky (warez, pornografie, hry atd)

TabNabbing

- Vysvětlit pojem TabNabbing Ukázat příklad (<http://misc.maly.cz/tabnabbing/>)
- Upozornit zaměstnance na kontrolu adresního řádku

Baiting

- Vysvětlit co je to baiting
- Uvést rizika plynoucí z útoku (backdoor, ztráta dat atd.)
- Předat IT oddělení požadavek na úpravu bezpečnostní politiky

Fyzická sociotechnika

- Vysvětlit fyzickou sociotechniku
- Prakticky zaměstnancům ukázat její záludnost, například vzít na školení cizí osobu, která bude všem tvrdit, že je nový zaměstnanec.
- Případně pokud jsou ve firmě prostředky, tak pořádat různé akce, kde se kolektiv více pozná

Pretexting

- Vysvětlit pretexting
- Ukázat zaměstnancům možný případ pretextingu v naší firmě (vzorový telefonát)
- Upravit politiku firmy (citlivé informace pouze osobně či doporučeně)