Univerzita Hradec Králové

Fakulta informatiky a managementu

BAKALÁŘSKÁ PRÁCE

2017 **Daniel Petera**

Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Využití metod sociálního inženýrství pro etický hacking

Bakalářská práce

Autor: Daniel Petera

Studijní obor: k-ai3

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové duben 2017

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 24. 4. 2017 Daniel Petera

Poděkování:

Děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi, Ph.D. za cenné rady, věcné připomínky a odborný dohled při zpracování této práce.

Anotace

Bakalářská práce přibližuje problematiku sociálního inženýrství. V úvodu práce definuji pojem sociální inženýrství a jeho využití či zneužití sociotechniky. Po seznámení s pojmem sociální inženýrství představuji nejslavnějšího sociotechnika světa. V další kapitole se zabývám psychologií útočníka. Od útočníka přecházím k popisu metod a mechanismů útoků. Následně uvádím, kde lze získat nejvíce základních informací pro započetí sociotechnického útoku. Po té seznamuji s možnostmi obrany vůči útokům, kterou můžeme zvýšit též pomocí etického hackingu. Ke konci práce zmiňuji právní postihy za kyberkriminalitu. Na závěr celé práce ukazuji aplikaci jednoho z mechanismů ve známém prostředí a seznamuji čtenáře s výsledky výzkumu.

Klíčová slova: sociální inženýrství, etický hacking, phishing, kyberkriminalita

Annotation

Title: The use of methods of social engineering for ethical hacking

Bachelor thesis approaches the issue of social engineering. In the beginning of thesis I define the concept of social engineering and its use or misuse socio-technics. After getting acquainted with the concept of social engineering, I present the most famous social engineer of the world. In the next chapter I deal with the psychology of the attacker. From the attacker I'm going to describe the methods and mechanisms of attacks. Subsequently, I describe, where can I get the most basic information to start socio-technical attack. After familiarizing myself with the options of defense against attacks, we can increase also the help of ethical hacking. Towards the end of the work I mention legal penalties for cyber crime. At the conclusion of the work showing the application of one of the mechanisms in a familiar environment and acquainted the reader with the results of the research.

Key words: social engineering, ethical hacking, phishing, cybercrime

Obsah

Úvod

Cílem práce je představit problematiku sociálního inženýrství, se kterým se setkáváme každý den. Může jít o běžné ovlivňování člověka tváří v tvář, nebo o využití nějakého mechanismu, kdy se vyhneme kontaktu s vybranou obětí. Spousta lidí si není vědoma, že by se stávala nebo mohla stát obětí útoku, i když je to v dnešní době reálnější než dříve. Mnoho z nás využívá internetbanking, který je velmi častým cílem různých útočníků. Cílem nemusí být jen odcizení financí, ale také cenné informace nebo třeba „know-how“, které lze dále zpeněžit.

V úvodní části je definován pojem sociální inženýrství a poté představen mediálně nejznámější sociální inženýr Kevin Mitnick. Nebyl nejlepším hackerem, ale uměl velmi dobře přesvědčovat, což mu vyneslo přídomek nejznámější sociotechnik světa. V souvislosti s uměním přesvědčovat navazuje kapitola charakterizující útočníka z psychologického hlediska. Jsou zmíněny jednotlivé lidské vlastnosti, které se snaží sociální inženýr zneužít ve svůj prospěch a snaží se o vzbuzení důvěry u oběti.

Následně jsou v práci popsány metody přístupů útočníka ke své oběti, jakým způsobem může sociální inženýr přímo přistoupit ke své oběti a zaútočit na ni. Pokračuji kapitolou seznamující s mechanismy, které využívá útočník při vzdáleném oslovení své oběti. Některé z těchto mechanismů jsou v dnešní době hojně využívány. Poté zmiňuji místo, kde se dá získat mnoho základních informací a nejen jich o potenciálních obětech. Mnoho lidí si neuvědomuje, co vše sdílejí na společenských sítích, jakou mají jejich informace hodnotu.

Další kapitoly jsou věnovány obraně vůči sociálnímu inženýrství. Můžeme investovat mnoho prostředků do nejlepších a nejdražších bezpečnostních technologií, můžeme proškolit personál tak, aby každá informace byla „pod zámkem“, můžeme si najmout nejlepší ostrahu majetku, a přeci bude celá organizace zranitelná. Prolomení různých bezpečnostních prvků je velmi zdlouhavé a náročné. Existuje však slabina každého systému a tím je lidský faktor. Díky této slabině se můžeme dostat i do nejlépe zabezpečeného systému. Pro lepší zabezpečení této slabiny můžeme využít etický hacking, který prověří, jak lidé reagují a kde dělají chyby proti bezpečnostním zásadám.

Bezpečnost s ohledem na lidskou lehkověrnost, naivitu a ignoranci je iluzorní. Sociotechnické útoky bývají často úspěšné jen díky porušení některé ze zásad zabezpečení.

Poslední kapitola je věnována výzkumu, který jsem provedl ve známém prostředí, kde jsem testoval, jakým způsobem jsou oběti schopny reagovat a zda prozradí nějaké osobní informace.

Toto téma jsem si vybral z důvodu osobního setkání se sociotechnickým útokem. Problematika sociálního inženýrství mě velmi pohltila, z tohoto důvodu bylo téma mé bakalářské práce jasné.

1 Sociální inženýrství

„Jen dvě věci jsou nekonečné – vesmír a lidská hloupost. Tím prvním si ovšem nejsem tak jist.“ – Albert Einstein

Sociální inženýrství (sociotechnika) je umění klamu. Je postaveno na základech psychologie a pokročilých počítačových znalostech. Sociotechnik zaměřuje svou podvodnou manipulaci hlavně na méně zkušené nebo nezkušené uživatele. Jeho cílem je vytvořit v člověku nějakým způsobem dojem, že situace je jiná, než ve skutečnosti je. Jinak řečeno: člověk nerozpozná, že mu telefonuje nebo e-mailuje nebo ho jinak oslovuje podvodník (sociotechnik), avšak na základě některých uměle vytvořených indicií se domnívá, že komunikuje s někým úplně jiným, důvěryhodným. Účelem útoku bývá získání informace, finanční zisk, diskreditace, atd. Útok může probíhat osobním kontaktem nebo vzdáleně s využitím počítačových technologií (např. spam). Sociální inženýrství je zakořeněno i v běžných podvodech z reálného světa: falešní výběrčí doplatků za elektřinu, plyn nebo vodu jsou ukázkovým příkladem.

Přestože jde o ohromné nebezpečí, o sociálním inženýrství se téměř nemluví. *„Přitom v kybernetickém prostoru je sociální inženýrství zneužíváno více než kde jinde – díky standardizované komunikaci a díky nesmírně jednoduchému ústupu i špatnému zajišťování stop v globálním médiu, jakým je internet.“* Před sociotechnickým útokem nás neubrání žádná aplikace, uchránit nás může jen ostražitost a „zdravá“ nedůvěra.[1]

Samotný termín „sociální inženýrství“ je značně nepřesný. V oblasti počítačové bezpečnosti jde o označení takových postupů, prostřednictvím kterých nám je umožněno obejít systémy zabezpečení, nikoli jejich technickým překonáním, ale využitím jejich klientů, fyzických uživatelů. Překonat sebelepší hardwarové a softwarové zabezpečení systému jako jsou antivirové programy, firewally apod. je zdlouhavější a hlavně mnohem složitější, než si vytypovanému uživateli jednoduše říci o heslo. Pravděpodobnost úspěchu takto vedeného útoku je vyšší než samotné překonání různých ochranných prvků systému. Předpokladem je, že kterýkoli systém, ač obsahující velmi kvalitní ochranu před neautorizovaným přístupem, musí kdykoli umožnit přístup autorizovaný. Jestliže následně útočník zneužije autorizovanou osobu k útoku, zabezpečený systém není schopen rozlišit mezi útočníkem a skutečnou autorizovanou osobou. Přesvědčit ke „spolupráci“ jakýmkoli způsobem vyškoleného a ostražitého

člověka – uživatele – je pak jednodušší, než oklamat technický systém. Zaměstnanec (uživatel) organizace představuje velké riziko v bezpečnostním systému kvůli své chybě, nepozornosti, nedbalosti, nevědomosti, atd.

Jelikož nelze předpokládat, že by uživatel informačního systému s útočníkem spolupracoval o své vlastní vůli, potřebuje ho útočník donutit k tomu, aby udělal, co potřebuje. Snahou útočníka je pomocí metod a praktik využít okolností ovlivňujících lidské chování a rozhodování. Mezi okolnosti, které člověka ovlivňují, řadíme důvěru, soucit, sympatie, stres, respektování autorit, snahu vyhnout se konfliktu a další. Sociální inženýrství je tedy jinak řečeno označení pro lest, pro uvedení v omyl. Důsledkem této lsti je, že útočník prolomí zabezpečení systému, o který tak usiloval skrytý za identitu skutečného autorizovaného uživatele. Případně s aktivní pomocí obelhaného autorizovaného uživatele.[2]

Pokud dojde k odcizení identity, jedná se o velice závažný problém. To znamená, že se někdo vydává za někoho jiného, jehož identita má reálný základ. Následky tohoto zločinu mohou být nedozírné. Jako příklad uvedu příklad z New Yorku. Jakýsi Philip Cummings byl zaměstnán ve společnosti Teledata Communications, Inc., která spravovala databáze pro banky. Díky tomu měl Cummings přístup k velmi citlivým údajům: osobním datům, heslům, informacím o bankovních transakcích, atd. Nevyužíval je pro svou potřebu, ale nabízel je za úplatu jiným zájemcům. Škodu vzniklou v důsledku Cummingsova jednání se pravděpodobně nikdy nepodaří přesně vyčíslit, dle odhadů se částka pohybuje v rozmezí padesát až sto milionů dolarů. Cummings byl za své jednání odsouzen k odnětí svobody na čtrnáct let.[3]

Důsledkem provádění sociotechnických útoků je, že obor informačních technologií chápeme jako značně virtuální. *„Chybí zde schopnost domýšlet přesahy do reality.“* Pro snazší vysvětlení uvedu následující příklad: Pokud kolegovi odcizím notebook, všichni bezprostředně chápou, že jsem dopustil trestného činu, jelikož mým jednáním kolega přišel o svou soukromou věc. Kdybych však kolegovi pouze zkopíroval data z harddisku, nikoli fyzickou přítomností u jeho notebooku, ale vzdáleně přes síťové připojení, nic se nestalo – kolega má přeci vše na svém místě a neutrpěl žádnou hmotnou škodu.[4]

Charakteristickým příkladem využití sociálního inženýrství jsou emailové výzvy nebo podvodné telefonáty. Dalším možným využitím sociotechniky může být „thrashing“, neboli prohledávání odpadků ve firmě a dalších místech mimo firmu, kam je vynášen nebo vyvážen odpad.[1]

Patrně jediným účinným opatřením je striktní bezpečnostní politika, která přesně určuje, jaké informace je kdo komu oprávněn poskytovat. Přihlašovací hesla se řadí mezi informace, které by měli znát výhradně sami uživatelé, přístup k nim nemá ani administrátor sítě. Zodpovědná osoba za dodržování takovéto politiky může aplikovat metody sociální inženýrství na uživatele systému a ověřit, zda heslo vyzradí. Je velmi pravděpodobné, že testovaný uživatel, který porušil bezpečnostní politiku a heslo vyzradil, po této lekci stejnou chybu neudělá.[5]

2 Kevin Mitnick

Kevin Mitnick není nejlepším hackerem na světě, za to je mediálně nejslavnějším.[6] Je tím, kdo poprvé definoval termín sociotechnika.

Na dráhu hackera se Kevin dostal již v dětství. Byl dítětem bez starostí, ale znuděný, jak píše ve své knize „Umění klamu“.[7] Vyrůstal v San Fernando Valley v Los Angeles. Po rozchodu rodičů žil s matkou, která pracovala jako servírka. Kevin tak trávil mnoho času osamoceně a sám sobě byl chůvou.

Ve dvanácti letech nalezl způsob, jak cestovat autobusem po Los Angeles zcela zdarma. Zjistil, že soustava dírek označovaná řidičem na jízdence představuje den, čas a autobusovou linku. Na zvídavé a velmi dobře promyšlené otázky mu odpověděl přátelsky naladěný řidič a prozradil mu i kde koupit děrovací strojek. Získat nepoužité jízdenky byla již maličkost, mnoho se jich nacházelo v odpadkových koších na autobusových nádražích, kam z části vypotřebované bločky vyhazovali řidiči po směnách.

Kevinovým dalším zájmem byla kouzla. Vždy, když přišel na způsob, jakým se trik provádí, cvičil ho tak dlouho, dokud ho plně neovládal. Tehdy objevil radost, kterou pociťoval při klamání lidí.

Na střední škole se prvně setkal s něčím, co začal později označovat jako sociotechniku. V té době poznal kamaráda, kterého pohltila záliba zvaná phreaking. Phreaking znamenalo pronikání do telefonních sítí a využívání jejich služeb. Kamarád předvedl Kevinovi, co vše lze pomocí telefonu dělat. Brzy byl ve phreakingu lepší jak jeho učitelé a tím byla předurčena Kevinova životní cesta na nejbližších patnáct let.

Všeobecně známou dráhu hackera zahájil už na střední škole. Motivem bylo přijetí skupinou osob, kteří byli Kevinovi podobní. Označení hacker bylo tenkrát používáno pro lidi, kteří trávili čas experimentováním s počítači a programy, psali efektivnější programy, vymýšleli lepší řešení problémů. Dnes je tímto slovem označován člověk, který je vnímán jako zločinec. Kevin ho však stále používá ve smyslu dřívějším a jemnějším.

Po absolvování střední školy studoval informatiku v Computer Learning Center v Los Angeles. Po několika měsících správce školní sítě zjistil, že Kevin objevil díru

v operačním systému a získal veškerá práva na počítačích IBM. Nikdo z vrcholných odborníků z řad učitelů nedokázal odhalit, jak toho Kevin dosáhl. Tehdy přišla nabídka, jaká se neodmítá, buď v rámci zápočtové práce opraví zabezpečení školního systému, nebo bude vyloučen. Volba byla jasná, tedy první varianta, díky níž mohl dokončit školu s vyznamenáním.

Mnoho výzev, úspěchů a uspokojení mu poskytovala práce soukromého detektiva, kdy využíval svých dovedností v přesvědčování lidí, aby činili tak, jak běžně pro neznámé osoby nečiní, navíc byl za to placený.

Vlastnostmi ideálního sociotechnika jsou manipulativní sklony a um lidi přesvědčovat a ovlivňovat. Možnosti, jak rozdělit manipulátora jsou dvě, jednou je manipulátor podvodník, který se snaží obrat lidi o peníze, a druhou sociotechnik toužící získat informace. Své dovednosti pravidelně piloval pomocí telefonu, kdy se snažil získat nejrůznější informace, aniž by nějakou z nich potřeboval.[7]

Kevin byl několikrát uvězněn a odsouzen. V minulosti byl FBI dle vlastního názoru fiktivně obviněn z činů, které neprovedl. Na základě tohoto obvinění byl odsouzen na jeden rok vězení s tříletou podmínkou. Pro porušení podmínky několik let utíkal. Po dopadení se obhajoval tím, že pokud stát už dříve nehrál dle pravidel, nezbylo mu nic jiného. Po posledním propuštění v roce 2000 mu bylo zakázáno používat všechny komunikační technologie mimo pevné linky, to u soudu napadl a spor vyhrál. Také mu bylo zakázáno napsat knihu nebo natočit film o svém životě. V roce 2002 vydal knihu „Umění klamu“.

Obr. 1 Kevin Mitnick [11]

Kevin změnil svůj život a dal se na druhou stranu bariéry. Dnes je z něj uznávaný expert na bezpečnost počítačových systémů. Vždycky tvrdil, že veškeré jeho jednání bylo čistě ze zvědavosti. Nikdy nezničil data na počítači, do kterého pronikl a nikdy se ani žádným způsobem pomocí získaných dat nijak neobohatil.[6]

3 Psychologie sociotechnika

Na základě dlouhodobého sociologického výzkumu bylo zjištěno šest základních vlastností lidské povahy, které se projeví při pokusu podřídit se něčí vůli. Tyto lidské vlastnosti, s jejichž pomocí dokáže člověk lépe manipulovat s někým jiným, popsal ve své knize profesor Robert B. Cialdini.[8]

3.1 Autorita

Autority můžeme rozdělovat na dvě skupiny, tou první je autorita neformální (přirozená) a tou druhou je autorita formální.

S autoritami se setkáváme již od narození. První autoritou jsou pro nás rodiče, kteří nás vychovávají. Následně do našeho života přichází autorita další, v podobě učitele ve škole. Po školní docházce přichází zaměstnání, kde nám je autoritou vedoucí oddělení, či jiný výše postavený zaměstnanec firmy.

Důsledkem těchto životních etap je pro nás přirozené, se podřídit autoritě v případě nějakého požadavku, který po nás vyžaduje splnit, například dodat nějakou důležitou informaci útočníkovi vydávajícího se za zaměstnance právního oddělení.

3.2 Sympatie

V běžném životě se snažíme obklopovat lidmi, kteří nám jsou sympatičtí a kteří mají s námi něco společného, mohou to být společné koníčky, názory nebo životní postoj a další.[41] Sociotechnik tak může využít některý ze společného zájmu a po získání důvěry je pak velmi snadné zmanipulovat oběť k získání potřebné informace.

Příkladem může být „společné nadšení“ pro tenis, kdy se lidé baví nejen o společném zájmu, ale v důvěře ke druhému i o soukromých věcech.

3.3 Vzájemnost

„Jak chcete, aby lidé jednali s vámi, jednejte i vy s nimi.“ (Bible - kniha Lukáš 6, 31)

Takto manipulovat s lidmi je snazší v momentě, kdy sociotechnik nejprve poskytne nějakou službu potencionální oběti, která se ve snaze „oplatit“ dobrý skutek chytne do nalíčené pasti.

Jako příklad můžeme uvést situaci, kdy sociotechnik předstírá, že je správce sítě, který varuje před možným virem, který není detekovatelný antivirovým programem a pomáhá oběti lépe zabezpečit počítač před únikem citlivých dat. Pak může požádat svou oběť o změnu nového hesla přes nastrčený formulář.[41]

3.4 Závazek a důslednost

Tento princip je velmi těžko odhalitelný, jelikož poslední krok rozhodnutí je na ovlivňovaném a útočník se pak může bránit, že není tím, kdo učinil špatné rozhodnutí.

Podstatu tohoto principu vystihuje Cialdini, kdy říká, že v případě rozhodnutí pocítíme vnitřní tlaky k tomu, abychom se zachovali v souladu s daným rozhodnutím. Dále také tvrdí, že všichni občas sami sobě lžeme, abychom uchovali myšlenky a pocity v souladu s tím, co jsme udělali nebo se udělat chystáme.[40]

3.5 Společenský souhlas

Tendence lidí přijmout nebo schválit něco, co již před nimi jejich kolegové přijali a schválili.[10]

Ukázkou může být vyplnění dotazníku, který již vyplnili kolegové, kde je oběť vyzvána k zadání osobních údajů pro zaslání statistiky výsledků. Lidé jsou velmi zvědaví, proto je pravděpodobné, že chtěné informace útočník dostane.

3.6 Vzácná příležitost

Situace, při které jsme zařazeni do úzké skupiny „šťastlivců“, kdy můžeme získat zdarma nějaký dar nebo můžeme vyhrát nějaký finanční obnos.

Běžný uživatel se setkává nejčastěji při procházení různých webových stránek s vyskakujícími pop-up okny vybízejícími ke kliknutí, aby mohlo dojít například k vyplacení výhry, kterou získáváme jako jubilejní x-tý návštěvník. Po kliknutí jsme přesměrováni na útočníkovu stránku, kde jsme vyzváni k zadání osobních údajů pro kontakt. Tyto údaje mohou být následně použity pro narušení bezpečnosti firemní sítě.[41]

V rámci firmy může jít například o rozeslání emailu, kde je požadováno zadat osobní údaje pro úplnost databáze a prvních x zaměstnanců dostane například volné vstupenky do divadla.[10]

4 Budování důvěry

Proniknutí do zabezpečeného systému firmy začíná ziskem informace nebo volně dostupného dokumentu, který nemá zdánlivě větší význam. Většina lidí ve firmě tedy nenachází důvod k ochraně takto dostupných informací, zdánlivě bezvýznamných. Útoky jsou nejčastěji vedeny proti lidem, kteří si neuvědomují důležitost informací, s nimiž pracují, a které dále poskytují jiným. Prvním předpokladem úspěšného útoku sociálního inženýra je však domněnka, že zaměstnanci firmy nejsou hlupí a očekává podezření či odpor, na něž musí být sociotechnik připraven a je nucen předvídat otázky potencionální oběti a mít na ně připravené odpovědi.

Po zisku předběžných informací z volně dostupných zdrojů se sociotechnik zaměří na vybudování důvěry a vztahu s obětí. Útočník si je vědom časové náročnosti jeho práce a nemožností vytvářet tlak na oběť pro zisk informací. Připravený první rozhovor sociotechnik obvykle směřuje na každodenní záležitosti, tím obejde podezíravost napadeného. Postupně do dalších rozhovorů nenápadně vkládá nevinné otázky vedoucí k zisku potřebných informací. Velmi často oběť nemá vůbec žádné tušení, že se stala zdrojem žádoucích informací.

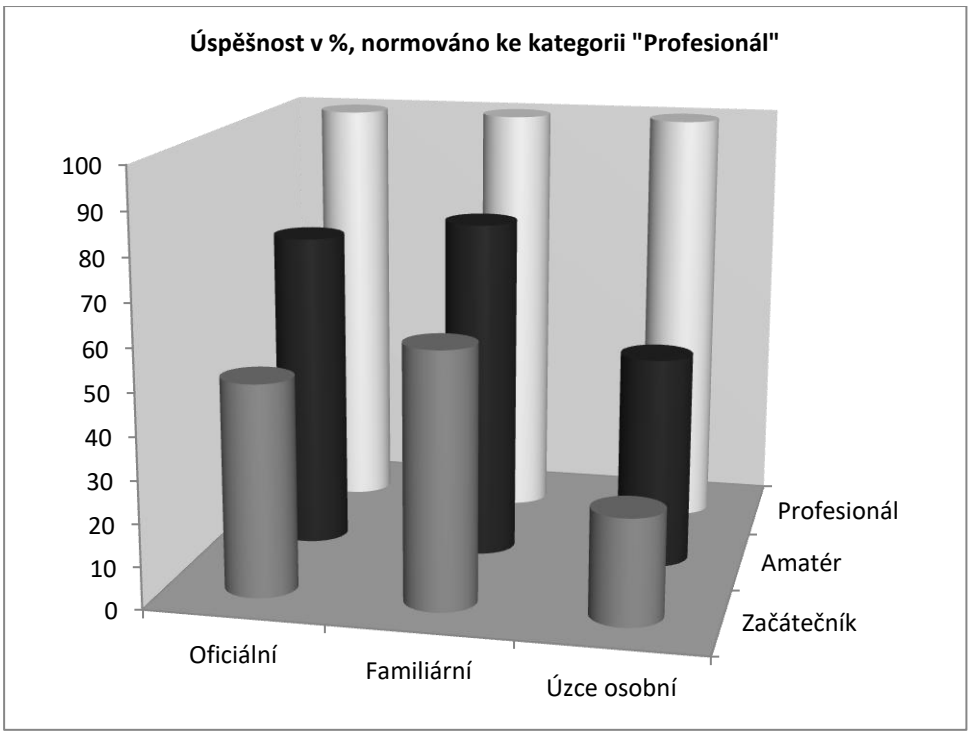
Znalost firemního a odborného žargonu při komunikaci s obětí je nutnou a nezanedbatelnou součástí práce sociotechnika. Správnost použití různých výrazů či slovních spojení běžných ve firemním prostředí nebo v daném oboru napomáhá k přesvědčení oběti, že jedná s někým ze své firmy. V opačném případě, kdy útočník působí nejistě nebo se vyjadřuje neobvykle k danému prostředí, oběť zbystří a útočník se pro ni stává podezřelým. Proto je užití správného žargonu, odkazování na další zaměstnance, sebejisté vystupování základní vybaveností zkušeného sociotechnika a je mu nápomocno k nepozorovanému pohybu uvnitř firmy.

Vhodné zvolení komunikační strategie je důležité pro úspěšnost útoku. Tyto strategie můžeme rozdělit do tří základních přístupů. Konkrétní přístup je sociotechnikem volen na základě odhadu mentality vybrané oběti:

- Oficiální komunikační strategie – útočník působí seriózně, zásadně nepoužije familiární tón. Sociotechnik nemusí být znalý osobních údajů oběti, ovšem je kladen důraz na profesionalitu komunikace a orientaci v odborném zaměření oběti.

- Familiární komunikační strategie – vychází se ze znalosti některých osobních údajů a osobnostních rysů cílové osoby. Sociotechnik většinou vyhledává osoby opačného pohlaví, kdy používá žertovný až flirtující tón. Tato strategie vyžaduje orientaci v prostředí, ale také i schopnost modulovat tón hlasu a herecké nadání.

- Úzce osobní komunikační strategie – je založena na vyvolání dojmu velmi důvěrné a dlouhodobé znalosti cílové osoby. Tato strategie je z těchto přístupů nejsložitější. Přístup je závislý na důkladné znalosti oběti. Útok může snadno selhat z důvodu nepřesvědčivosti nebo neznalosti. Zvolená strategie tak vyvolá vzrůstající nedůvěru.[9]



Obr. 2 Úspěšnost útoků v %, normováno ke kategorii "Profesionál" [9]

5 Metody útoků sociotechnika

Sociotechnik se snaží využít slabých míst v bezpečnostní politice organizace, své nadání v manipulaci a zosnované situace pro útok. Přípravu sociotechnik zahajuje průzkumem volně dostupných zdrojů informací, obvykle webových stránek organizace, nejrůznějších marketingových materiálů, apod. Volně dostupnými zdroji mohou být mimo jiné informace, které můžeme získat dotazem na tiskové oddělení firmy, uplatněním zákona o svobodném přístupu k informacím. Občas se člověk nestačí divit, co vše lze pomocí internetového vyhledávače zjistit o dané organizaci. Jedná se hlavně o telefonní a emailové kontakty, které zdánlivě působí jako neužitečné informace, ovšem pro sociotechnika jde o velmi důležitá data pro započetí sociotechnického útoku.

Všechny metody využívané k sociotechnickému útoku mají tentýž záměr – oklamat oběť útoku. Mezi hlavní pravidla ovlivňující výsledek sociotechnického útoku patří:

- umění útočníka přesvědčit svou oběť, že má nad situací kontrolu, vše koná ze své vlastní vůle a bude za to odměněna. Odměna však nemusí být nutně hmotná, postačí i dobrý pocit z potěšení nadřízeného nebo z dobrého skutku příteli.
- působit přátelsky. V momentě, kdy vše selže, se přátelsky usmívat a mít vlídný tón hlasu, který může výrazně pomoci i v mnohdy již prohrané situaci. Převážná část z nás ráda věří v dobrosrdečnost ostatních lidí, v poctivost našich kolegů.
- nebýt příliš horlivý, nadmíru se nevtírat a nevyvíjet velký tlak na oběť. To mnohokrát vede k podrážděnosti a podezíravosti oběti a následně k neúspěchu útočníka.
- předchozí pravidlo neplatí s výjimkou situace, kdy se útočník vydává za vysoce postavenou osobu a oběť by se měla dle předpokladu zaleknout a vyhovět požadavku.

S výše uvedenými pravidly využívá sociotechnik i psychické vlastnosti oběti. Toto spojení pak v podstatě představuje „neopravitelné bezpečnostní mezery“. Mezi největší slabá místa využívaná pro sociotechnické útoky v této oblasti patří:

- zbavení se odpovědnosti – oběť spíše uskuteční útočníkův požadavek, když má pocit, že na jeho bedrech neleží celá zodpovědnost. K navození tohoto pocitu stačí podotknout zapojení dalších kolegů do celého procesu nebo prohlášení, že je vše schváleno vyšším nadřízeným a tím pádem je vše v naprostém pořádku.

- lepší postavení v organizaci – jestliže oběť nabude dojmu, že mu splnění žádosti umožní získat nějaké výhody, na které jiní kolegové nemohou ani pomyslet, pokaždé ho to povzbudí žádosti vyhovět.

- důvěra – vzbudit důvěru u oběti je jedním z nejdůležitějších faktorů v sociotechnickém útoku. Budování důvěry je časově velmi náročné, leč se útočníkovi tento způsob značně vyplácí.

- morální povinnost – přesvědčit cíl útoku, že se děje bezpráví a tím vytvořit dojem, že mu může zabránit jednáním, kterého se sociotechnik dožaduje.

- pocit viny – nikdo se nechce cítit proviněný, z tohoto důvodu se každý pokouší těmto pocitům vyvarovat. Zavedení oběti do situace, kdy je na ni vytvořen psychický nátlak, vyvolá touhu vyhnout se pocitům viny a donutí ji konat, jak útočník potřebuje.

- touha být prospěšný – lidská vzájemnost, ohled na dobro druhého podnítí člověka pomoci někomu v nesnázích, navodí mu to příjemný pocit.

V případě, kdy sociotechnik ví, jak firma funguje, je ideálním cílem útoku nový zaměstnanec. Výhodou útočníka je neznalost nového zaměstnance. Předpokládá se, že po pár týdnech v novém zaměstnání nemůže znát všechny své nové kolegy a tímto směrem se sociotechnik orientuje. Nový zaměstnanec se snaží udělat dobrý dojem, a proto ochotně projevuje svou vůli spolupracovat rovněž i se značnou rychlostí vyřizování požadavků. Je velmi rád, když se o něho v začátcích někdo zajímá, v této situaci sociotechnik, a snaží se mu být nápomocen i za okolností, které vyvolá sám útočník. Nový pracovník pak projevuje snahu oplatit pomoc, která mu byla poskytnuta a ztrácí ostražitost.

Nejen nový zaměstnanec je vhodným cílem sociotechnického útoku. Jiným případem může být obrácení rolí, vydávání se za nového zaměstnance s prosbou o pomoc. Tato praktika je sociotechniky často využívána. Běžně se setkáváme se

situacemi, kdy se nový pracovník špatně orientuje v některých aplikacích, proto je správce systému zvyklý na podobné situace, kdy musel něco někomu vysvětlovat nebo mu s něčím pomáhat. Správce tak sociotechnikovi věnuje pozornost a napomáhá mu získat to, co potřebuje. Schopný sociotechnik se neobává kontaktu s policií, v nezbytném případě ji sám kontaktuje a pokouší se získat potřebnou informaci.[9]

5.1 Přímý přístup

Situace, kdy útočník přímo vyzve svou oběť, aby mu sdělila přihlašovací jméno a heslo. Tato metoda je velmi riskantní, ale není nemožná. Když útočník zacílí na neznalého uživatele, který je v časové tísni, má velkou šanci na úspěch. Zvýšit potenciální úspěch útoku může budování důvěry. Pokud útočník naváže blízký vztah se svou obětí, budou „dobrými známými“, nemá oběť důvod „svého známého“ - útočníka podezřívat v případě, kdy potřebuje pomoc s řešením problému. V tento okamžik si pro rychlejší vyřešení problému může útočník vyžádat od oběti uživatelské jméno a heslo.[4]

5.2 Bezmocný uživatel

Jedná se o způsob útoku, kdy se útočník vydává za nového zaměstnance nebo zaměstnance, který není moc zručný v ovládání počítače a například zapomněl své heslo a nutně potřebuje pokračovat na svém projektu. Lidé rádi vyjdou novému kolegovi vstříc a poskytnou mu dočasně své přihlašovací údaje, případně mu administrátor sítě sdělí nové heslo pro přístup.[4] Může jít i o obrácené role, kdy si sociotechnik vybere za cíl svého útoku nového zaměstnance organizace. Nový zaměstnanec ještě není úplně znalý bezpečnostních pravidel a firemního žargonu. Koho by napadlo, že se může stát v prvních dnech v novém zaměstnání obětí důmyslného útoku. Útočník se v tomto případě vydává za „kolegu“ v nouzi a žádá nového pracovníka o pomoc. Pracovník, nejspíše pomoc neodmítne, aby se dobře zapsal mezi svými novými kolegy, a tak nevědomky sociotechnikovi pomůže.[10]

5.3 Významný uživatel

Útočník se vydává za někoho z vedení firmy a předstírá, že má potíže, které potřebuje urychleně vyřešit. Požádá oběť, aby mu sdělila, který software se používá pro vzdálený přístup, jeho konfiguraci a další informace potřebné pro přihlášení k serveru. Útočník si pravděpodobně řekne i o uživatelské jméno a heslo oběti, které připomene, že

se jedná o urgentní záležitost. Jestliže sociotechnik působí svým počínáním věrohodně, má vysokou šanci na úspěch, k tomu mu může pomoci patřičná dříve získaná znalost firemního prostředí a zaměstnanců. Zaměstnanec zpravidla nechce žádné potíže s nadřízeným a už vůbec ne možnou výpověď, proto žádosti nejspíše vyhoví.[4]

5.4 Administrátor

Sociotechnik předstírá, že je administrátorem sítě nebo členem helpdesk týmu. Svou oběť kontaktuje buď emailem, nebo telefonicky. Požadavku sociotechnika pravděpodobně řadoví zaměstnanci vyhoví, jelikož nejsou proškoleni vůči sociotechnickým útokům a navíc pro ně člověk na některé z těchto pozic působí věrohodně a autoritativně. Na základě dobře vymyšleného scénáře, kdy je oběť postavena do situace, aby zadala uživatelské jméno a heslo, získává útočník přístup k uživatelskému účtu oběti.

Typickým scénářem může být situace, ačkoli jde o klam oběti, kdy byla „nabourána“ firemní síť a odcizeno několik hesel. V tomto momentě útočník vyzve oběť k urychlenému zadání nového hesla. Pod časovou tísní člověk obvykle nedokáže zadat heslo takové, aby si ho dobře pamatoval, a tak mu útočník poradí prozatímní heslo (například „Heslo12345“) a vyzve ho, aby si nové heslo zadal po jeho vymyšlení. Měli bychom mít však na paměti, že hesla se nikomu nedávají.[11]

5.5 Reverzní sociální inženýrství

Jedná se o značně pokročilou, avšak velmi úspěšnou metodu. Útočník předpřipraví sled událostí tak, aby se na něho sama oběť obrátila s prosbou o pomoc.[11] Do této situace se může dostat i sám technik nebo správce sítě, který není všeznalý a pomoc hledá na síti. To představuje otevřená vrátka pro sociotechnika, který se může vydávat za člověka, který je znalý problému a může tak pomáhat s jeho řešením. Samotný problém mohl předtím způsobit sám sociotechnik a pak už jen vyčkává, až se oběť obrátí s prosbou o pomoc.[9]

Reverzní sociální inženýrství má tři základní fáze:

a) Sabotáž – navození krizové situace na straně oběti (např. email s upozorněním před novým virem, aplikace tvářící se jako antivirus oznamující přítomnost viru, apod.)

b) Inzerce – nabídka řešení vzniklého problému (např. bezpečnostní konzultant)

c) Pomoc – útočník skrytý za identitu bezpečnostního konzultanta „odstraní“ bezpečnostní problém, ale současně nasazuje svůj vlastní software

Příkladem z nedávné doby může být situace, kdy se uživateli zobrazilo pop-up1 okno tvářící se jako antivirus, který dokáže virtuálně zkontrolovat osobní počítač. Každá kontrola končila oznámením o infikaci počítače. Po stisknutí tlačítka OK byla oběť přesměrována na důvěryhodně vypadající webové stránky, kde je možné si zakoupit „účinný“ antivirový software od AVG2.[12]

6 Mechanismy sociotechnického útoku

Pro sociotechnický útok můžeme využít různé mechanismy, které jsou obvykle použité pro přímou komunikaci. Mezi nástroje sloužící k přímé komunikaci s okamžitým spojením můžeme zařadit ICQ, IRC, NetMeeting nebo také webové chaty. Elektronická pošta je dalším velmi využívaným a mocným nástrojem přímé komunikace. Základem celého sociotechnického útoku, i když používáme jiných prostředků, je zneužití lidských vlastností (důvěra, lenost, zvědavost, apod.) pro zisk potřebné informace. Současně jsou na oběť aplikovány metody, aby nabyla dojmu, že se rozhodla sama a správně. Uživatel je obecně chápán jako nejslabší článek celého firemního zabezpečení, a tak je využit, aby sociotechnik nemusel obcházet jak hardwarové, tak softwarové zabezpečení.[9] Útočník časem navazuje kybernetické přátelství, pomocí kterého ovlivňuje svou oběť. Může jí například doporučit „lepší“ zabezpečovací software nebo nějakou šikovnou aplikaci pro usnadnění práce či pro zábavu.

Jiným způsobem oslovení oběti je využití telefonu. Sociotechnik se nejčastěji představí jako firemní autorita s požadavkem na vyřešení problému. Oběť se dostává do situace, kdy zvažuje, zda vyhovět nebo nevyhovět. Je-li ve firmě velké množství zaměstnanců, vzrůstá šance na kladné vyřízení požadavku.

6.1 Phreaking

Termín „phone phreaking“ vzešel ze slovního spojení „free use of the phone“ (přeloženo do češtiny jako volné užívání telefonu). Phreaking je soubor technik umožňující manipulaci s telefonní sítí.[13] Hlavním záměrem tohoto mechanismu bylo bezplatné telefonování nebo odposlouchávání hovorů. Za phone phreakera je označována člověk, který rád zkoumá telefonní systém, experimentuje s ním a snaží se pochopit jeho funkce. Počátek phone phreakingu se datuje ke konci padesátých let, jeho největší rozkvět byl na přelomu šedesátých a sedmdesátých let. Podle Phila Lapsleyho, který napsal knihu „Exploding the Phone“ věnující se phone phreakingu od historie až po současnost, lze phreakera označit, buď jako *„osobu, která je posedlá učením se, zkoumáním nebo hraním si s telefonní sítí“*, nebo jako *„osobu, která má zájem o volání zdarma“*.[14] Phreaker trávil mnoho času připojením na telefonní síť, kdy odposlouchával různé zvuky (zvuk pro vytáčení, apod.), aby pochopil, jak jsou hovory

směrovány. Dále četl různé technicky zaměřené časopisy, které napomáhaly pochopení fungování telefonní sítě.

Jakmile phreakeři pochopili fungování sítě, začala vznikat elektronické zařízení zvaná modrá, černá a červená krabička, která jim umožňovala bezplatně volat. Krabičky někteří z phreakerů používali k odposlechům. Mnoho z nich policie nebo FBI vyslýchala a zatkla.

Blue box (modrá krabička) – jde o elektronické zařízení generující stejné tóny, jaké využívá operátor, například pro přepojení dálkových hovorů. Tón o frekvenci 2600Hz znamenal volnou linku. Tyto krabičky se využívaly jak pro bezplatné hovory, tak pro odposlechy.

Black box (černá krabička) – zařízení, které umožňovalo hovory bez poplatku. Šlo obvykle o odpor nebo Zenerovu diodu připojenou do série s telefonní linkou, které ovlivňují napájecí napětí, pomocí kterého se rozpoznává, co se má stát (tón pro oznámení „obsazeno“, zahájení fakturace, apod.) Do obvodu se často přidával kondenzátor, aby nedocházelo k zeslabení signálu přenášející hlas.

Red box (červená krabička) – přístroj, který simuluje zvuk padající mince v telefonní budce, tedy sloužící k oklamání systému a bezplatnému hovoru.[15]

Phreaking jako takový nelze pokládat za sociální inženýrství, jelikož neútočí na lidi, ale na systém. Souvislost mezi phreakingem a sociálním inženýrstvím můžeme nalézt u jména Kevin Mitnick, který využíval telefonní síť pro zisk informací. Kevin začal svou „kariéru“ právě u phreakingu, který mu ukázali jeho přátelé. Phreaking, použitý během sociotechnického útoku, nám může pomoci k zahlazování stop při mechanismu vishing, kdy bude těžce dohledatelné, odkud útočník volal.

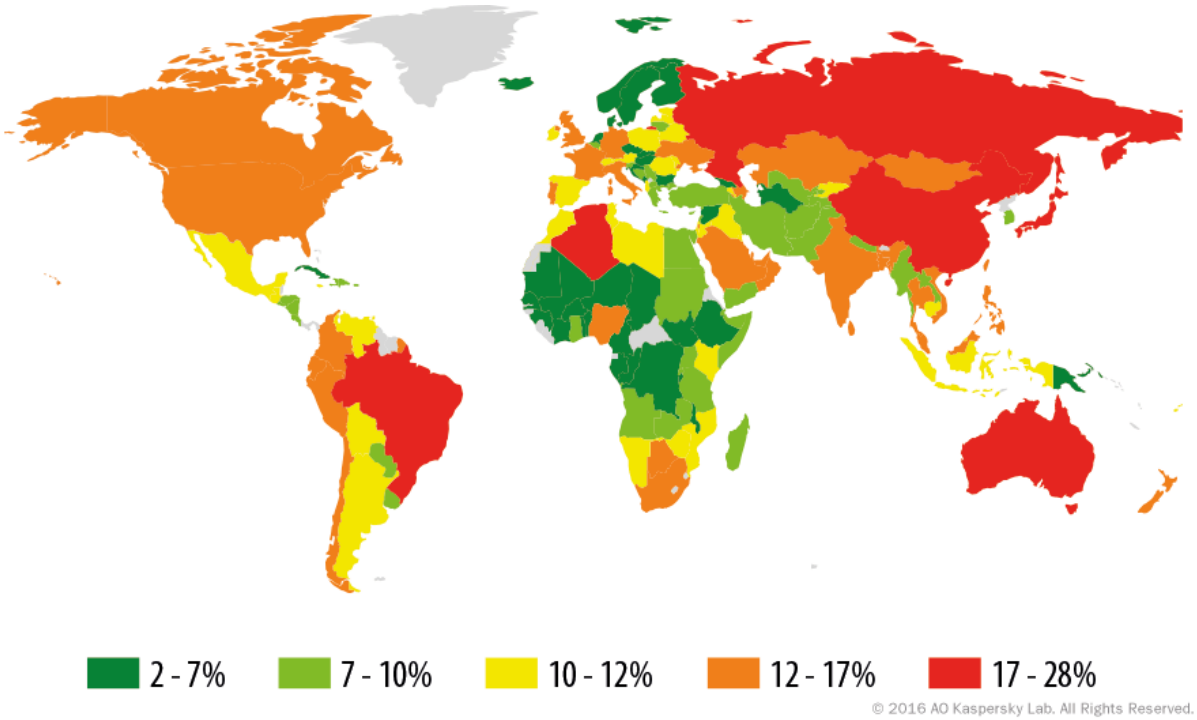
V současné době se tento mechanismus, vzhledem k měnící se technologii, téměř nepoužívá. Zastaralé sítě jsou nahrazovány modernějšími technologiemi, a jelikož jsou útočníci učenliví, dochází v době nedávné k obdobnému mechanismu útoku nazývajícímu se Vishing.[16]

6.2 Phishing

Útok zvaný „phishing“ (česky přeloženo jako rybaření nebo také rhybaření) je nejčastějším mechanismem útoku sociotechnika. Pojem phishing vznikl spojením slov fishing a phreaking.[17] Někdy je uváděno, ačkoli mylně, že vznikl ze slov „password haversting fishing“ (přeloženo do češtiny jako „sběr hesel rybařením“).[18] S rybařením má tento mechanismus mnoho společného. Sociotechnici loví stejně jako rybáři, jen jsou jejich úlovkem místo ryb informace. Rozešlou zprávy a poté vyčkávají, až se někdo chytí a zareaguje na ně.[19] Slovem phishing označujeme klamavé emaily, které mají za úkol z obětí útoku vylákat citlivé informace.

Phishing se poprvé objevil v roce 1995 ve spojitosti s firmou America Online (AOL), poskytovatelem internetových služeb. Z počátku nebyla pro útok využívána elektronická pošta, ale protokol IRC (Internet Relay Chat) pro komunikaci v reálném čase nebo systém upozorňování na nové zprávy od AOL. Útočníci (phisheři) se vydávali za administrátory AOL, oznamovali obětem vznik problému s vyúčtováním a vyzvali je k obnovení údajů o platební kartě a přihlašovacích údajů. V té době byl phishing velmi úspěšný, jelikož připojení osobního počítače k internetu bylo novinkou a nebylo všeobecné povědomí o těchto útocích.[20]

Dnes se využívají hlavně emailové zprávy, které se tváří jako oficiální zprávy od banky či jiné instituce (Paypal, Paysec, eBay, apod.). Obsahem emailu jsou mimo jiné odkazy na formulář pro zadání citlivých údajů. Hlavním úkolem je zisk informací o platebních kartách (číslo platební karty, platnost, CVV kód), přihlašovací údaje a jiná osobní data. V počátcích byly zprávy psány lámavou češtinou, takže působily hned podezřele (například oslovení na začátku emailu „Drahoušek zákazník“). V současnosti vypadají emaily velmi věrohodně a jsou velmi těžce rozeznatelné.[21] Velmi častými oběťmi v ČR jsou klienti České spořitelny a ostatních bank, ty o možných útocích své klienty pravidelně informují a zároveň na svých webových stránkách zveřejňují základní informace o phishingu.



Obr. 3 Uživatelé napadení phishingem v roce 2016 v % [45]

Phishingové emaily bývají mnohdy označovány jako spam. Spam můžeme obecně dělit na několik skupin:

- nevyžádané obchodní emaily – zprávy rozesílané skutečnými firmami za účelem oslovení potenciálního zákazníka
- neodpovídající obchodní sdělení – emaily zaslané reálnými firmami, které jsou nadále posílány i po odhlášení odběru těchto zpráv
- obchodníci s emailovými adresami – skupiny lidí tvořící seznamy příjemců za účelem dalšího prodeje
- scam – klamavá, lákavá nabídka vytvořená za účelem zisku financí[20]

6.2.1 Nigerijské dopisy

Nejznámější scamem jsou tzv. nigerijské dopisy (také označované jako Scam 419). Původ těchto dopisů směřuje do Nigérie, tomu odpovídá i číselné označení 419. Paragraf 419 znamená v trestním právu v Nigérii podvod.[22] Dříve se rozesílaly formou dopisů, později faxem a dnes nejčastěji emailem. Jde o dopisy, které mají za účel vylákat

z obětí peníze. Obsahem dopisu je sdělení od neznámého člověka, který zdědil velké množství peněz, aby je mohl získat, potřebuje uhradit administrativní poplatky. Za uhrazení poplatků nabízí příjemci část peněz, ovšem s dobou se objevují další a další poplatky a převod části peněz se neustále oddaluje. Tento sociotechnický útok se nedá považovat za phishing, i když je využíváno emailu, jelikož útočník nemanipuluje obětí, aby vyzradil citlivé údaje.[23]

6.3 Vishing

Mechanismus zvaný „vishing“ můžeme označit jako technologického nástupce phreakingu. Vishing vychází ze slovního spojení „voice phishing“ (česky přeloženo jako hlasové rybaření). K tomuto typu útoku se používá technologie VoIP. Technologie VoIP umožňuje bezplatné volání přes internet. Společností, která tuto službu nabízí je například Skype. Jedná se o podvod, který je založen na stejném principu jako phishing, jen se k němu využívá telefonního hovoru a ne emailu. Vishing se stále více rozšiřuje, kvůli lepší ochraně proti nevyžádané poště (phishingovým emailům), avšak phishing stále výrazně vede před ostatními mechanismy sociotechnického útoku. Pomocí vishingu se sociotechnik snaží z oběti vylákat osobní údaje, hesla či čísla platebních karet.[24] Oběti je během telefonátu nebo hlasové zprávy telefonním automatem oznámeno, že se vyskytl problém na jeho bankovním účtu a je vyzván, aby se obrátil pro vyřešení problému na podvrženou bezplatnou telefonní linku.[25]

Lidé telefonům důvěřují mnohem více než internetu a velmi často si neuvědomují, že i přes telefon se mohou stát obětí promyšleného útoku sociotechnika. Pocit, který máme z komunikace s další osobou, uměle vzbuzuje důvěru. Útoky vedené tímto mechanismem jsou natolik promyšlené, že je značně obtížné rozpoznat, zda se jedná o podvod nebo o skutečného operátora. V tomto momentě je velmi důležité, aby byl uživatel obezřetný a prověřil si, s kým skutečně jedná.[26]

6.3.1 Smishing

Jde o tentýž podvodný mechanismus jako je vishing jen s tím rozdílem, že útočník pro kontaktování své oběti nepoužívá hlasový rozhovor, ale sms zprávu. V sms zprávě jsou uvedené instrukce, jak má uživatel postupovat při řešení daného problému, aniž by tušil, že se stal obětí rafinovaného sociotechnického útoku. V sms bývají informace například o podezřelé transakci, kterou je nutno potvrdit nebo zamítnout telefonátem

na číslo uvedené v sms zprávě. Pod uvedeným číslem se často skrývá automat, jenž postupně vede oběť útoku všemi kroky, kterými ho má provést (od zadání podvrhnutého autorizačního kódu, přes klientské číslo až po heslo k internetbankingu).[27]

6.4 Pharming

Vzhledem k čím dál většímu povědomí široké veřejnosti o phishingu přešli sociotechnici k mnohem důmyslnějšímu mechanismu získávání uživatelských jmen a hesel. Mechanismus se nazývá „pharming“ („farmaření“) a má dvě metody. První z nich je velmi efektivní, avšak pro sociotechnika nadmíru složitá a to její použití značně omezuje. Druhá je jednodušší, ale na druhou stranu se jí lze snadněji bránit, což je nevýhodou útočníka.

Pharming se nezakládá na přímém oslovování uživatele, ale útočí na DNS server. DNS (Domain Name System) je hierarchická databáze udržující seznam názvů internetových domén a jim příslušných IP adres. Jestliže se útočníkovi podaří změnit záznam na špatně zabezpečeném DNS serveru, uživatelé se při zadání určité adresy ve webovém prohlížeči (například svého internetbankingu) dostanou na podvržené stránky. Pokud je falešná webová stránka kvalitně zpracovaná, je vysoká šance, že i zkušený uživatel nepozná rozdíl. Rozdíl lze poznat důkladnou kontrolou certifikátu, který není sociotechnik schopen dokonale zfalšovat.

Druhou metodou je lokální pharming, cílený na osobní počítače uživatelů. Počítače s nainstalovaným operačním systémem Windows obsahují hosts soubor, který má podobnou funkci jako DNS server, obsahuje názvy domén a příslušné IP adresy. V případě změny tohoto souboru je efekt stejný jako u varianty s DNS serverem.

První metoda je sice nezávislá na klientských počítačích, ovšem je nutné překonat zabezpečení DNS serveru. Jelikož DNS servery představují páteř internetu, patří k nejlépe zabezpečeným serverům. Najít chybu v jejich zabezpečení a využít ji tak, aby si toho správci nevšimli, je neskutečně obtížné, proto se útočníci zaměřují na druhou metodu.

Změna hosts souboru je možná v momentě, kdy má útočník schopnost do něho zapisovat. Tuto schopnost může sociotechnik získat na základě instalace trojského koně,

který provede změnu, ideálně pomocí vzdáleného příkazu. Trojský kůň může být zaslán jako příloha emailu nebo si ho oběť na základě falešného emailu sama stáhne nebo si ho stáhne jako rozšíření skutečné aplikace. Je-li instalace trojského koně a zároveň změna souboru úspěšná, probíhá útok výše popsaným způsobem.[28]

6.5 Baiting

Mechanismus vycházející z anglického slova „bait“ (česky „návnada“). Oběti útoku je podstrčena návnada, která u ní vzbudí zvědavost. Díky ní se uživatel obvykle chytí do pasti, kdy si myslí, že má příležitost získat něco jedinečného, avšak je oklamán.[29] Návnada bývá zpravidla ukryta na USB flash discích, CD-R, DVD-R nebo nějakém jiném přenosném médiu. Paměťové médium pak útočník zanechává na frekventovaném místě, kde je velká šance, že si ho někdo všimne. Přenosné médium útočník opatří popiskem vzbuzující zmíněnou zvědavost, například „platy zaměstnanců“ nebo názvem nově vydané aplikace, tedy popiskem, co uživatele na první pohled velmi zaujme. Samotné médium musí útočník donést do uvedených prostorů, kde jej zanechává. Tímto jednáním vzniká velká šance, že ho někdo zahlédne, čímž podstupuje vysoké riziko prozrazení. Jinou variantou doručení zařízení zaměstnanci je zanechání jej na recepci nebo zaslání poštou do firmy.

Po vložení přenosného média do osobního počítače, může dojít k automatickému spuštění a instalaci infikovaného souboru nebo se instalace spustí po otevření nakaženého souboru uživatelem. Následně mohou být odeslány informace o daném počítači a ty využity pro stažení dalších virů. Výhodou tohoto mechanismu je možnost infikování systému i bez připojení k internetu. Na médiu je přítomen požadovaný soubor pojmenovaný tak, aby působil věrohodně, ovšem obsah, který v prvopočátku vzbudil zvědavost, bývá přítomen na médiu jen velmi zřídka.[30] Historicky se tento mechanismus podobá Trojskému koni.[31]

6.6 Trashing

Mechanismus „trashing“ je také znám pod pojmenování „dumpster diving“, volně přeloženo jako „prohledávání odpadků“ nebo „prohrabávání popelnic“. Pokud jste někdy vyhodili něco s citlivými informacemi do koše, měli byste zpozornět, kdo se může k těmto informacím dostat. Prohledáváním odpadků v popelnicích může útočník získat důležité informace, které následně využije ke kontaktu se zaměstnanci firmy nebo přímo

ke vniku do firemní sítě.[30] Útočník nejprve zjišťuje, kam jsou odpadky vynášeny, zda jsou tříděny nebo jestli popelnice využívá více než jedna firma. Podstatné je, kde se popelnice nachází, jestli jsou volně přístupné nebo umístěné v zabezpečeném prostoru. V závislosti na místě, kde se popelnice nachází, můžeme uvažovat, zda se v případě trashingu jedná o trestný čin nebo nikoli, což je ale diskutabilní.

K prohledávání popelnic dochází obvykle za tmy, kdy je útočník oblečen do černé barvy, aby na sebe zbytečně neupozorňoval a unikl tak pozornosti ostrahy objektu. Metoda je to účinná a celkem bezpečná, jelikož nedochází ke konfrontaci s obětí, ale má své nevýhody. Jednou z nich je zdlouhavý proces získávání informací a tou druhou je špinavé prostředí, kde útočník materiály hledá.

Dumpster diver hledá v popelnicích papíry s informacemi o zaměstnancích, přihlašovací údaje a hesla, kontakty, bankovní transakce, technické nápady, apod. Nutně nemusí jít jen o vyhledávání informací na papíře, ať už skartovaném, nebo jen vyhozeném bez známky poškození, ale i o vyhledávání CD, DVD a dalších přenosných médií nebo o hledání harddisků (HDD). Mnoho uživatelů se domnívá, že smazáním dat z HDD zajistí, že data již nejdou získat zpět, opak je ale pravdou. Takto odstraněná data jdou zpětně obnovit za pomocí různých aplikací.[29]

Při vyhazování odpadků do koše musí zaměstnanec jednat v souladu s bezpečnostní politikou firmy. Stává se, že si současní i odcházející zaměstnanci berou materiály s citlivými daty domů, kde je často pro další nepotřebnost vyhazují do odpadků, k čemuž by nemělo docházet. Bezpečnostní politikou musí být jasně definováno, jaké materiály mohou být z firemních prostorů odnášeny domů a i ty by měly být po upotřebení nejlépe spáleny v kotli.[30]

7 Sociální sítě jako zdroj dat

7.1 Význam sociální sítě

Sociální sítě lze obecně charakterizovat jako soubor vztahů mezi lidmi, organizacemi nebo národy. Jedině lidé mají schopnost tvořit sociální sítě. Přesnější pojmenování pro tyto sítě je „společenské sítě“. Sociální sítě jsou jedním z projevů lidskosti. Lidé mají potřebu se sdružovat, někam patřit. Právě prostřednictvím sítí mají možnost komunikovat, někam se začlenit. Společenské sítě se vyznačují interakcí tváří v tvář, tudíž zahrnují rodinu, známé, kolegy z práce a další lidi z totožného geografického prostředí. [32]

7.2 Současné chápání pojmu

V současné době je pojem sociální síť nejčastěji používán v souvislosti s internetem. Chápeme ji jako internetovou službu umožňující uživatelům vytvářet veřejné nebo soukromé profily, prezentace, diskusní fóra. Dává nám prostor pro sdílení fotografií, videí, prostor pro tvorbu obsahu. Převážnou část obsahu na sociálních sítích tvoří sami uživatelé. Obsah je tvořen prostřednictvím příspěvků, veřejné komunikace, sdíleného obsahu. Velmi oblíbené jsou skupiny zaměřené na určité téma. Uživatelé by měli velmi pečlivě dbát na sdílený obsah, komu se zobrazuje a kdo ho může sdílet či komentovat. Potenciální zaměstnavatel, kterému zašlete životopis, můžeme projít váš profil a nevhodný obsah může ovlivnit vaše přijetí do zaměstnání.

„Rozmach sociálních sítí nastal v období takzvaného neomezeného internetu, který byl do té doby pro mnohé uživatele drahý a nedostupný.“ Mezi lidmi, nevyužívajícími těchto sítí, převládá názor, že sítě využívají výhradně mladí lidé. Realita ukazuje na opak, největší základnou sociálních sítí jsou dospělí uživatelé.

Zahraniční sociální sítě byly pro české uživatele do nedávné doby méně zajímavé až nezajímavé, mohla za to jazyková bariéra. S lokalizací těchto služeb došlo ke změně. K atraktivnosti těchto služeb přispělo využití nových technologií a trendů, zejména mobilní verze služeb. Nezapomínejme, že *„mnoho sociálních sítí je lokalizováno do českého jazyka, ale to z nich nedělá českou službu. Pamatujte, že v případě problémů na této síti, se podmínky řídí právem a zvyklostmi státu, ve kterém je zaregistrována. Domáhat se spravedlnosti, vyžaduje mnoho času a trpělivosti. Většina cizích služeb nemá*

ani technickou podporu v českém jazyce a je plně automatizována. Domoci se tak spravedlnosti je jednodušší na českých sociálních sítích, které, až na malé výjimky, nabízejí možnost spojení se s českým operátorem.“ [33]

7.3 Historie sociálních sítí

První náznaky sociálních sítí vznikly v 90. letech. Primárním účelem byla komunikace studentů s rodinami. První takto vytvořená síť byla theGlobe.com (1995). O pár let později vznikla síť sixdegrees.com (1997), podobnost se současnými sítěmi byla již větší. Byla tu možnost vytvořit si profil, propojit se s přáteli, prohlížet si profil ostatních uživatelů. V roce 2003 vznikla sociální síť MySpace.com vlastněná Rupertem Murdochem. MySpace jako první síť podporovala internetový marketing. Ve stejném roce vznikla první profesní sociální síť LinkedIn, podporující trh práce. O rok později vznikla na Harvardu síť Facebook (2004) používaná pro komunikaci mezi samotnými studenty. Během měsíce se k síti přihlásila více než polovina z 19 500 studentů univerzity. Dnes se jedná o největší světovou sociální síť vlastněnou Markem Zuckerbergem. Twitter byl spuštěn v roce 2006, slouží jako prostor pro mikroblogy. Sociální síť Google+ (2011) patřící společnosti Google, spojuje její služby v jednu. Jedná se o Youtube, Picasa, Gmail a další. Dále existují sociální sítě mající spoustu uživatelů, avšak pouze omezenou lokalizaci. Příkladem takovéto sociální sítě může být vk.com, celým názvem VKontakte (2006), používaná hlavně v Rusku a bývalých sovětských zemích. Jde o obdobu amerického Facebooku.[34]

7.4 Informace na síti

Na sociálních sítích o sobě můžete sdílet mnoho osobních údajů. Od barvy očí, data narození, zálib nebo informací, co na síti hledáte. Profil můžete doplnit také o profilovou fotografii. Bohužel tyto sdílené informace mohou být i zneužity. *„Proto se zamyslete, jaké informace o sobě chcete sdělit. Zveřejňujte pouze ty, které byste byli schopni vyvěsit na místě plném lidí, třeba zastávce autobusu nebo na školní nástěnce.“*[33]

Informací, kterou hledá či požaduje útočník k úspěšnému vniku do systému, může být i každá zpětná vazba. Zpětnou vazbou je „olajkování“ libovolného příspěvku, komentář pod příspěvkem, ať už vlastním nebo cizím, odpověď na zdánlivě nic neříkající dotazník, sdílení obsahu na zaměřené téma, apod. Všechny takto sdělené informace, ač neškodně vypadající, mohou být zneužity pro útok.

Sociální sítě jsou v dnešní době největší databází nijak netříděných soukromých informací o uživatelích. Málokdo z nich si je tohoto faktu vědom, proto je zde většinou velmi snadné získat při malém úsilí požadovanou informaci.

7.5 Ukázka zneužití informací ze sociální sítě

Na sociální sítí Youtube je k vidění mnoho různých videí. Jedno z nich, natočené belgickou reklamní agenturou, poukazuje na obsahy soukromých profilů jednotlivých uživatelů. Společnost Duval Guillaume udělala průzkum v belgickém hlavním městě Bruselu. Náhodně oslovovala kolemjdoucí, zda jsou ochotni se podrobit čtení z mysli. Bylo jim sděleno, že připravují televizní program s Davem v hlavní roli. Dave je postarší pán „umějící číst z mysli“. Vybrané osoby byly postupně zavedeny do provizorního stanu na ulici a svěřeni do rukou Davea. V místnosti sezení byly jen dvě židle a stůl. Dave postupně začal se „čtením z mysli“.

První ženě ve videu správně odhadl město, ve kterém studuje. Další ženě uhodl tetování na bedrech, a co je na nich vytetováno. Následující ženě cizince uhodl její národnost. Takhle pokračoval postupně u všech osob zapojených do průzkumu. Po sdělení obecných informací přešel k oznamování více soukromých informací, jako jsou číslo bankovního účtu, stavu na bankovním účtu, informaci o prodeji domu a konkrétní částky za něj, konkrétní utracené částky za oblečení, apod. Lidé podrobovaní výzkumu se nestačili divit, co vše o nich ví.

Pak přišel čas na odhalení celé skutečnosti, kdy spadla plenta na boční stěně. Za ní bylo k vidění několik osob skrytých v maskách za obrazovkami počítačů, na kterých vyhledávali informace o osobách, které byly osloveny na ulici. Směrem k nim byla natočena jedna obrazovka, na které bylo k vidění několik fotek, osobní profil na facebooku a další osobní informace. Všechny osoby byly udiveny tím, co se děje a také tím, co vše jsou schopny o sobě sdílet na sociálních sítích. Po chvíli jim na obrazovce vyskočila hláška „tvůj celý život je online a může to být použito proti tobě.“ Na konci videa společnost zobrazuje hlášku „buďte bdělí.“[35]

8 Etický hacking

Hacker je počítačový specialista mající znalosti o fungování systému či různých programů. Dokáže je velmi schopně využít nebo případně upravit pro svou potřebu.

Slovo „hacking“ v původním smyslu znamenalo vylepšování programů pro počítače, aby došlo k dosažení větší výkonnosti. V dnešní době se tento výraz více používá pro praktiky lidí, kteří se snaží obohatit k vlastnímu prospěchu. Jeho původní pozitivní význam se stal v současnosti negativním.

Etický hacking provádí člověk označovaný jako etický hacker nebo také jako „whitehat“ hacker. Je najímán na testování odolnosti systému dané firmy, instituce, apod.

Dále je skupina hackerů označovaných za „greyhat“ hackery, kteří systémy testují bez vědomí firem, ale po obdržení výsledků testované firmy upozorní na konkrétní nedostatky v systémech a na jejich vylepšení.

Poslední skupinou hackerů jsou „blackhat“ hackeři. Tito hackeři používají své znalosti k vlastnímu obohacení a nijak jim nezáleží na dobrém zabezpečení firmy, ba naopak.

Etický kodex hackera neexistuje. Každý hacker věří něčemu jinému a dle toho i jedná. Obecně lze tvrdit, že se každý hacker dostal do situace, kdy jeho činy byly na pokraji legality, přičemž dle své úvahy jednal morálně.[42]

EC-Council je mezinárodní rada konzultantů elektronického obchodu. Tato rada vytvořila certifikáty a provádí školení v různých oblastech hackingu. Vytváří tak certifikované etické hackery. Jedním z nich je i poslední dobou velmi zmiňovaný Edward Snowden, který pracoval pro CIA a NSA. Nejprve pracoval jako „whitehat“ hacker, později se stal „blackhat“ hackerem. Díky dovednostem, které si osvojil, získal přísně tajné dokumenty o projektu PRISM, na kterém se podílí velké společnosti, jako jsou Microsoft, Yahoo!, Google, Facebook, Youtube, Skype, Apple a další. Společnosti spolupráci nad rámec zákonů popřely.[43]

Přibližme si více spojení etický hacking. Etický hacking je proces, při kterém etický hacker zkoumá počítačové i síťové služby a jejich možné zneužití. Výzkum služeb je prováděn pomocí penetračního testování, to se liší od běžného hledání slabých míst.

Hledání slabých míst obvykle provádíme síťovým skenerem. Známé nástroje pro skenování jsou Heat, Nessus, Retina, atd. Skenery prochází služby a porty na celém bloku IP adres. Většina nástrojů dokáže zjistit typ operačního systému, verze aplikací, nainstalované záplaty, uživatelské účty a data SNMP. Některé nástroje umí i nízkoúrovňové hádání hesel. Výsledkem hledání slabých míst je seznam, který říká, jaké chyby se v síti nachází a co udělat pro jejich odstranění. Hledání slabých míst je vhodné pro odhalení základních bezpečnostních problémů systému. Na skutečné odzkoušení systému a posouzení rizik jeho chyb je většinou potřeba etický hacker.

Penetrační testování je příležitost pro využití hackerových znalostí. Etický hacker může přezkoumat chyby nalezené při hledání slabých míst nebo se může pokusit všemi možnými prostředky proniknout do firemní sítě. Při penetračním testování se etický hacker pokouší postupně dostat pod kontrolu celý systém. Testování končí v momentě, kdy se hackerovi podaří získat root účet nebo účet správce domény. Během pokusů o ovládnutí celého systému sbírá etický hacker správcovská hesla, tajné dokumenty, hesla k účtům nebo sejfu. Tyto materiály pomáhají posoudit riziko, které nalezené chyby představují pro firmu.

V souhrnu by mělo hledání slabých míst najít chyby v systému, následně by mělo penetrační testování ukázat zneužití těchto chyb k proniknutí do systému. Výsledkem by mělo být navržení řešení ke snížení chyb systému a zvýšení jeho zabezpečení.[44]

9 Obrana proti sociálnímu inženýrství

Základním stavebním kamenem obrany je propracovaná bezpečnostní politika, která jasně určuje části organizace se zvýšeným stupněm ochrany dat.[9] Častým jevem dobře propracovaných politik je zanedbání málo patrné, ale přesto zranitelné části systému. Do této části řadíme zaměstnance firmy na nižších pozicích, kteří se setkávají s klienty, dodavateli, apod. Jmenovitě jsou to pozice recepčních, sekretářek, vrátných, apod. Tito zaměstnanci bývají obvykle prvními cíli útoku sociotechnika. Teoretické vzdělávání zaměstnanců, ale také například simulování reálných situací, zachovávání zvýšené opatrnosti, je velmi důležité.[36] Mít vypěstovaný zdravý skepticismus výrazně pomáhá v předcházení sociotechnického útoku. Zaměstnancům je potřeba vysvětlit, která data jsou tajná a co smí a nesmí povědět jiným osobám. Musí zvládnout základní techniky ověřování totožnosti při jakémkoli kontaktu s jinými osobami. Mezi základní postupy pro snížení nebezpečí útoku můžeme řadit:

- metoda dvojitého ověřování
- správná volba hesla, jasně dané politikou firmy; kladen důraz na minimální složitost hesla (počet znaků, malá a velká písmena, číslice); odstranění „defaultního“ hesla
- jasně dané postupy pro žádost o bezpečnostní kód nebo při selhání ověřovacího procesu
- přesně stanovená opatření při zrušení pracovního poměru a během výpovědní lhůty; statistika říká, že největší hrozbou pro firmy jsou bývalí zaměstnanci (velmi dobře se orientují v prostředí firmy), je vhodné informovat i spolupracující firmy; důraz kladen na včasné odevzdání všech klíčů, identifikátorů, apod.
- prověřování IT zaměstnanců (přístup k citlivým firemním datům); některé organizace sledují výchylky v chování svých informatiků, například záliba v hazardu[9]

Nezbytnou součástí obrany proti útokům jsou samozřejmě kvalitní antivirové programy, firewally a spamové filtry, které by neměly chybět na žádném zařízení.

Důležité je udržovat všechny aplikace zabezpečující osobní počítač stále aktualizované, aby byly schopny zachytit i ty nejnovější hrozby.[36]

Mezi nejčastější hrozby v České republice patří phishingový útok vedený emailem. V dnešní době jsou emaily velmi zdařilé a působí věrohodně. Emaily tipu „Ahoj já strýček John z Korea“ jsou dávnou minulostí, i přesto však emaily obsahují chyby. Příkladem může být neutrální oslovení „Ahoj“ nebo třeba chyba v použití i/y při shodě přísudku s podmětem. V emailech, s pro nás neznámým odesílatelem, bychom neměli klikat na žádné podezřelé odkazy, které obvykle obsahují v názvu stránky překlep (například www.seznann.cz) a ani bychom neměli v těchto emailech otevírat žádnou přílohu. Další zásadou, kterou bychom měli ctít, je použití zabezpečeného protokolu „https://“ při práci s citlivými informacemi.[37]

Obr. 4 Ukázka podvodného emailu [37]

Měli bychom pamatovat, že se nás administrátor ani nikdo jiný nebude ptát na heslo k uživatelskému účtu a ani se nás nikdy nebude ptát operátor banky na heslo k internetbankingu, výjimkou může být rodné číslo. V situaci, kdy jsme v časové tísni a je na nás vyvíjen tlak, musíme si pořádně rozmyslet následující krok, i kdyby mělo dojít ke

zdržení vyřízení požadavku. Nebýt líný, zbytečně sdílný a hlavně si nemyslet, že by nám dal někdo něco zadarmo.[38]

Účinnou metodou, jak prozkoušet zaměstnance firmy, je simulovaný přímý útok vybranými mechanismy. Sociotechnický útok je prováděný najatou bezpečnostní firmou. Může jít o etické hackery, kteří vyzkouší v daném časovém období různé mechanismy sociálního inženýrství a vyhodnotí výsledky útoku. V návaznosti na výsledky doporučí firma vylepšení zabezpečení pro následnou eliminaci útoků. Velkým přínosem testování jsou zkušenosti, které získají otestovaní uživatelé. Pokud se zaměstnanci firmy setkají v budoucnu se stejným sociotechnickým útokem, předpokládá se, že útoku zvládnou odolat a zachovají se v souladu s bezpečnostní politikou.

Obrana před sociálním inženýrstvím není snadná, jelikož nejčastěji míří na nejméně spolehlivý a přitom nejsložitější článek celého systému – člověka.[9]

10 Zákony postihující kyberkriminalitu

Úsilí právně regulovat a postihovat trestnou činnost páchanou pomocí informačních a komunikačních technologií je od samého zrodu těchto nežádoucích činností. Kybernetická kriminalita se výrazně liší od ostatních druhů trestné činnosti.[39] Rozdíl tkví v dynamice vývoje a okamžité změně v závislosti na úspěchu či neúspěchu útoku, to s sebou přináší určité problémy ve spojitosti s legislativou.

V trestním právu hmotném můžeme kybernetické činy zařadit pod zákonné ustanovení určité skutkové podstaty, i když tato podstata cílí na obvyklé způsoby spáchání trestného činu. Přesto existuje mnoho trestných činů páchaných v kyberprostoru, u nichž nemůžeme podobné přiřazení využít. V těchto případech je snaha zákonodárců jednotlivých zemí reagovat a vyplnit tak mezery ve vnitrostátní legislativě.

Problém kyberkriminality se řeší na mezinárodní úrovni. Mezi první dokumenty týkající se problematiky kybernetické trestné činnosti patří Manuál OSN o prevenci a kontrole trestných činů spojených s počítači, přijatý v Havaně v roce 1990. V roce 2001 byla na mezinárodní úrovni přijata Úmluva o kyberkriminalitě a dodatkový protokol k ní. Jde o dva nejvýznamnější právní dokumenty usnadňující ochranu společnosti před kybernetickou kriminalitou, jelikož vymezují základní okruh trestných kybernetických činů a zároveň určují možnosti, jak tuto trestnou činnost odhalit a vyšetřit. V ČR byly dokumenty přijaty v roce 2005.

Z důvodu bezmeznosti kyberkriminality a potřeby efektivně mezinárodně spolupracovat, je snahou EU přiblížit legislativu jednotlivých členských států, aby bylo možné účinněji postihovat spáchané trestné činy. Sbližování práva jednotlivých členů EU probíhá prostřednictvím rámcových rozhodnutí, směrnic a dalších dokumentů.

Kybernetickou trestnou činnost v ČR upravují různé právní normy:

- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 127/2005 Sb., o elektronických komunikacích
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 89/2012 Sb., občanský zákoník

- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 160/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

Novela trestního zákoníku platná od 1. ledna 2010 obsahuje mnoho podstatných změn v oblasti trestního práva hmotného. Změny se rovněž týkaly znění skutkových podstat trestných činů. Byly zavedeny nové speciální skutkové podstaty ve spojitosti s kyberkriminalitou.

Kybernetické trestné činy ve vztahu k informačním a komunikačním technologiím dělíme na trestné činy, při kterých využíváme těchto technologií k páchání trestné činnosti a na trestné činy, při kterých jsou cílem právě tyto technologie.

Ke zmíněným trestným činům řadíme:

- § 180 neoprávněné nakládání s osobními údaji
- § 181 poškození cizích práv
- § 182 porušení tajemství dopravovaných zpráv
- § 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí
- § 205 krádež
- § 206 neoprávněné užívání cizí věci
- § 209 podvod
- § 216 legalizace výnosů z trestné činnosti
- § 228 poškození cizí věci
- § 230 neoprávněný přístup k počítačovému systému a nosiči informací

- § 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti
- § 234 neoprávněné opatření, padělání a pozměnění platebního prostředku
- § 316 vyzvědačství
- § 317 ohrožení utajované informace

Mimo uvedené paragrafy se problematice kyberkriminality věnuje i § 120 trestního zákoníku, který zní: *„Uvést někoho v omyl či využít něčího omylu lze i provedením zásahu do počítačových informací nebo dat, zásahu do programového vybavení počítače nebo provedením jiné operace na počítači, zásahu do elektronického nebo jiného technického zařízení, včetně zásahu do předmětů sloužících k ovládání takového zařízení, anebo využitím takové operace či takového zásahu provedeného jiným.“*[39]

11 Praktická část

11.1 Napadení uživatelé v ČR

Mnoho lidí se denně setkává s phishingem, dle statistiky společnosti Kaspersky Lab. bylo v ČR v roce 2016 napadeno 2-7% uživatelů. Nikdo není schopen přesněji určit, zda se jednalo o uživatele proškolené v bezpečnosti práce na internetu nebo uživatele, kteří jsou z oboru IT nebo o uživatele, kteří jsou technicky méně zdatní. Proškolení uživatelé nebo uživatelé z oboru by měli snadněji identifikovat možný útok na jejich osobu, oproti neznalému. Ovšem v dnešní době jsou útoky neustále zdokonalovány a jejich rozpoznání je čím dál složitější.

11.2 Výběr lokality pro útok

Vzhledem k důležitosti problematiky sociálního inženýrství jsem provedl výzkum, kdy jsem využil jednoho z mechanismů v rámci etického hackingu. K vlastnímu útoku jsem si vybral skupinu lidí, kde se předpokládá, že jsou technicky zdatnější a uvědomělejší a dokážou rozpoznat hrozící nebezpečí. Vybraní lidé jsou úzce spjatí s univerzitou, kde studuji. Terčem phishingového útoku se stali studenti předmětu Operační systémy na Univerzitě Hradec Králové (UHK). Jde většinou o studenty prvního ročníku, ale jsou mezi nimi i studenti druhého či třetího ročníku. Celkem bylo emailem osloveno 193 studentů. Pro útok bylo vymezeno krátké časové období, abych zamezil rychlému rozšíření informace o možném podvodném emailu. Období pro studenty informačního managementu (IM) bylo 3 dny a pro studenty aplikované informatiky (AI) 2 dny. Rozdíl v období byl způsoben omezením, které má Google nastaveno u odesílání formulářů. Limit je cca 100 odeslání za 24 hodin.

11.3 Obsah phishingové zprávy

Pro obsah phishingové zprávy jsem si vybral problematiku, kterou jsme se spolužáky řešili každý ročník. Problematika se týkala aktuálnosti kurzů ve vzdělávacím prostředí Blackboard e-Education, jinak známé jako Oliva. Se spolužáky jsme hledali způsob, jak odstranit kurzy, které jsme již absolvovali, ale i přesto je máme v Olivě v „Moje kurzy“ stále zavedené. Myšlenkou podvodné zprávy bylo vydávání se za administrátora UHK, který zjišťuje, zda student kurz používá či nikoli. V případě, kdy by

student uvedl, že kurz nepoužívá, mělo dojít k odstranění kurzu Operační systémy ze studentova plánu výuky (Moje kurzy) v Olivě.

Základem celé zprávy byl text oznamující možnost si aktualizovat kurzy v Olivě a přiložený formulář pro zjištění, o kterého studenta se jedná. Text v emailu zněl:

„Dobrý den,

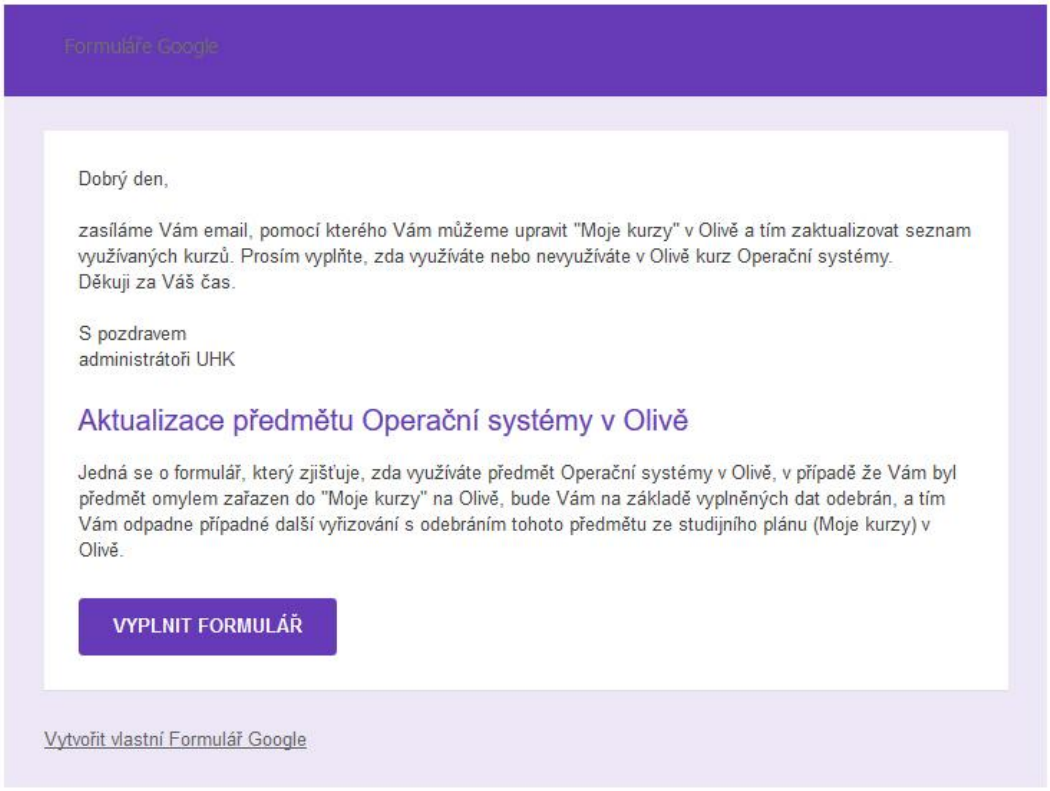
zasíláme Vám email, pomocí kterého Vám můžeme upravit "Moje kurzy" v Olivě a tím zaktualizovat seznam využívaných kurzů. Prosím vyplňte, zda využíváte, nebo nevyužíváte v Olivě kurz Operační systémy.

Děkuji za Váš čas.

S pozdravem

administrátoři UHK“

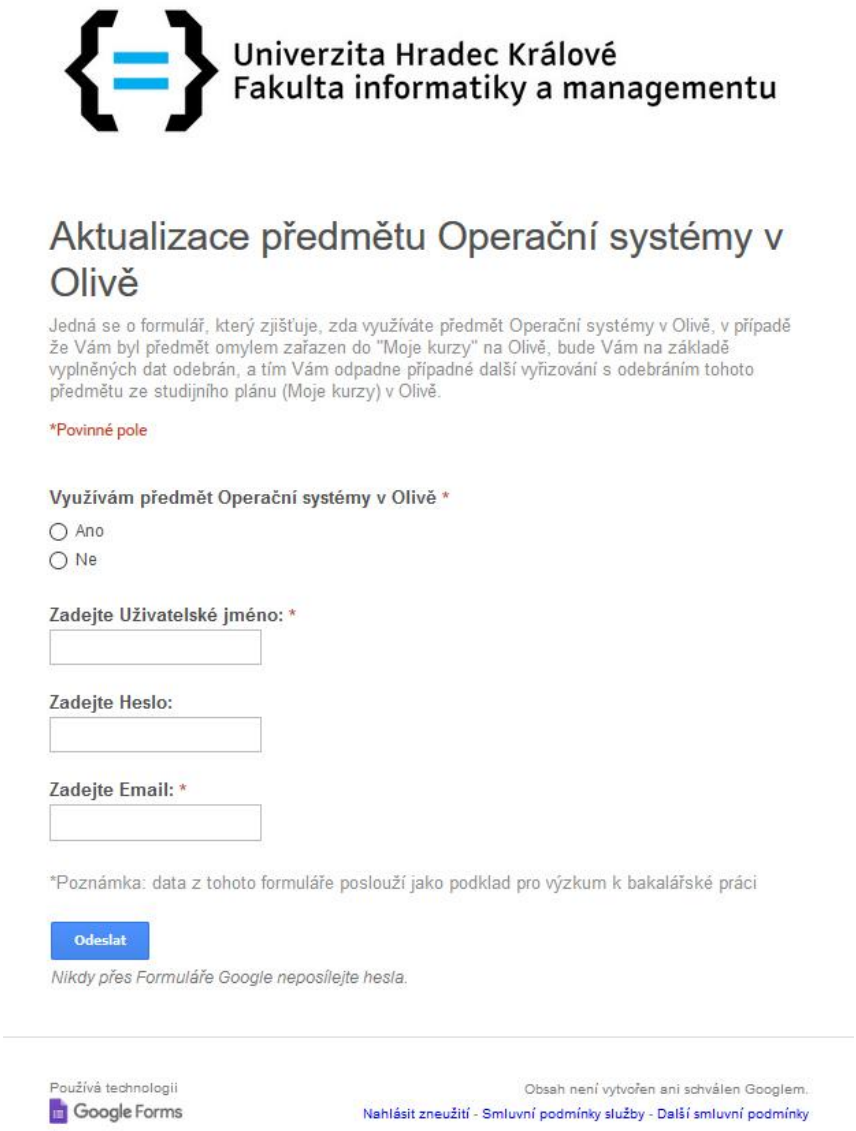
Vzhled emailu jsem několikrát předělával v závislosti na formuláři, který byl vytvořen v prostředí Google Forms. Google nabízí možnost vložení formuláře do obsahu emailu. Tuto možnost jsem nevyužil, jelikož k vloženému formuláři přidává Google další pozadí, které ubírá na důvěryhodnosti celého emailu, avšak hlavním důvodem, proč nebyl formulář vložen do obsahu emailu, byla blokace formulářových prvků na straně poskytovatelů poštovních služeb. Spousta z nás totiž používá více emailových schránek, ale nechává si zprávy z nich přesměrovat do jedné, aby měla vše na jednom místě a nemusela se starat o každou z nich samostatně. Z důvodu této pestrosti poskytovatelů jsem potřeboval zajistit funkčnost vytvořeného formuláře pro výzkum ve všech prostředích. Na základě zjištěného faktu jsem se tedy rozhodl pro email, jehož obsahem bude zmíněná zpráva a odkaz na formulář vytvořený v prostředí Google Forms.



Obr. 5 Obsah phishingového emailu

11.3.1 Vzhled formuláře

Obsahem formuláře vytvořeného v prostředí Google Forms byly jen základní informace. Základem bylo logo fakulty Informatiky a managementu UHK, které jsem získal na stránkách UHK a které dodávalo na důvěryhodnosti. Pod ním bylo vloženo oznámení, proč formulář vznikl a proč ho vyplnit. Následovaly pak formulářové prvky vybízející k vyplnění informací, zda daný předmět studuji, dále uživatelského jména, hesla a emailu. Pod formulářovými prvky bylo dopsáno sdělení (*„*Poznámka: data z tohoto formuláře poslouží jako podklad pro výzkum k bakalářské práci.“*), které informovalo o záměru využití dat získaných vyplněním formuláře. Všechny prvky až na heslo byly zvolené jako povinné, aby mohl být formulář úspěšně odeslán. Samotný Google automaticky dodává nakonec každého formuláře pod tlačítko „Odeslat“ oznámení, kde informuje uživatele, aby nikdy přes Google Form neodesílali svá hesla.

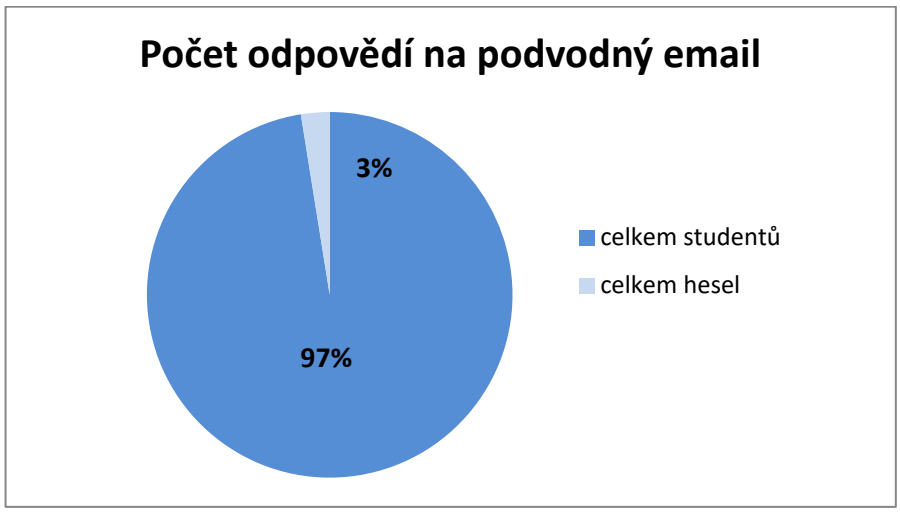


Obr. 6 Odkazovaný formulář v emailu

Podvodný email na první pohled musel uživatel technicky zdatný a uvědomělý rozpoznat, jelikož nevypadal moc důvěryhodně (viz. obr. 5). Důvěryhodnosti zcela jistě ubíral i email, ze kterého byl celý útok veden. Šlo o email založený na službě Google – Gmail.com, což muselo vzbudit podezření, proč by administrátor UHK měl email vedený jinde než v univerzitní doméně www.uhk.cz. Naopak důvěryhodnost zvyšoval přiložený formulář, protože obsahoval logo FIM UHK a málo kdo by předpokládal, že bylo zneužito pro sociotechnický útok.

11.4 Získané odpovědi

Útoku bylo podrobeno zmíněných 193 studentů. Zajímavostí je, že reakce na podvodný email přicházely vždy jen v den odeslání phishingové zprávy. Nikdo ze studentů na email nereagoval druhý ani pozdější den. Jak jsem již psal výše, doba na odpovědi byla omezena na 2 respektive 3 dny. Celkem přišlo 29 odpovědí vyplněných přes formulář. Nikdo však neví, kolik studentů podvodný email četlo, protože víme, že četnost otevření univerzitního emailu není u všech studentů stejná. Někteří studenti kontrolují poštovní schránku denně, někteří jednou za čtrnáct dní, apod. Jedna reakce vyplněná přes formulář, dokazuje, že někteří studenti znají problematiku sociálního inženýrství nebo se jednoduše nenechali nachytat. Další reakce přišla přímo na email, kde se student dotazuje, proč má zadávat i heslo. Celkem tedy zareagovalo 30 lidí.

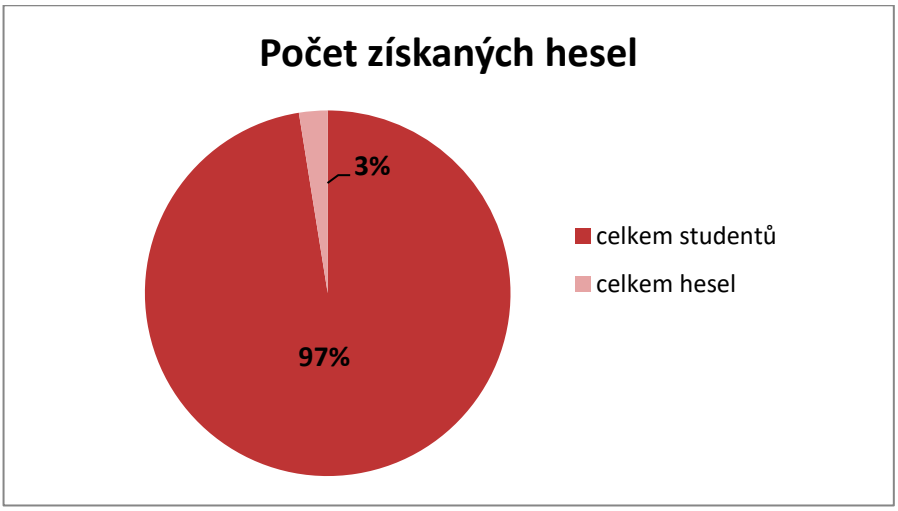


Obr. 7 Počet odpovědí na podvodný email

11.4.1 Obsah odpovědí

Studenti, kteří odpověděli na podvodný email, o sobě nezávazně sdělili i další osobní informace. Sdělili mi soukromou emailovou adresu, přestože byli kontaktování na univerzitní email, počet uvedených soukromých adres byl 5. Jako nepovinnou položku jsem po studentech vyžadoval heslo. Z celkového počtu 29 odpovědí přes formulář jsem získal 5 hesel, což je cca 17% studentů, co mi odpovědělo a zároveň poslalo i heslo. Studenti, kteří mi sdělili heslo, mi ve 2 případech sdělili i soukromý email. Touto kombinací nahráli potencionálnímu útočníkovi, aby vyzkoušel získané

heslo i ke vniknutí do soukromé pošty a tam našel nějaké citlivé informace nebo obsah, se kterým by mohl naložit ke svému obohacení.



Obr. 8 Počet získaných hesel ze všech odeslaných emailů

11.5 Shrnutí sociotechnického útoku

Sociotechnický útok provedený v univerzitním prostředí UHK na studenty předmětu Operační systémy považuji za úspěšný, protože se mi povedlo získat 5 hesel k uživatelským účtům. Po ukončení výzkumu byli studenti na nejbližší přednášce informováni přednášejícím, že se stali terčem sociotechnického útoku provedeného v rámci bakalářské práce a byli vyzváni ke změně hesla ke svému uživatelskému účtu. Údaje získané v rámci tohoto výzkumu mi posloužily výhradně pro zpracování statistiky, nebyly použity pro vnik do cizích uživatelských účtů a ani nijak jinak zneužity. Na základě získaných dat lze říci, že jsou studenti málo obeznámeni s problematikou sociálního inženýrství a v závislosti na tomto zjištění by bylo vhodné studenty více informovat o možných útocích na jejich osobu, a tím vzniklými škodami a problémy.

Útok byl proveden v prostředí, kde se předpokládá, že potencionální oběti hrozbu odhalí a předejdou možným komplikacím. Pokud by se však podobný útok provedl ve společnosti, kde je předpoklad odhalení výrazně nižší, může být objem získaných informací, vycházím-li ze statistiky získaných dat, několikrát vyšší a tím se otevírají možnosti pro potencionálního útočníka, proto by bylo vhodné informovat širokou veřejnost o této problematice, aby se předešlo možným škodám a problémům.

Závěr

Cílem práce bylo seznámit s problematikou sociálního inženýrství. Důležité je, že na danou problematiku nelze nahlížet jen z technického hlediska. Velmi podstatnou součástí sociálního inženýrství je psychologie útočníka, to jak na nás působí a kam cílí. Ne každá oběť reaguje podobně, proto je důležité, jakým směrem se útočník bude ubírat.

Představením metod přístupů jsme získali přehled, jak může útočník působit na oběť při osobním kontaktu. Sociotechnik však nemusí využívat pouze osobní kontakt, může využít kontaktu pomocí technologií. V dnešní době je nejvíce využíváno phishingových útoků, které každým rokem nabírají na kvantitě. Při těchto útocích je velmi pravděpodobné, že se chytí mnoho lidí, jelikož útočné zprávy či webové stránky působí velmi věrohodně a málokdo z obětí si v daný moment uvědomí, že se stal obětí nějakého útoku. Na to přichází oběti až po zpětné vazbě, kdy se dozvídají o následcích svého jednání.

Účinnou metodou obrany vůči těmto útokům je pravidelné školení zaměstnanců, kvalitní bezpečnostní software, občasné testování pomocí etického hackingu a firemní politika, která musí být striktně dodržována.

Ve svém výzkumu pro zpracování bakalářské práce jsem zkusil napadnout skupinu studentů na univerzitě. Z počátku jsem se pokoušel vymyslet nejvěrohodnější způsob oslovení studentů. Pravděpodobnost úspěchu by tak téměř jistě byla velmi vysoká, proto jsem se rozhodl udělat phishingový útok méně věrohodný, abych zjistil, zda na něj i přesto budou studenti reagovat. Výsledky jejich reakcí lze najít na konci kapitoly „Praktická část“. Svůj výzkum v závislosti na výsledcích považuji za úspěšný.

Možné budoucí rozšíření práce vidím v aplikaci etického hackingu, pomocí jehož výsledků lze následně navrhnout přímé řešení pro lokalitu, kde by byl útok veden. Jiným možným rozšířením může být pokus o zisk osobních informací z nějaké sociální sítě a následně pokus o slovníkové prolomení hesla na základně získaných dat.

Seznam použitých zdrojů

[1] PŘIBYL, Tomáš. Sociální inženýrství z pohledu útočníka. B2B magazín o bezpečnosti ICT ze všech úhlů - ICT Security [online]. 2009 [cit. 2017-03-06]. Dostupné z: http://www.ictsecurity.cz/component/content/article?id=2756

[2] BEDNÁŘ, Vojtěch. Principy a postupy sociálního inženýrství. B2B magazín o bezpečnosti ICT ze všech úhlů - ICT Security [online]. 2009 [cit. 2017-03-06]. Dostupné z: http://www.ictsecurity.cz/component/content/article?id=2765

[3] PŘIBYL, Tomáš. Ukradli mě!. Computerworld.cz | Deník pro IT profesionály [online]. 2005 [cit. 2017-03-07]. Dostupné z: http://computerworld.cz/securityworld/ukradli-me-46392

[4] ŠIMEK, Richard. Sociotechnika (sociální inženýrství) [online]. Brno, 2003 [cit. 2017-03-08]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm. Kolokviální práce. Masarykova univerzita.

[5] CMUNT, Jarda. Počítačová bezpečnost a Linux I - zjišťování informací o serveru. Linuxové noviny [online]. 1999 [cit. 2017-03-08]. Dostupné z: http://www.linux.cz/noviny/1999-11/clanek03.html

[6] ERBEN, Lukáš. Příchod hackerů: Kevin Mitnick, Stanley Mark Rifkin a sociální inženýrství. Root.cz - informace nejen ze světa Linuxu [online]. 2014 [cit. 2017-04-10]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-kevin-mitnick-stanley-mark-rifkin-a-socialni-inzenyrstvi/

[7] MITNICK, Kevin. Umění klamu. 2. vydání. Gliwice, Polsko: HELION S.A., 2003. ISBN 83-7361-210-6.

[8] CIALDINI, Robert B. Zbraně vlivu: Manipulativní techniky a jak se jim bránit. V Brně: Jan Melvil Publishing, 2012. Žádná velká věda. ISBN 978-80-87270-32-5.

[9] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[10] HORNÍČEK, Jan. Sociální inženýrství [online]. Zlín, 2009 [cit. 2017-02-24]. Dostupné z: http://digilib.k.utb.cz/bitstream/handle/10563/9113/horn%C3%AD%C4%8Dek_2009_bp.pdf?sequence=1. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně.

[11] BUDAI, David. Sociální inženýrství v praxi: Když si hacker o heslo prostě řekne. Cnews.cz | Od tranzistorů až po PC sestavy [online]. 2012 [cit. 2017-03-24]. Dostupné z: https://www.cnews.cz/socialni-inzenyrstvi-v-praxi-kdyz-si-hacker-o-heslo-proste-rekne/

[12] SLINTÁK, Jiří. Nebezpečí sociálního inženýrství a jak se mu účinně bránit. Svět sítí - informace ze světa počítačových sítí [online]. 2009 [cit. 2017-03-26]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Nebezpeci-socialniho-inzenyrstvi-a-jak-se-mu-ucinne-branit-26102009

[13] WORSHAM, Jack L. From phone phreaking to cyber war: Cyber crime´s impact on business. Jack Worsham´s professional portfolio [online]. neuvedeno [cit. 2017-04-11]. Dostupné z: http://it-professional.vpweb.com/upload/From%20Phone%20Phreaking%20to%20Cyber%20War%20Cyber%20Crime%E2%80%99s%20Impact%20on%20Business.pdf

[14] LAPSLEY, Phil. Exploding the phone: The untold story of the teenagers and outlaws who hacked ma bell. Neuvedeno. New York: Grove Press, 2013. ISBN 978-0-8021-9375-9.

[15] LAPSLEY, Phil. The history of phone phreaking. The history of phone phreaking [online]. 2005 [cit. 2017-04-12]. Dostupné z: http://www.historyofphonephreaking.org/faq.php

[16] KALVODA, Bc. Ondřej. Sociální inženýrství: v kontextu kybernetické bezpečnosti [online]. Brno, 2014 [cit. 2017-04-12]. Dostupné z: https://is.muni.cz/th/333077/fss_m/Diplomova_prace_ngwzunsd.pdf. Magisterská práce. Masarykova univerzita.

[17] Slovníček pojmů - root.cz. Root.cz - informace nejen ze světa Linuxu [online]. [cit. 2017-04-13]. Dostupné z: https://www.root.cz/slovnicek/phishing/

[18] Phishing a pharming. Bezpečný internet | Rady pro bezpečnost na internetu [online]. [cit. 2017-04-13]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

[19] MCCARTHY, Linda a Denise WELDON-SIVIY, ed. Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online. Neuvedeno. Praha: CZ.NIC, 2013. ISBN 978-80-904248-6-9.

[20] JAMES, Lance. Phishing bez záhad. Praha: Grada, 2007. ISBN 978-80-247-1766-1.

[21] Phishing. Bezpečný internet | Rady pro bezpečnost na internetu [online]. [cit. 2017-04-13]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/e-mail/phishing.aspx

[22] ERBEN, Lukáš. Příchod hackerů: nigerijský scam „419“. Root.cz - informace nejen ze světa Linuxu [online]. 2014 [cit. 2017-04-14]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-nigerijsky-scam-419

[23] SCAM419. HOAX [online]. [cit. 2017-04-14]. Dostupné z: http://www.hoax.cz/scam419/

[24] Vishing. Správa sítě - slovník pojmů: správa sítě, zabezpečení sítě, outsourcing IT [online]. [cit. 2017-04-15]. Dostupné z: http://www.sprava-site.eu/vishing/

[25] JASNÝ, Libor. Malware a sociální inženýrství [online]. Zlín, 2009 [cit. 2017-04-15]. Dostupné z: http://digilib.k.utb.cz/bitstream/handle/10563/9852/jasn%C3%BD_2009_bp.pdf?sequence=1. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně.

[26] Hacknout mozek je snazší než hacknout počítač. VTM.cz - věda, technika, zajímavosti, budoucnost [online]. [cit. 2017-04-15]. Dostupné z: http://vtm.e15.cz/clanek/hacknout-mozek-je-snazsi-nez-hacknout-pocitac

[27] Čo je vishing? Slovenská sporiteľňa [online]. [cit. 2017-04-15]. Dostupné z: https://www.slsp.sk/sk/otazky-a-odpovede/co-je-vishing

[28] BEDNÁŘ, Vojtěch. Pharming je zpět a silnější. Lupa.cz - server o českém Internetu [online]. 2007 [cit. 2017-04-16]. Dostupné z: http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/?version=1&utm_expid=.1rnVC9uKTLGPIiC_juvx9A.1

[29] WATSON, Gavin. Social engineering penetration testing: executing social engineering pen tests, assessments and defense. Waltham: Elsevier, 2014. ISBN 978-0-12-420124-8.

[30] CROSS, Michael. Social media security: leveraging social networking while mitigating risk. Waltham: Elsevier, 2014. ISBN 978-1-59749-986-6.

[31] KUNEŠ, Jakub. Co je sociální inženýrství? - 2. díl. PC World.cz | Recenze, novinky a testy: Hardware, Software, Download a Internet [online]. 2012 [cit. 2017-04-17]. Dostupné z: http://pcworld.cz/internet/co-je-socialni-inzenyrstvi-2-dil-44372

[32] DOBOSIOVÁ, Martina. Co to jsou sociální sítě. Středisko mediální výchovy - Teologické fakulty Jihočeské univerzity [online]. 2015 [cit. 2017-03-04]. Dostupné z: https://www.stremev.cz/co-to-jsou-socialni-site/

[33] KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

[34] BORNOVÁ, Lucie. Úvod do sociálních sítí. IBM developerWorks : IBM´s resource for developer and IT professionals [online]. 2011 [cit. 2017-03-05]. Dostupné z: https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/W2ee553718f13_4825_b4e6_343b81350b95/page/%C3%9Avod%20do%20soci%C3%A1ln%C3%ADch%20s%C3%ADt%C3%AD

[35] Amazing mind reader reveals his 'gift'. YouTube [online]. 2012 [cit. 2017-03-05]. Dostupné z: https://www.youtube.com/watch?v=F7pYHN9iC9I

[36] GAJDOŠOVÁ, Markéta. Sociální inženýrství – e-mail jako kybernetická hrozba. Interval.cz | Svět Internetu, Technologií a Bezpečnosti [online]. 2016 [cit. 2017-04-03]. Dostupné z: https://www.interval.cz/clanky/socialni-inzenyrstvi/

[37] Základní rady pro uživatele. CSIRT.CZ [online]. 2015 [cit. 2017-04-03]. Dostupné z: https://www.csirt.cz/page/2789/zakladni-rady-pro-uzivatele/

[38] Sociální inženýrství. Národní centrum kybernetické bezpečnosti [online]. [cit. 2017-04-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/

[39] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[40] GÁLIK, Stanislav. *Psychologie přesvědčování*. Praha: Grada, 2012. Psyché (Grada). ISBN 978-80-247-4247-2.

[41] Nebezpečné komunikační praktiky a sociální inženýrství. *E-Bezpečí - bezpečněji na internetu pro všechny* [online]. 2008 [cit. 2017-02-24]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sociotechnika/18-20

[42] DOLEŽELOVÁ, Veronika. Hackeři jsou často etičtější než ostatní, říká whitehat hacker Pavol Lupták. *Tyinternety.cz - Startupy, sociální sítě, ty internety!* [online]. 2016 [cit. 2017-02-26]. Dostupné z: http://tyinternety.cz/technologie/hackeri-jsou-casto-eticteji-nez-vetsina-populace-tak-pravil-jeden-z-nich/

[43] JENÍKOVÁ, Markéta. Edward Snowden má výcvik „etického hackera". *Objevit.cz: IT magazín, zprávy a novinky ze světa IT* [online]. 2013 [cit. 2017-02-26]. Dostupné z: http://objevit.cz/edward-snowden-ma-vycvik-etickeho-hackera-t30186

[44] HARRIS, Shon. *Hacking: manuál hackera*. Praha: Grada, 2008. ISBN 978-80-247-1346-5.

[45] GUDKOVA, Darya, Maria VERGELIS, Nadezhda DEMIDOVA a Tatyana SHCHERBAKOVA. Spam and phishing in 2016. Securelist - Information about Viruses, Hackers and Spam [online]. 2017 [cit. 2017-04-13]. Dostupné z: https://securelist.com/analysis/kaspersky-security-bulletin/77483/kaspersky-security-bulletin-spam-and-phishing-in-2016/

Seznam obrázků

Zadání k závěrečné práci

Jméno a příjmení studenta: **Daniel Petera**

Obor studia: Aplikovaná informatika

Jméno a příjmení vedoucího práce: **Mgr. Josef Horálek, Ph.D.**

Název práce:

Využití metod sociálního inženýrství pro etický hacking

Název práce v AJ:

The use of methods of social engineering for ethical hacking

Podtitul práce:

Podtitul práce v AJ:

Cíl práce: Cílem práce je představit metody sociálního inženýrství a jejich využití pro etický hacking. Autor provede analýzu přístupů a metod využívaných pro sociální inženýrství, jež vysvětlí a na vhodných ukázkových příkladech předvede. Autor provede podrobnou rešerši o využívání metod sociálního inženýrství pro etický hacking a zvýšení bezpečnosti informačních systémů a komunikačních sítí. V praktické části autor provede testování vybraných metod a jejich praktické využití pro hacking.

Osnova práce:

1. Sociální inženýrství
2. Kevin Mitnick
3. Psychologie sociotechnika
4. Budování důvěry
5. Metody útoků sociotechnika
6. Mechanismy sociotechnického útoku
7. Sociální sítě jako zdroj dat
8. Etický hacking

9. Obrana proti sociálnímu inženýrství
10. Zákony postihující kyberkriminalitu
11. Praktická část

Podpis studenta: **Datum:**

Podpis vedoucího práce: **Datum:**