VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, O.P.S., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

Počítačová kriminalita se zaměřením na hacking

Autor práce: Jakub Kažimír
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Prezenční
Vedoucí práce: Mgr. Vladimír Čížek, DiS.
Katedra: Katedra právních oborů a bezpečnostních studií

2014

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s §47b zákona č. 111/1998 Sb. v platném znění.

……..

Děkuji vedoucímu bakalářské práce Mgr. Vladimíru Čížkovi, DiS. Za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

KAŽIMÍR, J. *Počítačová kriminalita se zaměřením na hacking : bakalářská práce.* České budějovice : Vysoká škola evropských a regionálních studií, o.p.s., 2014. Vedoucí bakalářské práce : Mgr. Vladimír Čížek, DiS.

Klíčová slova: hacking, hacker, cracking, cracker, pentest

Bakalářská práce „Počítačová kriminalita se zaměřením na hacking“ se zabývá poměrně novou oblastí hospodářské kriminality, a to kriminalitou páchanou za pomoci informačních zařízení, kde cílem pachatelů je získat přístup do počítačového systému nebo počítačového programu jinou než legální cestou a následně tento systém nebo program pozměnit, popřípadě zneužít k jinému účelu, než pro který byl určen. Obsahem práce je analýza odborné literatury z oblasti informatiky, analýza zákonů, zahrnující regulaci trestných činů, spáchaných proti informačním zařízení a jejich obsahu. Dále jsou uvedeny možnosti zabezpečení a následně detailně rozebráno penetrační testování systémů, jako jedna z účinných a využívaných preventivních metod.

V praktické části je kvantitativním dotazníkovým šetřením zjišťován postoj respondentů na hacking a jakým způsobem chrání své informace nebo zařízení před možným zneužitím, poškozením či ztrátou.

ABSTRACT

KAŽIMÍR, J. *Cybercrime focusing on hacking : Bachelor thesis.* České Budějovice : The College of European and Regional Studies, 2014. Supervisor : Mgr. Vladimír Čížek, DiS.

Key words: hacking, hacker, cracking, cracker, pen test

Bachelor thesis „Cybercrime focusing on hacking“ conversants relatively new sector of economic crime, respectively commission of crimes with the help of information technologies, where the goal is to get offenders access to a computer systems or computer programs other than legal mean, then this system or program; or exploit for any purpose other than that for which it was designed. Work includes the analysis of scientific literature in the field of computer science, analysis of the law, including the regulation of crimes committed against information systems and their content. The following are the security options, and then discussed in detail penetration testing of systems, as one of the effective and preventive methods used.

In the practical part is quantitative questionnaire survey investigated respondents' attitude to hacking and how to protect their information and equipment from possible damage, abouse or loss.

OBSAH

ÚVOD

Globální informatizace symbolizuje 21. století, neboť zavádí informační prostředky téměř do každé složky lidské činnosti. Je to dáno především snadnou dostupností výpočetní techniky, vcelku za malý obnos finančních prostředků, a potřebou po informacích. Cenná informace představuje hybnou sílu zejména pro politiku, podnikatele, vědce i normální občany.

Máme-li si vytyčit pozitiva informatizace, bude mezi ně bezpodmínečně patřit rychlost, jakou se informace přenáší, dostupnost informací a informačních zařízení, a cena při pořizování zařízení, dále co přináší je mezinárodní propojení. Ovšem s pozitivy, musí přijít i negativa, a ty se vážou na prostor, ve kterém se nachází informační zařízení zejména budovy, byty, chlazené prostory pro superpočítače a další, rovněž prostor, kde dochází k přenosům informací mezi zařízeními, často je tento prostor nazýván kyberprostor. V kyberprostoru, stejně tak jako v reálnem světě, se naskýtá příležitost ke kriminální činnosti.

Hlavně v duchu kyberprostoru se nese i obsah bakalářské práce, a to konkrétně na hacking, protože znalost slabin v sítích a programů, umožní možnému pachateli zmocnit se cenných informací s poměrně dostupnými prostředky. V první kapitole jsou stanoveny cíle a metodika způsobilá k postupu v bakalářské práci. Druhá kapitola podává přehled o vybraných termínech pro naše potřeby, jejichž znalost usnadní pochopení problematiky. Kapitola třetí podává přehled o legislativních úpravách narušování sítí a informačních zařízeních a regulaci bezpečnostních rizik, která úzce souvisí s narušováním. Od narušování přejdeme ke straně defenzivní, kde budou zjištěny způsoby a nástroje vhodné k obraně proti narušitelům. Poslední teoretická část charakterizuje penetrační testování. Jedná se o způsob, jak předcházet cílenému útoku. Zjednodušeně jde o simulovaný útok hackera, kdy správci napadeného zařízení testují výdrž útoků, než dojde ke kolapsu testovaného zařízení. Ve vlastním výzkumu budou zkoumány dotazníkovým šetřením základní aspekty obrany běžných uživatelů, před nežádoucími hackery, spolu s povědomím o hackingu.

1 CÍLE A METODIKA BAKALÁŘSKÉ PRÁCE

Bakalářská práce „Počítačová kriminalita se zaměření na hacking“ se zabývá vším, co souvisí s úmyslným narušováním informačních systémů. Protože informační zařízení v současnosti jsou všudypřítomná, uchovávají mnohdy důležité informace a úmyslným narušením chodu zařízení mnohdy pachatel způsobí nevyčíslitelnou škodu. Toto téma je aktuálním problémem, protože počítačová kriminalita se řadí dnes mezi nejčastěji páchanou hospodářskou kriminalitu.

Hlavním cílem je tuto činnost objasnit a zjistit, jak může být hacking pro společnost nebezpečný, a podle zjištěných informací vydat doporučení, jakými způsoby se lze bránit nebo jak nežádoucímu incidentu předcházet.

Teoretická část je dělena do čtyř kapitol. V kapitole první teoretické části, budou za pomoci analýzy odborných publikací vysvětleny a porovnány klíčové pojmy, co svým způsobem souvisí s problematikou nebo se kterými jsou často neodborníky zaměňovány. Ve druhé kapitole bude analyzována legislativní regulace na území České republiky a mezinárodní smlouvy, kterými je Česká republika vázána. Třetí kapitola má za cíl charakterizovat a porovnat dostupné nástroje zabezpečení informačních systémů. Poslední teoretická kapitola podrobně popisuje penetrační testování, jako jeden z účinných způsobů prevence před možnými útoky hackerů. Zde se bude zjišťovat, jaké metody a postupy penetračních testů jsou obvykle používány a rovněž budou vytyčena pozitiva a negativa jednotlivých typů testů.

Vlastní výzkum má za cíl kvantitativním dotazníkovým šetřením zjistit povědomí o hackingu a zhodnotit postoj dotázaných uživatelů počítače k zabezpečení informačních zařízení. Kontaktováni k vyplnění dotazníku budou především lidé, kteří znají počítač a zvládají alespoň základní orientaci v oblasti ICT.

Stanovení hypotézy

Hypotéza 1: Alespoň 60% má ponětí co je hacking.

Hypotéza 2: Více než polovina respondentů nechrání své počítače antivirovým programem.

2 VYBRANÉ POJMY

Kapitola obsahuje výčet pojmů, které s hackingem úzce souvisí, a které bývají mezi sebou často zaměňovány nebo nesprávně interpretován například v médiích nebo neodborníky. Uvedené pojmy pomohou ke správné orientaci v řešené problematice a k jejímu pochopení.

Pojmy definované na základě Úmluvy o počítačové kriminalitě:

Počítačový systém – znamená jakékoli zařízení nebo skupinu propojených nebo přidružených zařízení, z nichž jedno nebo více provádí automatické zpracování dat podle programu (např. počítač, smartphone, tablet).[1]

Počítačová data – znamenají jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.[2]

Poskytovatel služby – je jakýkoli veřejný nebo soukromý subjekt, který uživatelům své služby umožňuje komunikovat prostřednictvím počítačového systému, a jakýkoli jiný subjekt, který zpracovává nebo uchovává počítačová data pro takovou komunikační službu nebo pro uživatele takové služby.[3]

Provozní data – jsou to jakákoli počítačová data vztahující se ke komunikaci prostřednictvím počítačového systému, vytvořená počítačovým systémem, jakožto součásti komunikačního řetězce, uvádějící původ, cíl, cestu, čas, datum, objem nebo trvání komunikace nebo typ příslušné služby.

[1] ČESKO. Úmluva o počítačové kriminalitě. In *Sbírka mezinárodních smluv, Česká republika.* 2013, částka 56, s. 10790

[2] ČESKO. Vládní návrh, kterým se předkládá Parlamentu České republiky k vyslovení souhlasu s ratifikací Úmluva o počítačové kriminalitě. In *Senátní tisk č.28* [online]. Senát, © 2014 [cit. 2014-4-16]. Dostupné z WWW:< http://www.senat.cz/xqw/xervlet/pssenat/historie?action=detail&value=3266>.

[3] ČESKO. Úmluva o počítačové kriminalitě. In *Sbírka mezinárodních smluv, Česká republika.* 2013, částka 56, s. 10790

Počítačová kriminalita – EU pojem definuje jako nemorální a neoprávněné jednání, které zahrnuje zneužití údajů získaných prostřednictvím informačních a komunikačních technologií nebo jejich změnu.[4]

SMEJKAL[5] počítačovou kriminalitu chápe jako páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení včetně dat, případně některá z komponent počítače nebo většího množství počítačů samostatných, či propojených do počítačové sítě, a to buď jako předmět trestné činnosti nebo jako nástroj trestné činnosti.

Hacking – ERICKSON[6] definuje, že podstatou hackingu je nalézat nezamýšlená nebo rovnou přehlížená využití zákonitostí a vlastností dané situace, která jsou poté aplikována novými a vynalézavými způsoby pro vyřešení nějakého problému – ať už je jím míněno cokoliv.

Počítačový program – je souborem příkazů nebo instrukcí určených k přímému nebo nepřímému použití počítačem za účelem dosažení určitého výsledku.[7]

Exploit – může to být program, operace nebo např. nějaká speciálně zadaná URL, která způsobí neobvyklé chování systému. Ve většině případů jde o tzv. Buffer Overflow, to znamená „Přetečení zásobníku“, který většinou používají hackeři k získání administrátorských práv.[8]

[4] JIROVSKÝ, V., HNÍK, V., KRULÍK, O. Základní definice, vztahující se k tématu kybernetických hrozeb. In Ministerstvo vnitra České republiky. *Informační kriminalita* [online]. Praha : MVČR, 2008 [cit. 2013-12-20]. Dostupné z WWW: <http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/zakladni_info.pdf>.

[5] SMEJKAL, V. Internet a §§§. Praha : Grada Publishing, 2001, s. 151-152.

[6] ERICKSON, J. Hacking - umění exploitace. Brno : Zoner Press, 2008. s. 13.

[7] UNITED STATES. Copyright act of 1976. Copyright Law of the United States [online]. [cit. 2014-1-11]. Dostupný z WWW:< http://www.copyright.gov/title17/circ92.pdf>.

[8] *Pakoš* [online]. [cit. 2013-12-20]. Dostupný z WWW< http://pakos.cz/co-je-to-hacking>.

2.1 Pojem hacker a cracker

V podkapitole je detailně rozebrán pojem hacker a následně porovnán s pojmem cracker, jelikož dochází k častým záměnám mezi zmíněnými subjekty.

Hacker – je označován subjekt využívající své znalosti v oblasti výpočetní techniky k vyhledávání a objevování bezpečnostních nedostatků. Může se jednat o osobu orientující se v detailech programových kódů a jejich zlepšování. Osoba programující s posedlostí se dá také označit za hackera.[9]

White hat hacker

V internetovém slangu „etický hacker“. „Etičtí“ hackeři napomáhají odhalit slabiny programů, systémů či počítačů a na chyby správce upozornit. Správci jsou najímáni a pracují za úplatu. Jejich výhoda je, že mají s hackingem zkušenosti a v hackerské komunitě se pohybují.[10]

Black hat hacker

Do skupiny „černých klobouků“ patří uzavřená společnost hackerů (zejména drobné skupiny), jejichž cílem je nalezení bezpečnostních slabin a jejich využití pro „svou potřebu“. Řadu bezpečnostních slabin odhalí dříve než white hat hackeři, téměř nikdy je nezveřejňují. Právě mezi černými klobouk je možné sledovat spatřovat počítačový underground s opravdovými e-zločinci.[11]

[9] *Počítačová bezpečnost a ochrana dat* [Online]. [cit. 2014-1-10]. Dostupný z WWW:<http://marlib.cmsps.cz/bezpecnost/bezpecnost.html/>.

[10] Hacker. In *Wikipedia: the free encyclopedia* [online]. St. Petersburg (Florida): Wikipedia Foundation, 11.12.2006, poslední aktualizace 30.5.2014 [cit. 2014-5-30]. Dostupné <http://cs.wikipedia.org/wiki/Hacker>.

[11] MIKO, K. Nebezpečí zvané hacking. *Business World*

Gray hat hacker

Hackeři titulování „šedým kloboukem“ se pohybují na pomezí obou skupin. Tato skupina byla zřejmě vytvořena proto, že předcházející skupiny spolu na mnoha místech interferují a rozdíl je jenom v přístupu k problému. Zároveň slouží jako doplňující prvek v taxonomii a obvykle je přechodovým stadiem rodícího se hackera, který nemá ujasněn svůj budoucí úkol.[12]

2.1.1. Hnutí Anonymous

Anonymous je hnutí hackerů, kteří především prostřednictvím DDoS útoků, vedené často skrze software Low Orbit Ion Cannon, zahlcují a odstavují vybrané webové stránky. Hnutí přispělo k protestům za volné šíření informací. Například v roce 2009 se Anonymous společně s íránskými hackery aktivně podílely na demonstracích v době tamějších prezidentských voleb.[13]

Anonymous v ČR

Anonymou v ČR působí od roku 2011 a častým cílem útoku se staly webové stránky protipirátské unie, české vlády nebo databáze ODS, ze které získali hackeři citlivé údaje o jejich členech citlivé údaje o jejích členech (adresy, telefonní čísla, emaily). Jedním z posledních cílů Anonymous v ČR byl útok na stránky OSA, kdy tímto chtěli vyjádřit svůj nesouhlas s cenzurou internetu (stahováním hudby).[14]

[12] JIROVSKÝ, V. *Kybernetická kriminalita: nejet o hackingu, crackingu, virech a trojských koních bez tajemství*. : Grada, 2007, s. 55.

[13] Anonymous (Skupina). In *Wikipedia: the free encyclopedia* [online]. St. Petersburg (Florida): Wikipedia Foundation, 11.12.2006, poslední aktualizace 19.4.2014 [cit. 2014-4-22]. Dostupné WWW: < http://cs.wikipedia.org/wiki/Anonymous_(skupina)>.

[14] *Slideshare* [online]. [cit. 2014-3-26]. Dostupné z WWW: < http://pt.slideshare.net/antropologiemedii/anonymous-antropologie-mdi>.

2.2 Cracker

Cracker – je to osoba, která se snaží vniknout do systému bez autorizace. Tito jedinci tak velmi často činí opačně než hackeři, tedy ze zlomyslnosti, a znají mnoho způsobů, jak se do systému dostat.[15]

Nebo za crackera lze považovat nabourávače do systémů, za hranicí zákona, zloděje a škodiče dat.[16]

Podle definic pojmů hacker a cracker, můžeme sledovat určitou odchylku v pojmech. Při porovnání primárních cílů těchto subjektů zjistíme, že hackerův záměr je spíše pomoci nebo nalézt neobvyklý přístup k systému. Kdežto crackerovým hlavním cílem je způsobit škody nebo se obohatit.

[15] USER GLOSARRY WORKING GROUP. *Internet Users´Glossary.* Texas : Xylogics, 1993. s. 12. Dostupné také z WWW< http://tools.ietf.org/html/rfc1392>.

[16] INSTITU PRO KRIMINOLOGII A SOCIÁLNÍ PREVENCI, *Počítačová kriminalita.* Praha : Institut pro kriminologii a sociální prevenci, 2000. s. 283.

3 PRÁVNÍ ÚPRAVA TÝKAJÍCÍ SE HACKINGU

V této kapitole jsou uvedeny právní předpisy, které svým obsahem nebo míněním upravují problematiku počítačové kriminality a počítačové bezpečnosti. Právní předpisy přímo neupravují trestné činy spojené s hackingem, ale jen některé skutky, s nimiž tato činnost souvisí. Trestné činy spojené s kybernalitou reguluje na území České republiky trestní zákoník č. 40/2009, který rozšířil seznam skutkových podstat ze starého trestního zákoníku č. 140 z roku 1961 o skutkové podstaty v ratifikované Úmluvě o počítačové kriminalitě. Pro srovnání jsou zde uvedeny i zákony podle amerického federálního práva.

3.1 Právní úprava v České republice

Trestní zákon 140/1961 Sb., trestní zákon

Zákon č. 140/1961 Sb., trestní zákon. Tento zákon upravuje trestné činy, spáchané výhradně za pomoci informačních zařízení nebo proti nim, pouze v §257a Poškození a zneužití záznamu na nosiči informací.[17]

Je zjevné, že objektem tohoto trestného činu je ochrana počítačových dat uložených na nosiči informací proti neoprávněným změnám, zničení nebo neoprávněnému použití a ochrana počítače (počítačového systému) před neoprávněnými zásahy. Jinými slovy je chráněn hardware i software. Postihována je nejen změna software, ale i to, čemu by se dalo říci odcizení dat, tedy slovy zákona neoprávněné užití informací uložených na nosiči. Pro naplnění skutkové podstaty je potřebné získat přístup k nosiči informací, což může být přístup oprávněný nebo neoprávněný. Z hlediska naplnění skutkové podstaty to nemá žádný význam. Musí zde být další úmyslné jednání, a to v podobě užití informací, zničení informací nebo zásah do technického či programového vybavení. Toto ustanovení nechání před nedbalým jednáním. Zničení představuje takový zásah do nosiče informací, jímž zcela zaniká

[17] ČESKO. Zákon č. 140 ze dne 29. listopadu 1961 trestní zákon. In *Sbírka zákonů České republiky*. 2002, částka 146, s. 8093. Dostupné také z WWW:< http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=2002&typeLaw=zakon&What=Rok&stranka=6>.

hodnota jeho informačního obsahu, přičemž nejde o zničení informace jako takové, neboť ta může existovat nadále např. jako záložní kopie programu, souboru atd., ale o odstranění záznamu dat z příslušného nosiče. Z hlediska subjektivní stránky se vyžaduje úmyslné zavinění, přičemž úmysl musí být provázen zištnou pohnutkou nebo snahou způsobit újmu. Pachatel může úmysl pojmout až dodatečně v době, kdy už fakticky přistup k nosiči informací má. [18]

Trestní zákoník č. 40/2009 Sb.

Nový trestní zákoník vychází pojmoslovím z Úmluvy o počítačové kriminalitě. Česká republika tuto Úmluvu podepsala už v roce 2005, avšak ratifikována byla až v roce 2013 s výhradami proti konkrétním článkům.[19]

Oproti starému trestnímu zákoníku jsou v tomto novém lépe popsány a postihovány protiprávní skutky, jenž jsou spojeny s počítačovou kriminalitou.

§ 230 vymezuje skutky, které se vážou s neoprávněným přístupem k počítačovému systému a nosiči informací. Pachatel je postihován již za samotný neoprávněný přístup k počítačovému systému nebo jeho části, a to za předpokladu, že předtím překonal bezpečnostní opatření. Tento čin bývá též označován anglickým termínem hacking, přičemž osoba, která se ho dopustí, se označuje jako hacker. Základní skutková podstata uvedená v § 230 odst. 1 nevyžaduje úmysl způsobit škodu, jinou újmu, získat prospěch, ani vznik takového účinku. Způsobení některého z těchto účinků tvoří přitěžující okolnosti podle odstavců 3 a 4.[20]

Kybernetický zákon

Zákon je „postaven“ na dvou zásadách a třech pilířích. První zásadou je minimalizace zásahu do práv soukromoprávních subjektů, druhou zásadou je individuální odpovědnost za bezpečnost vlastních informačních systémů. Tři pilíře tvoří: 1. bezpečnostní opatření (standardizace), 2. hlášení kybernetických

[18] *Právní rádce* [online]. [cit. 2014-2-1]. Dostupný z WWW:< http://pravniradce.ihned.cz/c1-37865090-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>

[19] ČESKO. Úmluva o počítačové kriminalitě. In *Sbírka mezinárodních smluv, Česká republika.* 2013, částka 56, s. 10785.

[20] VANTUCH, P. *Trestní zákoník s komentářem.* Olomouc : ANAG, 2011. s. 829.

bezpečnostních incidentů, 3. protiopatření, tzn. reakce na incidenty. Návrh zákona počítá se dvěma dohledovými pracovišti – národním a vládním. Národní CSIRT pro soukromou a akademickou sféru, Vládní CERT pro státní instituce a kritickou informační infrastrukturu.[21]

Předmětem úpravy připravovaného zákona je úprava práv a povinností fyzických a právnických osob, pravomoc orgánů veřejné moci a jejich vzájemnou spoluprací v oblasti kybernetické bezpečnosti. Nevztahuje se na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.[22]

3.2 Právní úprava v EU

Úmluva o počítačové kriminalitě

Cílem Rady Evropy je dosáhnout větší jednoty mezi členskými státy, které uznávají hodnotu budování spolupráce s ostatními státy, s nimiž byla Úmluva podepsána, jsou přesvědčeny o potřebě prioritního uskutečňování společné trestní politiky zaměřené na ochranu společnosti proti počítačové kriminalitě. Úmluva je nezbytná pro odrazení od činů namířených proti důvěrnosti, integritě a dostupnosti počítačových systémů, sítí a počítačových dat, i proti zneužití těchto systému, sítí a dat tím, že stanoví kriminalizaci takového chování, jak je popsáno v této Úmluvě, a přijetí pravomocí dostatečných pro účinné potírání takových trestných činů tím, že usnadňuje zjišťování, vyšetřování a trestní stíhání takových trestných činů na vnitrostátní i mezinárodní úrovní a stanoví mechanismy pro rychlou a spolehlivou mezinárodní spolupráci.[23]

[21] *NCKB* [online]. [cit. 2014-2-2]. Dostupný z WWW:< http://www.govcert.cz/cs/legislativa/legislativa/>.

[22] ČESKO. Vládní návrh zákona z roku 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dostupné z WWW:< http://www.govcert.cz/download/nodeid-577/>.

[23] ČESKO. Vládní návrh, kterým se předkládá Parlamentu České republiky k vyslovení souhlasu s ratifikací Úmluva o počítačové kriminalitě. In *Senátní tisk č.28* [online]. Senát, © 2014 [cit. 2014-5-1]. Dostupné z WWW:< http://www.senat.cz/xqw/xervlet/pssenat/historie?action=detail&value=3266>.

3.3 Právní úprava v USA

Zákon o přístupových zařízeních

Zákon o přístupových zařízeních popisuje deset typů trestných činů týkajících se přístupových zařízení. Výrazem přístupové zařízení se v něm označuje údaj nebo hardware, který se dá (ať už samostatně nebo v kombinaci s jiným zařízením) použít k získání nebo převodu peněz, služeb nebo jakýchkoliv jiných cenností. Patří sem například hesla, čísla kreditních karet, přístupové kódy pro meziměstská volání nebo PIN, ale i zařízení pro výrobu těchto informací. Aby byly činy uvedené v tabulce č. 1 trestné, musí se jich pachatel dopustit vědomě, s cílem někoho oklamat, a jeho čin musí mít souvislost s mezistátním nebo zahraničním obchodem.[24]

Tabulka 1: Trestné činy podle ustanovení v §1029[25]

Trestný čin	Trest	Příklad
Výroba, použití a obchodování s padělanými přístupovými zařízeními.	Pokuta 50 tisíc dolarů nebo dvojnásobek škody a/nebo až 15 let vězení. Pokuta 100 tisíc dolarů a/nebo až 20 let vězení, pokud se čin opakuje.	Napsání nebo použití programu pro generování čísel kreditních karet.
Použití přístupového zařízení ke získání neautorizovaného přístupu a jakékoliv cennosti v ceně přes 1000 dolarů v průběhu jednoho roku.	Pokuta 10 tisíc dolarů nebo dvojnásobek škody a/nebo až 10 let vězení. Pokuta 100 tisíc dolarů a až 20 let, pokud se čin opakuje	Pachatel pomocí programu odchytí autentizační údaje pro přihlášení do vnitřní sítě firmy Pepsi, odkud následně ukradne recept na Pepsi Colu.

[24] HARRIS, S., HARPER, A., EAGLE, CH., JONATHAN, N., LESTER, M. *Hacking: manuál hackera*. 1. vyd. Praha : Grada, 2008, s. 42-43.

[25] HARRIS, S., HARPER, A., EAGLE, CH., JONATHAN, N., LESTER, M. *Hacking: manuál hackera*. 1. vyd. Praha : Grada, 2008, s. 43-44.

Držení patnácti nebo více falšovaných nebo neautorizovaných zařízení.	Pokuta 10 tisíc dolarů nebo dvojnásobek způsobené škody a/nebo až 10 let vězení. Pokuta 100 tisíc dolarů a/nebo až 20 let vězení, pokud se čin opakuje.	Hacker se dostane do databáze nějaké firmy a ukradne patnáct nebo víc čísel kreditních karet.
Výroba, držení a obchodování s vybavením pro výrobu přístupových zařízení	Pokuta 50 tisíc dolarů nebo dvojnásobek způsobené škody a/nebo až 15 let vězení. Pokuta milion dolarů a/nebo až 20 let vězení, pokud se čin opakuje.	Vytváření, držení anebo prodej zařízení, která umožňují nelegálně získat autentizační údaje.
Ovlivňování transakcí pomocí přístupových zařízení vydaných jiné osobě za účelem získání peněz nebo jiných cenností v celkové hodnotě alespoň tisíc dolarů v průběhu jednoho roku.	Pokuta 10 tisíc dolarů nebo dvojnásobek způsobené škody a/nebo až 10 let vězení. Pokuta 100 tisíc dolarů a/nebo až 10 let vězení. Pokuta 100 tisíc dolarů a/nebo až 20 let vězení, pokud se čin opakuje.	Vytvoření webové stránky, která nabízí neexistující zboží nebo služby a slouží jen ke krádeži čísel kreditních karet.
Nabízení přístupových zařízení nebo prodej informací s návodem, jak získat přístupové zařízení, bez povolení vydavatele přístupového zařízení.	Pokuta 50 tisíc dolarů nebo dvojnásobek způsobené škody a/nebo až 15 let vězení. Pokuta 100 tisíc dolarů a/nebo až 20 let, pokud se čin opakuje.	Prodej kradených čísel kreditních karet.
Použití, výroba, držení nebo obchodování s telekomunikačními	Pokuta 50 tisíc dolarů nebo dvojnásobek způsobené škody a/nebo	Klonování mobilních telefonů a jejich prodej nebo užívání pro osobní účely.

zařízeními, které byly upraveny za účelem získání neautorizovaných telekomunikačních služeb.	až 15 let vězení. Pokuta 100 tisíc dolarů a/nebo až 20 let vězení, pokud se čin opakuje.	
Používání, výroba, držení nebo obchodování s odposlouchávacími zařízeními.	Pokuta 50 tisíc dolarů nebo dvojnásobek způsobené škody a/nebo až 15 let vězení. Pokuta 100 tisíc dolarů a/nebo až 20 let vězení, pokud se čin opakuje	Odposlouchávací zařízení může být libovolné zařízení schopné odposlechu elektronické komunikace a získávání elektronických sériových čísel nebo například identifikačních čísel mobilních telefonů za účelem klonování.
Výroba, držení nebo obchodování s hardwarem nebo softwarem pro úpravu telekomunikačních zařízení za účelem získání neautorizovaného přístupu k telekomunikačním službám.	Pokuta 10 tisíc dolarů nebo dvojnásobek způsobené škody a/nebo až 10 let vězení. Pokuta 100 tisíc a/nebo až 20 let vězení, pokud se čin opakuje.	Do této kategorie spadají například nástroje, které umožňují přenastavení mobilních telefonů za nějakým nekalým účelem nebo hacking telefonních ústředen, a různá zařízení, která útočníkovi dovolují získat telekomunikační služby zdarma.

Zákon o soukromé elektronické komunikaci

Odposlechový zákon už existuje od roku 1918, ale když společnost začala používat elektronickou komunikaci, ECPA platnost tohoto zákona rozšířila i na ni. Pokud si chce vláda poslechnout vaše telefonní rozhovory, sledovat vaši internetovou komunikaci, číst vaše e-maily, sledovat provoz na vaší síti nebo poslouchat, jak šeptáte do kelímku, má možnost. K ochraně komunikace během přenosu slouží Odposlechový zákon, k ochraně komunikace po uložení na nějaké elektronické médium slouží Zákon o ukládání komunikace.[26]

[26] HARRIS, S., HARPER, A., EAGLE, CH., JONATHAN, N., LESTER, M. *Hacking: manuál hackera*. 1. vyd. Praha : Grada, 2008, s. 51

4 ZPŮSOBY ZABEZPEČENÍ PROTI ÚTOKŮM HACKERŮ

Naleznout optimální zabezpečení proti cílenému útoku není jednoduchou záležitostí. Vyžaduje zde vysokou míru informovanosti o konkrétních zabezpečovacích typech a jejich kombinací. Cílem kapitoly je tedy přiblížit informační bezpečnost a konkrétní typy ochran.

4.1 Informační bezpečnost

Tento bezpečnostní obor můžeme stručně vymezit jako specializaci zabývající se ochranou informací. Pod termínem „informační bezpečnost“ tak máme na mysli celý soubor aktivit, směřujících k zajištění důvěrnosti, integrity a dostupnosti. Ve své podstatě je informační bezpečnost multidisciplinární obor nabízející komplexní pohled na problematiku ochrany informací, jež se zabývá otázkami organizačními, řídícími, metodickými, technickými, právními, sociálními a dalšími.[27]

Dostupnost – je pojem z oblasti řízení bezpečnosti v organizaci. Znamená to, že data jsou přístupná v okamžiku jejich potřeby. Označení narušení dostupnosti stanovuje takové případy, ve kterých došlo k nežádoucímu zničení nebo k nedostupnosti. Dostupnost lze vyjádřit jako procento času v daném období, obvykle za rok. Například 90% dostupnost znamená výpadek na 36.5 dne.[28]

Důvěrnost – znamená zajištění, že informace jsou přístupné nebo sděleny pouze tomu, kdo je k jejich přístupu oprávněn.[29]

[27] *Systém online* [online]. [cit. 2014-5-18]. Dostupný z WWW: < http://www.systemonline.cz/clanky/informacni-bezpecnost-pojem-ne-znamy.htm>.

[28] *MANAGEMENT MANIA* [online]. [cit. 2014-5-20]. Dostupný z WWW: < https://managementmania.com/cs/dostupnost-availability>.

[29] *T-soft* [online]. [cit. 2014-5-21]. Dostupný z WWW: < https://www.tsoft.cz/slovnik-pojmu>.

Integrita – dá se definovat jako zajištění správnosti a úplnosti informací, proto se o nežádoucí modifikaci v informační bezpečnosti hovoří jako o narušení integrity. Nutné je si uvědomit, že pokud dojde k nežádoucí změně dat, a to ať už úmyslně, náhodou, nebo technickým selháním v důsledku působení vyšší moci, nemusí být tato nežádoucí změna vůbec odhalena a může uplynout dlouhá doba, než si někdo něčeho všimne.[30]

4.2 Konkrétní způsoby zabezpečení

V oblasti ochrany před útoky hackerů se nabízí tradiční technické prostředky, jakými jsou firewally, kterou jsou v současnosti prakticky téměř nutnost. Dále například IDS, které jsou především monitorovacím nástrojem, umožňující včasnou identifikaci podezřelých aktivit. IDS sice často nabízí i reakční mechanizmy, jejich praktické využití a efektivita je však často přeceňována. Zdánlivě nesouvisející obrany proti útokům jsou produkty z oblasti Content security (antiviry a další). Jak se v průběhu času ukázalo, tak je jednodušší uživateli nějakým způsobem podstrčit škodlivý program (virus, červ, trojský kůň) a např. odposlechnou jeho heslo přímo z klávesnice než složitě luštit zašifrovanou komunikaci. Z kontrolních nástrojů lze uvést kontrolní audit na různé úrovni detailu. Nejrozšířenější slabiny lze jednoduše odhalit vlastními silami s využitím scannerů zranitelnosti. Případně lze využít služeb externích firem a na důkladné pověření systému si můžete najmout White hat hackera, který provede penetrační testování (viz kapitola 5).[31]

4.2.1. Šifrování HDD

Šifrování celého disku můžeme provést jak softwarově, tak hardwarově. V případě softwarové realizace šifrování disku musí být operace šifrování a dešifrování implementována přímo v jádru operačního systému. Pak jsou data šifrována podobně jako u kontejnerového šifrování. Každý blok dat předtím, jako má být uložený na fyzický disk, musí být zašifrován. Tady nastává hlavní problém

[30] *Clever and Smart* [online]. [cit. 2014-5-20]. Dostupný z WWW: < http://www.cleverandsmart.cz/integrita/>.

[31] MIKO, K. Nebezpečí zvané hacking. *CIO Business World.* 2003. č.8, s. 4. ISSN 1803-7321.

softwarového šifrování. Celá tato operace musí být dostatečně efektivní, aby uživatel nepoznal omezení a mohl klidně pracovat, jak je zvyklý.[32]

4.2.2. Firewall

Firewallem by měl být vybaven každý počítač připojený k internetu. Firewall totiž představuje jakousi zeď mezi počítačem a internetem. Chrání váš počítač před útoky hackerů a zároveň řídí odchozí a příchozí data. Umožňuje vám rozhodnout se, zdali třeba nějakému programu umožníte přístup k internetu, nebo nikoliv.[33]

4.2.3. Typy firewallů

Na trhu se vyskytuje mnoho firewall ale v současnosti dominují dva typ: aplikační proxy servery a paketové filtry. Aplikační proxy servery jsou považovány za bezpečnější, hodí se díky své restriktivní podstatě a limitované výkonnosti spíše k řízení toku dat plynoucích směrem ven, než ke kontrole dat směřujících dovnitř na webový server společnosti. Naopak paketové filtry můžeme najít v mnoha velkých organizacích, které kladou vysoké nároky na kapacitu přenášených dat a kvantitu spojení přicházejících z Internetu. Nelze však hovořit o stoprocentní bezpečnosti při použití firewallů. Mnoho firewalů je chybně nakonfigurováno nebo ponecháno bez dozoru.[34]

Tři základní typy filtrování, prováděného firewally:[35]

Filtrování paketů – znamená, že přenášené datové pakety filtruje podle hlavičky použitého přenosového protokolu (IP, TCP/UDP a ICMP). Filtrováním paketů lze uvolnit nebo zablokovat specifické IP adresy nebo čísla portů.

[32] CINKALS, R. Úvod do technik využívaných pro šifrování harddisku. *Hackin9*. 2008, č. 1, s. 27. ISSN 1214-7710.

[33] POČÍTAČ PRO KAŽDÉHO. *Firewally* [online]. © 2014 [cit. 2015-5-14]. Dostupné z WWW: < http://ppk.chip.cz/cs/novinky/ppk-13-2014-vychazi-9-cervna-2014.html>.

[34] SCAMBRAY, J., MCCLURE, S., KURTZ, G. *Hacking bez tajemství.* 2. aktualizované vydání. Praha : Computer Press, 2002. s. 422.

[35] MINISTR. J. *Informatika: informační bezpečnost* [online]. [cit. 2014-5-1]. Dostupný z WWW: < http://www.ivsosoom.cz/_doc_download.php?idd=15>.

Filtrování spojení – je založeno na filtrování spojení souvisejících s již navázaným spojením. Pokud paket není součástí navázaného spojení, nebude propuštěn srze firewall.

Filtrování aplikací – filtruje protokoly odpovídající určitým aplikacím. Například zablokovat Java applety nebo skripty jazyka Visual Basic.

Hardware firewall

Hardwarovým firewallem se dá rozumět soubor technického a programového vybavení, které slouží pouze pro účely sledování a filtrování síťového provozu.[36]

4.3 Aktualizace software

Dalším účinným aspektem obrany je aktualizace operačního systému a softwaru nainstalovaného v něm. Žádný software není bezchybný a v průběhu provozu jsou nalézány bezpečnostní nedostatky.

Podle výzkumu společnosti Avonet vyplývá, že okolo 40 procent uživatelů internetu se pravidelným updatům vyhýbá. Sebelépe zabezpečený systém pak může ohrozit bezpečnostní díra v aplikaci, kterou uživatel nebo administrátor opomněl updatovat.[37]

4.3.1. Aktualizace operačního systému Windows

V případě operačních systémů Windows 2000, XP, Vista, 7 a Windows 8 vycházejí záplaty obvykle dvanáctkrát ročně, a to konkrétně druhé úterý v každém

[36] PŘIBIL, T. Firewall: software nebo hardware?. In *ICT SECURITY: Nezávislý odborný on-line magazín* [online]. Praha : AVERIA LTD., © 2010 [cit. 2014-5-10]. Dostupné z WWW: <http://www.ictsecurity.cz/odborne-clanky/firewall-software-nebo-hardware.html>.

[37] KŘEHÁČEK, P. 9 typů, jak se ochránit před hackery. In *Zlín* [online]. 11.2.2014, [cit. 2014-5-12]. Dostupné z WWW: < http://zlin.cz/512422n-9-tipu-jak-se-ochranit-pred-hackery>.

měsíci. Pro starší systémy (jako jsou třeba Windows 9x/Me a od dubna 2014 na Windows XP) už žádné aktualizace nevycházejí.[38]

4.4 Proxy server

Proxy server neboli počítačový systém nebo aplikace, která se chová jako prostředník pro požadavky klienta, který hledá věci na jiném serveru. Probíhá to tak, že se klient připojí k proxy serveru, vyžádá si určitou službu (připojení, soubor, webovou stránku a další) a proxy server následně tento požadavek zpracuje a zhodnotí dle svých pravidel.[39]

4.5 Bezpečnostní díry

Jedná se o chyby v systému – případně v softwaru, pomocí níž se může do systému dostat útočník, nejčastěji v podobě viru nebo hackera – využívají je i software napsané pro hackery k vytvoření „zadních vrátek“, kterými se může hacker dostat do systému a využívat jej pro své potřeby.[40]

Časté bezpečnostní díry jsou:[41]

1. Špatně definovaná přístupová politika hraničního směrovače. Špatně nakonfigurované ACL mohou způsobit unik informací pomocí ICMP, IP a NetBiosu, což může vést k neoprávněnému přístupu k službám na serverech s DMZ.

[38] *Počítač pro každého.* Jak a proč se aktualizují Windows. Praha : Burda Communications, 2010, č. 6. ISSN 1212-0723.

[39] *Hosting BlueBoard* [online]. [cit. 2014-5-4]. Dostupný z WWW: < http://hosting.blueboard.cz/slovnicek-pojmu/proxy-server>.

[40] *Banan.* [online]. [cit. 2014-5-7]. Dostupný z WWW: < http://www.banan.cz/serialy/nebezpecni-na-internetu/Nebezpeci-na-internetu-Hacking-a-Bezpecnostni-diry>.

[41] SCAMBRAY, J., MCCLURE, S., KURTZ, G. *Hacking bez tajemství.* 2. aktualizované vydání. Praha : Computer Press, 2002. s. 618.

2. Nezabezpečené a špatně monitorované body vzdáleného přístupu představují jednu z nejsnadnějších cest do podnikové sítě. Zaměstnanci se často připojují do Internetu s minimálním zabezpečením a vystavují tak citlivé soubory útoku.
3. Časté používání vztahů důvěry mezi NT doménami, nebo unixové .rhosts a hosts.equiv soubory mohou útočníkům umožnit přístup k důležitým systémům.
4. Uživatelská, nebo testovací konta s rozsáhlými privilegii.
5. Software, který není ošetřen pomocí záplat, je zastaralý, náchylný k útokům, nebo ponechaný v implicitní konfiguraci.
6. Chybějící bezpečnostní politika, procedury a návody.
7. Příliš rozsáhlá přístupová práva k souborům a adresářům (sdílené prostředky NT, NFS exporty pod Unixem).
8. Neautentizované služby typu X Windows, umožňující odposlouchávání vstupů z klávesnice.
9. Slabá, snadno odhadnutelná a neustále znovu používaná hesla na pracovních stanicích mohou vést k ovládnutí serverů.
10. Špatně nakonfigurované Internetové servery, zvláště CGI skripty na webových serverech a anonymní FTP servery.
11. Špatně nakonfigurované ACL na firewallech, nebo směrovačích mohou umožnit přístup do systému ve vnitřní síti buď přímo, nebo prostřednictvím ovládnutého systému z DMZ.
12. Počítače se spuštěnými nepotřebnými službami (například RPC, FTP, DNS, SMPT) mohou být snadno ovládnuty.
13. Prosakování (únik) informací může útočníkovi odhalit verze operačního systému a aplikací, jména uživatelů, skupin, sdílených prostředků, informace z DNS a běžící služby jako je SNMP, finger, SMTP, telnet, rusers, rpcinfo a NetBIOS.
14. Neadekvátní logování, monitorování a detekce průniků na úrovni sítě a systému.

4.6 Typy hackerských útoků

Pro přiblížení hackerský praktik a technik budou v podkapitole uvedeny typy hackerských útoků, zejména sociální inženýrství a metody prolamování hesel.

4.6.1. Sociální inženýrství

Obecně se dá říci, že jde o způsob získávání užitečných informacích od různých lidí, kdy tito lidé netuší, že se stávají cílem útoku. Jsou pak ochotni vyzradit své osobní údaje, přístupová hesla či jiné informace, které mohou útočníkovi pomoci získat neautorizovaný přístup do zabezpečeného systému, případně využít tyto informace ke kompromitaci.[42]

Existují obecné postupy, jak přesvědčit napadeného o potřebě či nutnosti spolupracovat s útočníkem (ať už pasivně, nebo aktivně). První z nich je založen na tom, že se útočník vydává za někoho, koho napadený zná a komu důvěřuje. Čím je iluze důvěryhodnosti dokonalejší, tím pravděpodobnější je, že napadený bude spolupracovat. Významnou limitu tohoto přístupu ale představuje fakt, že útočník může po napadené chtít pouze to, co by po něm mohla vyžadovat autorita, za kterou se vydává. Druhou možností je vydávání se útočníka za někoho, koho napadený osobně nezná, respektive, jehož chování si nedokáže jasně definovat, ale koho považuje za významnou autoritu. Příkladem může být zaměstnanec, který na určité pozici ve firmě osobně nezná nadřízeného, jenž se třeba nachází o tři úrovně výšea o něco zaměstnance požádá. Z toho vyplývá, že když o něco zažádá, měl by zaměstnanec poslechnout, tudíž může nechtěně sdělit citlivé informace.[43]

4.6.2. Prolamování hesel

Nástroje k prolamování hesel lze legálně použít za předpokladu, že chtěné heslo jste si sami nastavili. Nedoporučuje se stahovat žádné nástroje, určené

[42] BUDAI, D. Sociální inženýrství v praxi: Když si hacker o heslo prostě řekne. In *CNEWS* [online]. 2.4.2012, [cit. 2014-3-15]. Dostupné z WWW: < http://www.cnews.cz/socialni-inzenyrstvi-v-praxi-kdyz-si-hacker-o-heslo-proste-rekne >.

[43] BEDNÁŘ, V. Principy a postupy sociálního inženýrství. In *ICT security: nezávislý odborný on-line magazín* [online]. [cit. 2014-5-9]. Dostupné z WWW: < http://www.ictsecurity.cz/odborne-clanky/principy-a-postupy-socialniho-inzenyrstvi.html>.

k prolamování hesel, z pochybných internetových stránek. Na ně totiž umisťují své často pochybné aplikace programátoři s úmyslem například infikovat počítač nežádoucím softwarem.[44]

Útok hrubou silou

Při tomto pokusu o prolomení ochrany heslem jsou automaticky zkoušeny všechny možné kombinace znaků (písmena, číslice, zvláštní symboly apod.), je přitom možné definovat ohraničení délky testovací hesel. Zvláštní variantou jsou takzvané masky, kdy útočník zná určité části hesla na vybraných pozicích, takže testuje pouze zbývající.[45]

Slovníkový útok

Slovníkový útok je technika v oblasti počítačové bezpečnost a kryptoanalýzy, která spočívá ve snaze uhodnout heslo tak, že útočník zkouší pravděpodobná hesla z připravovaného seznamu. Tento seznam je nazýván slovník. Jedná se o potencionálně efektivnější metodu než v případě útoku hrubou silou, poněvadž slovníková metoda obsahuje takové klíče, u kterých útočník pokládá za pravděpodobné, že si je někdo zvolí za heslo.[46]

[44] *PCWorld* [online]. [cit. 2014-5-2]. Dostupné z WWW: < http://pcworld.cz/software/jak-prolomit-temer-kazde-heslo-i-9930>.

[45] *Czech national team* [online]. [cit. 2014-5-6]. Dostupné z WWW: < http://www.czechnationalteam.cz/view.php?cisloclanku=2007090003>.

[46] Slovníkový útok. In *Wikipedia: the free encyclopedia* [online]. St. Petersburg (Florida): Wikipedia Foundation, 11.12.2006, poslední aktualizace 23.12.2013 [cit. 2014-3-17]. Dostupné z WWW: < http://cs.wikipedia.org/wiki/Slovníkový_útok>.

5 PENETRAČNÍ TESTOVÁNÍ

„Hlavním cílem penetračního testování je získat kontrolu nad celou sítí. Sekundárním cílem je dokázat to co nejvíce způsoby, abyste zákazníkovi mohli předložit seznam všech chyb. Penetrační testování (někdy krátce *pen testing*) je výborný způsob, jak vyzkoušet efektivitu firemních bezpečnostních opatření a přijít na hluchá místa v obraně sítě.“[47]

Při bezpečnostních testech infrastruktury je potřeba se zejména zaměřit na:[48]

1. Penetrační testy vnitřní i vnější (scanning, sniffing, redirecting)
2. Zkušební útoky
3. Analýzu zranitelnosti firewallů
4. Kontrolu bezpečnostních pravidel mezi zónami firewallů
5. Analýzu zranitelnosti aktivních prvků
6. Analýzu zranitelnosti operačních systémů na serverech a stanicích
7. Analýzu systému zálohování

5.1 Typy testů

V oblasti informačních technologií podle SELECKÉHO[49] lze testy rozdělit do několika základních kategorií podle způsobu provedení na:

1. Manuální testy – jsou testerem vykonávány manuálně. Mezi výhodami lze klasifikovat možnost vytvořit sofistikované procedury a testy na míru pro specifické podmínky, což automatické testy někdy nedokážou. Další velkou výhodou manuálních testů je, že je provádí člověk a ten umí popsat, co, jak a proč testuje. Výsledky je schopen interpretovat i nezainteresovaným osobám, které nemají o dané oblasti potřebné znalosti (top management, vedení atd.). Za nevýhody je možné považovat časovou

[47] HARRIS, S., HARPER, A., EAGLE, CH., JONATHAN, N., LESTER, M. *Hacking: manuál hackera*. 1. vyd. Praha : Grada, 2008, s. 88

[48] *Svět sítí* [Online]. 2000-2014 [cit. 2014-3-10]. Dostupný z WWW:< http://www.svetsiti.cz/clanek.asp?cid=Penetracni-testy-v-bezpecnostni-analyze-informacniho-systemu-28102007/>.

[49] SELECKÝ, M. *Penetrační testy a exploatace.* Brno : Computer Press, 2012. s. 15.

a znalostní náročnost. Vzhledem k téměř neomezeným možnostem, jak například vytvořit webovou aplikaci, jsou nezbytně rozsáhlé znalosti testované oblasti (HTML, SQL, JavaScript atd.). Časová náročnost je dále způsobena manuálním prováděním testů.

2. Automatizované testy – nabízejí výhody v rychlosti, možnostech, rozšířitelnosti podle vlastních potřeb a v relativně jednoduché verifikovatelnosti a reprodukovatelnosti. Nástroje, které se využívají při automatizovaném testování, byly vytvořeny profesionály, kteří v dané oblasti pracují několik let. Další z výhod v porovnání s manuálními testy je kratší čas na zaučení a následnou aplikaci testů v praxi. Je totiž jednodušší (i časově) naučit se používat aplikaci pro provádění testů než pochopit princip celého testu prováděného manuálně. Mezi nevýhody je možné zařadit neschopnost prezentovat výsledky v uživatelsky přívětivé formě či blíže vysvětlit podrobnosti k danému problému. Pro správnou interpretaci jsou opět nutné znalosti o použité aplikaci a testované oblasti. Další nevýhodou je také nemožnost testovat některé typy zranitelných míst.
3. Semiautomatické testy – jsou kombinací automatických a manuálních testů. Představují kompromis mezi oběma formami se snahou o maximální využití výhod obou forem. Závěrem je třeba připomenout, že žádná forma testů nikdy nepokrývá 100% kódu, a tudíž ani neodhalí všechna přítomná zranitelná místa.
4. Black-box testy – simulují vnější přístup útočníka, který zná jenom vstupy a potenciální výstupy aplikace, ale nikoliv vnitřní strukturu aplikace či sítě. Pro určení vstupů a výstupů testovaného systému je v některých případech nezbytný poměrně rozsáhlý průzkum. Samotná funkcionalita systému je pro testera černou skříňkou (angl. Black-box). Výhodou tohoto typu testů je, že v případě testování aplikací a systému není potřeba znalost použitého programovacího jazyka a není vyžadováno ani zpřístupnění zdrojového kódu, který se často firmy snaží udržet v tajnosti. Další výhodou je vysoká míra variability, tj. možnost přizpůsobit testy na míru požadavkům zadavatele. Mezi nevýhody lze zařadit potřebu širokých znalostí testera. Dále nemusí být objeveny chyby, které vyžadují sofistikovanější přístupy, a není ověřena efektivita (optimalizace) kódu.

5. White-box testy – v porovnání s předchozím typem testů (black-box) jsou pro tyto testy typické plné vstupní znalosti. Jsou založeny na znalosti architektury a zdrojového kódu aplikace nebo, v případě počítačových sítí, na znalosti architektury, typu a počtu přítomných zařízení a na firemních politikách. Při testování probíhá analýza zdrojového kódu, v němž se hledají chyby. Takový druh testů vyžaduje znalost použitého programovacího jazyka a dobře napsaný a okomentovaný kód. Hlavní výhodou je, že znalost kódu nebo struktury sítě umožňuje najít potenciální zranitelná místa v podstatně kratší době při současně podrobnější kompletní analýze. V případě aplikací je přidruženou výhodou také optimalizace kódu, kterou je možné provést na základě nalezených chyby a zranitelných míst. V případě aplikací je nevýhodou nutná znalost použitého programovacího jazyka, což může v nepřímém důsledku zvýšit cenu testu, jelikož je od testera vyžadována vyšší kvalifikace. Další nevýhodou je časová náročnost a relativně úzké zaměření na kód a architekturu.
6. Grey-box testy – jsou alternativou k předchozím dvěma typům testů. Ty se snaží maximálně využít výhody a přínosy obou výše uvedených typů testů. Při testech se využívají znalosti vnitřní logiky aplikace, ale testy probíhají z hlediska uživatele nebo, v případě bezpečnostních testů, potencionálního útočníka. Grey-box testy mohou také zahrnovat metody reverzního inženýrství pro určení limitních hodnot vstupních údajů nebo chybových hlášení.

5.2 Metodiky provádění penetračních testů

Existuje zde řada metodik, podle kterých se penetrační testování provádí. Metodiky komerčních firem jsou veřejnosti utajovány z důvodu možné finanční ztráty či ztráty klientely. Pro naše účely a základní orientaci v problematice dobře poslouží volně šiřitelné a dostupné metodiky OSSSTMM a Testing Guide (viz níže).

- OSSTMM – „Open Source Security Testing Methodology Manual je metodika, která vznikla na základě kolektivních posudků a recenzí předních

odborníků na informační bezpečnost organizace ISECOM, a je určena k provádění bezpečnostních testů a jejich hodnocení. Tato metodika definuje základní kategorie, které souhrnně testují kontrolu informací a dat, bezpečnostní povědomí zaměstnanců, ochranu před podvody a sociálním inženýrstvím, počítačové a telekomunikační sítě, bezdrátová a mobilní zařízení, fyzickou bezpečnost, bezpečnostní procesy, fyzické objekty jako budovy, oblasti či vojenské základny.“[50]

- OWASP – Open Web Application Security Project je celosvětová nezisková organizace, zaměřená na zlepšení bezpečnosti softwaru. Jejím posláním je, aby zviditelnila bezpečnost software, jak pro jedince, tak pro celosvětové organizace, aby mohli učinit, na základě informovanosti, rozhodnutí týkajících se rizik, plynoucích z bezpečnosti softwaru. Každý má možnost podílet se v OWASP a všechny materiály jsou k dispozici pod svobodnou a softwarově otevřenou licencí. OWASP neschvaluje ani nedoporučuje komerční produkty nebo služby.[51]
    - Testing Guide – je projekt OWASP, jehož cílem je pomoci lidem pochopit, co, proč, kdy, kde a jak testovat ve svých webových aplikacích, a to nejen poskytnutím seznamu nebo předpisu otázek, které by měly být řešeny. Výsledkem tohoto projektu je kompletní testovací rámec, ze kterého jiní mohou vytvářet své testovací programy.[52]

5.3 Red teaming

Výraz red team (červený tým) pochází z armádní terminologie (červený tým znamená, že je nepřátelský). Red teaming je tedy simulace nepřítele. Nepřítel může být obecný nebo dobře obeznámený s technikou exploitování a sociálních útoků. Přístupů k red teamingu je mnoho, ale pokud má útok skutečně simulovat nepřítele, musí si červený tým najít svůj vlastní přístup do sítě, a pokud to bude možné, zůstane

[50] *Trustica* [Online]. 2002-2009 [cit. 2014-3-15]. Dostupný z WWW< http://www.trustica.cz/penetracni-testy/>.

[51] *Owasp* [Online]. Last modified on 31 January 2014 [cit. 2014-3-21]. Dostupný z WWW< https://www.owasp.org/index.php/Main_Page>.

[52] OWASP. OWASP Testing guide v3.0. In *OWASP: OWASP Testing Projects* [online]. United States : [cit. 2014-4-14], United States. Dostupné z WWW: < http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf>.

po celou dobu skrytý. Dříve než proběhne testování, je nutné stanovit si primární cíle samotného testu.[53]

[53] HARRIS, S., HARPER, A., EAGLE, CH., JONATHAN, N., LESTER, M. *Hacking: manuál hackera*. 1. vyd. Praha : Grada, 2008, s. 90-91.

6 DOTAZNÍKOVÉ ŠETŘENÍ

Účelem dotazníkového šetření je zjistit, jaké mají uživatelé povědomí o hackingu, jakožto formě počítačové kriminality, a také zjistit, jestli alespoň částečně chrání svá data před případným odcizením, poškozením, změnou či ztrátou. Obecný přehled o vytyčených cílech nám dá 14 uzavřených otázek.

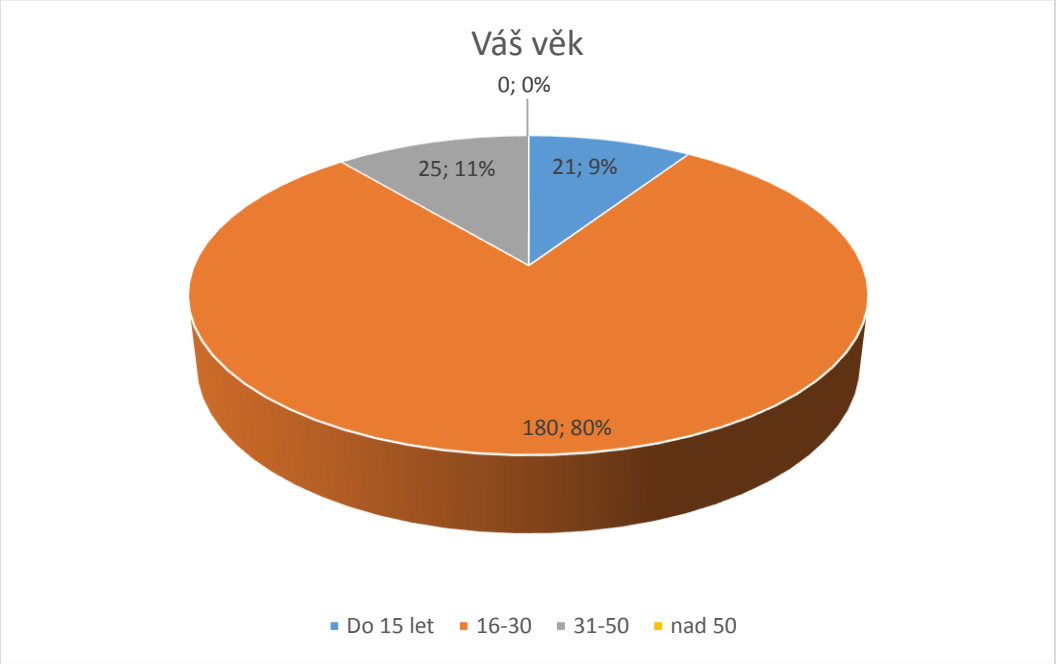
Dotazník byl prezentován převážně v elektronické formě a částečně ve formě tištěné. Výběr respondentů probíhal především na sociálních sítích, protože je zde pravděpodobnost, že uživatelé znají počítač a komunikační techniku, a využívají tak zmíněná informační zařízení téměř denně. Dotazník vyplnilo 226 respondentů, přičemž ze získaných tak jsou v závěru vydaná doporučení, jakými nástroji je vhodné chránit bezpečnost.

V rámci dotazníkového šetření byly stanoveny dvě hypotézy. V první hypotéze se domnívám, že 60% dotazovaných se již setkala s termínem hacking. Druhá hypotéza stanovuje nedbalost respondentů, co se týče ochrany dat a informačních systémů, konkrétně, že na počítači nemají nainstalovanou antivirovou ochranu.

1. Věková skupina

Otázka cílená na věkovou kategorii byla stanovena spíše orientačně. Mladších 15 let bylo 21 respondentů. Mezi 16-30 lety vyplnilo dotazník nejvíce respondentů, a to v celkovém počtu 180. Do věkově kategorie 31-50 spadalo celkem 25 dotazovaných. Mezi dotazovanými nad 50 nikdo nebyl.

Graf 1: věkové skupiny respondentů[54]



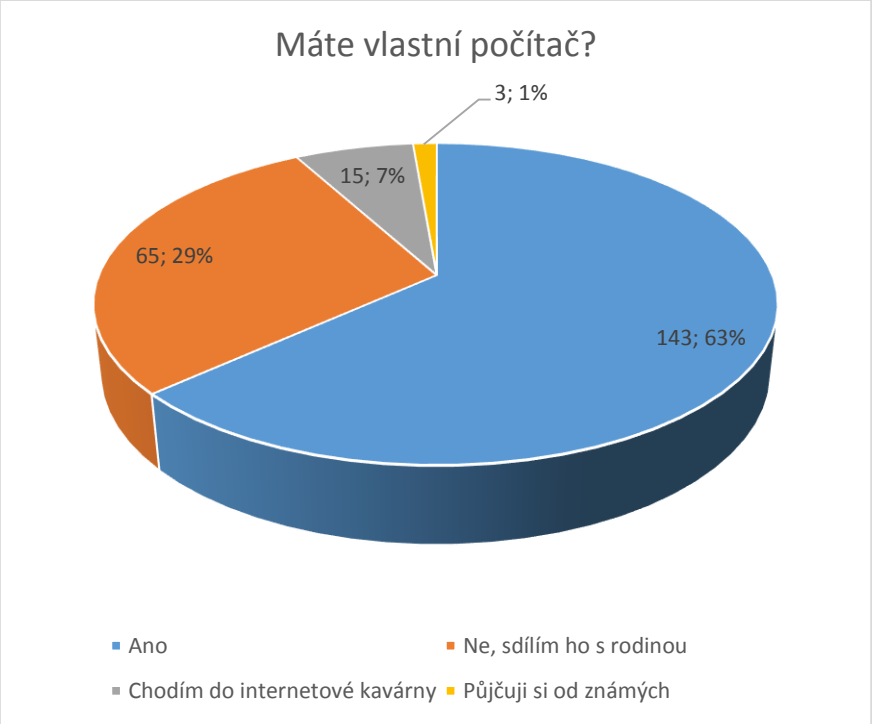
[54] Vlastní zdroj

2. Máte vlastní počítač

Tato otázka si klade za cíl zjistit, zda uživatelé vlastní svůj počítač nebo ho sdílí s jinými uživateli. Sdílení počítače s jinými uživateli přináší více bezpečnostních rizik, než je tomu u uživatele, který disponuje vlastním počítačem.

Hodnoty grafu však ukazují, že ne každý disponuje vlastním počítačem. Dá se tedy říci, že jsou vystaveni vyššímu riziku kyberzločinu, jelikož zařízení, která využívají, spravuje někdo jiný. Plyne z toho fakt, že uživatelé nemohou adekvátně zabezpečit svá data dle doporučení, či vlastních potřeb.

Graf 2: vlastní počítač[55]

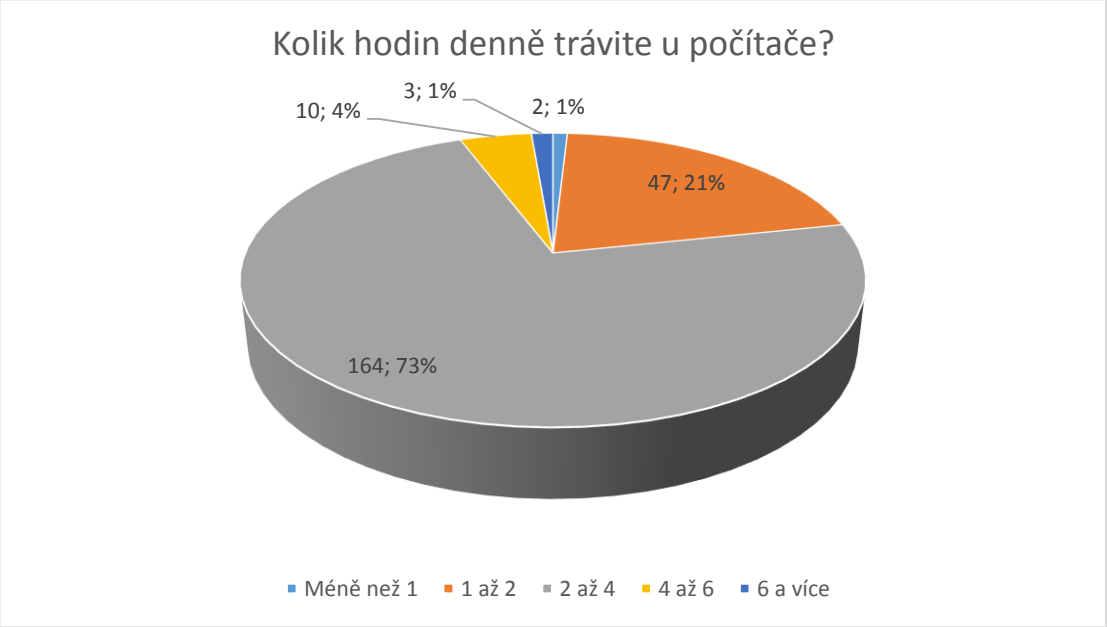


[55] Vlastní zdroj

3. Kolik hodin denně trávíte u počítače?

Čím více strávených hodin na počítači (bereme v úvahu neustále připojení k internetu), tím větší je pravděpodobnost, že se stane uživatel potencionální obětí počítačové kriminality či on sám bude pachatelem této sofistikované kriminality. Na méně než 1 hodinu odpověděli 2 dotazovaní, 47 sedí u počítače 1-2 hodiny denně, nejvíce respondentů prosedí u počítače 2-4 hodiny denně, a to v celkovém počtu 164. Možnost 4-6 hodin zvolilo 10 a víc jak 6 hodin denně tráví 3 respondenti.

Graf 3: počet strávených hodin na počítači[56]

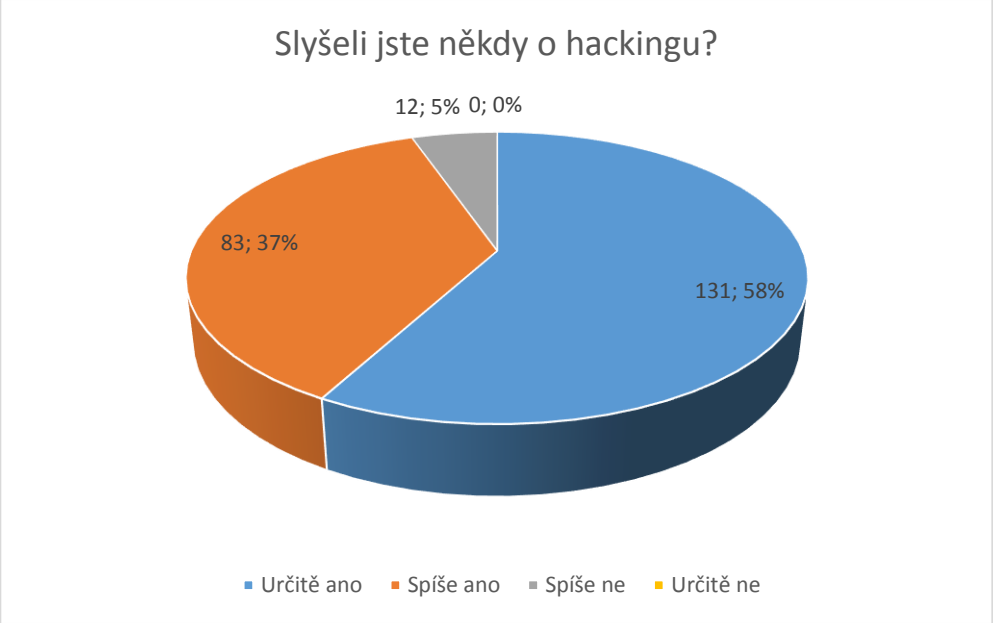


[56] Vlastní zdroj

4. Slyšeli jste někdy o hackingu?

Cílem této otázky je zjistit, zda se uživatelé počítačů setkali s termínem hacking. Vyhodnocení otázky reflektuje, že většina uživatelů se s tímto pojmem setkali, a to v počtu 131. Dalších 83 dotazovaných odpovědělo spíše ano. Možnost spíše ne vybralo 12 a určitě o tom neslyšelo 0 respondentů.

Graf 4: znalost pojmu hacking[57]

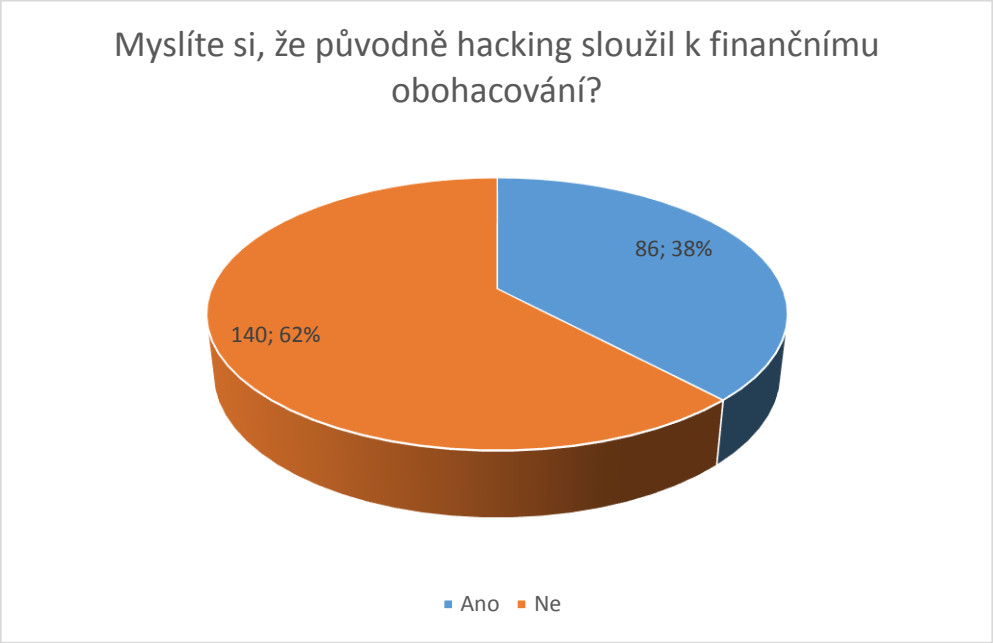


[57] Vlastní zdroj

5. Myslíte si, že původně hacking sloužil k obohacování?

Smyslem této otázky je poznat, zdali respondenti alespoň tuší, že původně hacking nesloužil k nelegálním účelům, nýbrž měl pomoci ke zjednodušení postupu a ke zdokonalení a odhalování chyb v softwarových produktech. Díky desinterpretaci a rovněž sjednocování výrazů hacking a cracking v masmédiích, může docházet k tomu, že budou stejně tak zaměňovány u dotazovaných. Celkem 15 dotazovaných má mylnou představu o hackingu, tudíž vybrali možnost Ano. Zbývajících 201 zná původní primární cíl.

Graf 5: znalost původního významu hacking[58]



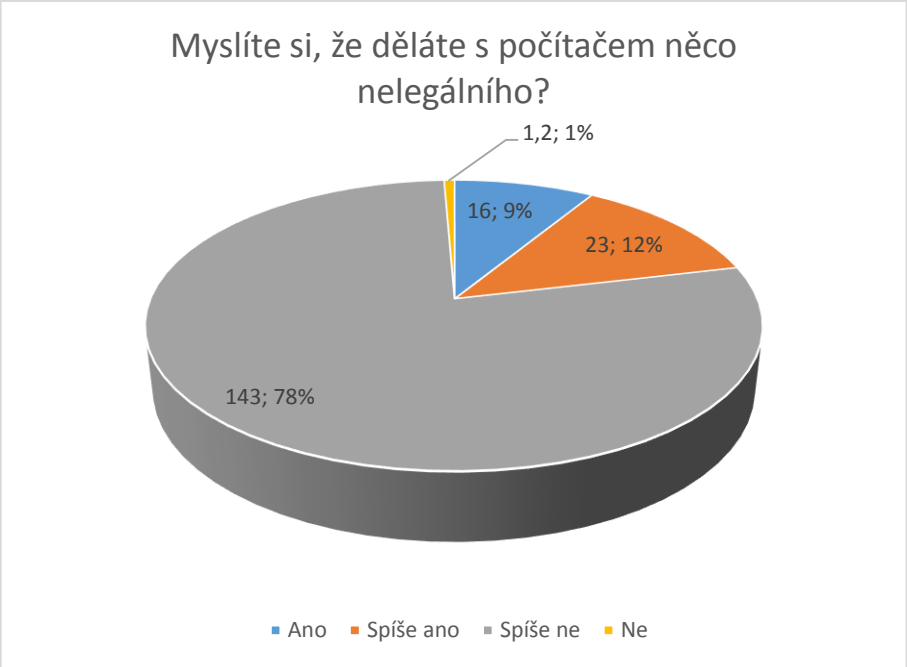
[58] Vlastní zdroj

6. Myslíte si, že děláte s počítačem něco nelegálního?

Dle očekávání, většina dotázaných si je jista nebo se domnívá legitimností svého chování na počítači. Z výstupních dat poznáme následující: možnost „Určitě ano“ vybralo celkem 16 dotazovaných. Ti, kteří shledávají ve svém počínání možnou nelegálnost, vyšli do celkového počtu 23. Naopak, volbu „Spíše ne“, zvolili ve 143 případech, a uživatelů, vědomích si etického jednání a jednání v souladu se zákonem, odpovědělo 44.

V získaných datech mohou vznikat mírné niance, poněvadž ne všichni respondenti mají dostatečné povědomí o trestných činech v kyberprostoru a o kriminalizaci určitých skutků a jejich právní povědomí není tak široké, aby si toho mohli být vědomi. Rovněž stojí za připomenutí fakt o tom, že informační technologie je poměrně novou záležitostí, tudíž zákonné podchycení není natolik efektivní jako v trestných činech, při nichž se pachatel na místě činu nachází nebo nacházel fyzicky.

Graf 6: vědomí uživatelů o legitimnosti svého chování v kyberprostoru[59]



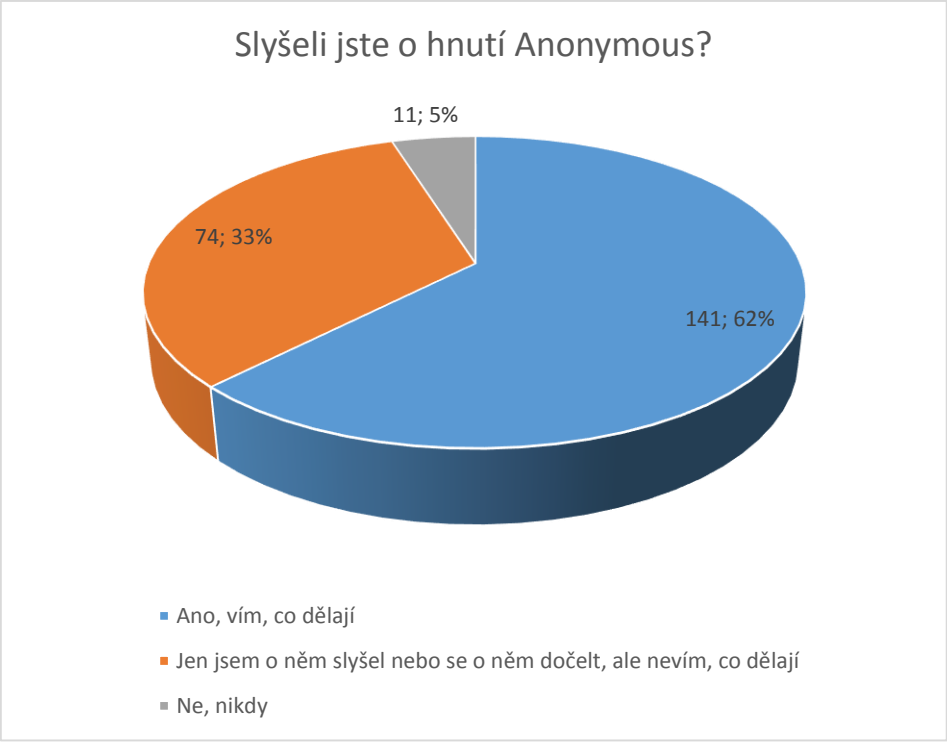
[59] Vlastní zdroj

7. Slyšeli jste o hnutí Anonymous?

Jelikož v bakalářské práci je zmínka o hnutí Anonymous, s nimiž úzce souvisí hacking a podobné aktivity, tak bylo zapotřebí zjistit, jestli veřejnost zná zmíněné hnutí a jejich cíle.

Téměř ¾ dotázaných prokázalo jejich povědomí o tom, kdo nebo co Anonymous je, a jaké jsou jejich záměry. Zbytek o hnutí slyšel, nebo vůbec neví, co nebo proč hnutí existuje.

Graf 7: hnutí Anonymous[60]



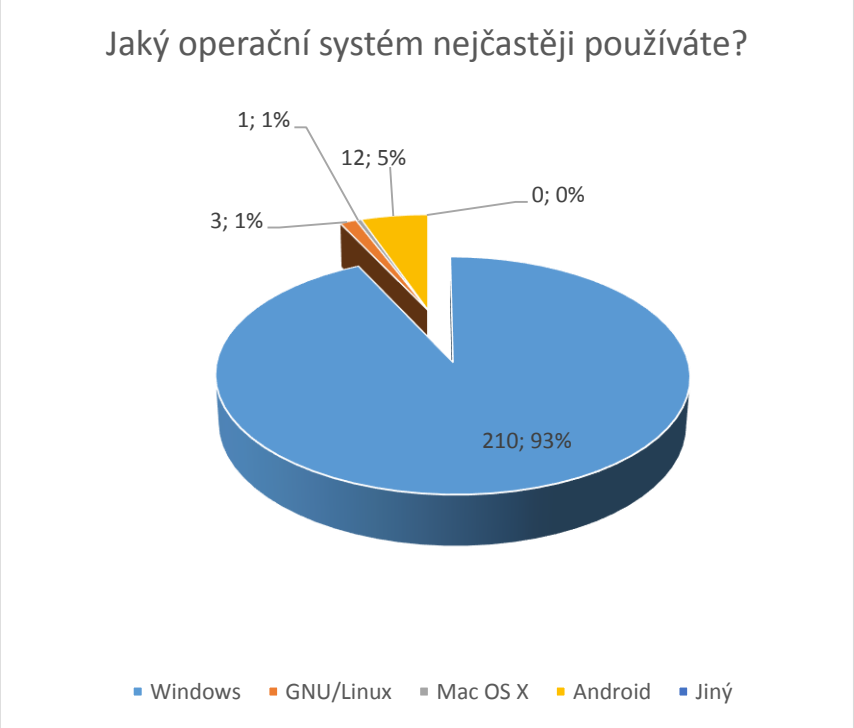
[60] Vlastní zdroj

8. Jaký operační systém nejčastěji používáte?

Volbě operačního systému musíme věnovat patřičnou pozornost. Je dobré si předem stanovit priority, pro které chceme výpočetní zařízení používat.

Výsledky průzkumu můžeme předpokládat, ale s příchodem operačního systému Android, to není až tak jednoznačné, jak se může na první pohled zdát. Samozřejmě nejvíce respondentů pro svou činnost využívá komerční produkt od Microsoftu, hodnota je 210 z 226 dotázaných. Překvapivý výsledek byl zaznamenán u GNU/Linux a Androidu. Osobní odhad se pohyboval v rozmezí 5-6 pro GNU/Linux, ale výstupní data ukazují, že 3 z celkového počtu dotázaných využívají právě Linux. Pro Android byl odhadovaný počet nižší, než v případě Linuxu. Překvapivý výsledek ale ukazuje popularitu Androidu. Celkem 12 dotázaných pro denní potřebu využívá převážně Android. Výsledek Mac OS X dopadl dle očekávání, a to v celkovém počtu jednoho uživatele z 226 dotázaných.

Graf 8: operační systém[61]



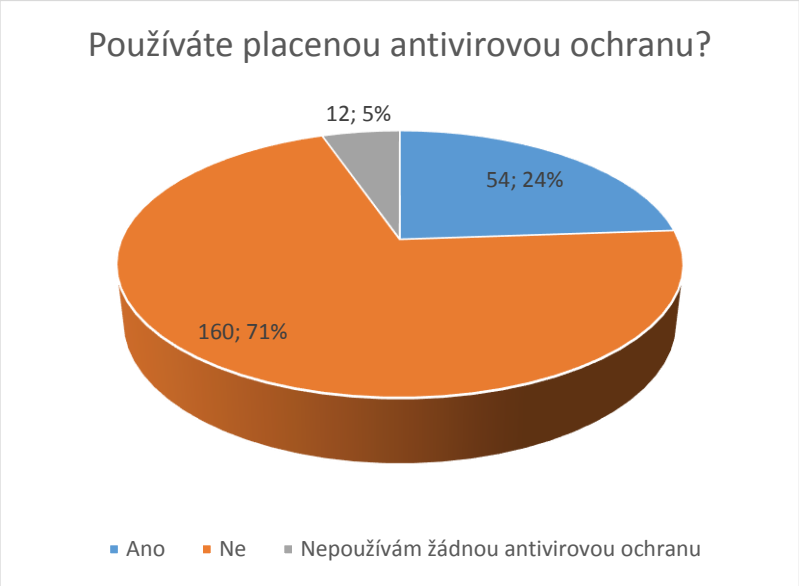
[61] Vlastní zdroj

9. Používáte na počítači antivirovou ochranu?

Zřízení kvalitní antivirová ochrana je správným krokem k zabezpečení citlivých dat. Kdo používá systém Windows, tak je skoro povinen nainstalovat antivirovou ochranu, protože právě na Windows, díky své rozšířenosti, nalezneme nejvíce škodlivého softwaru a povětšinou je v hledáčku škůdců.

Graf znázorňuje následující: 54 dotázaných se chrání antivirovou programem, 160 dotázaných má antivir s bezplatnou licencí a 12 nemá žádnou ochranu. Respondenti, kteří v dotazníku uvedli, že využívají většinou operační systém GNU/Linux, Mac OS X a Android, rovněž uvedli, že na zařízeních se zmíněnými operačními systémy, nemají žádnou antivirovou ochranu.

Graf 9: antivirová ochrana[62]



[62] Vlastní zdroj

10. Aktualizujete pravidelně operační systém a programy v něm nainstalované?

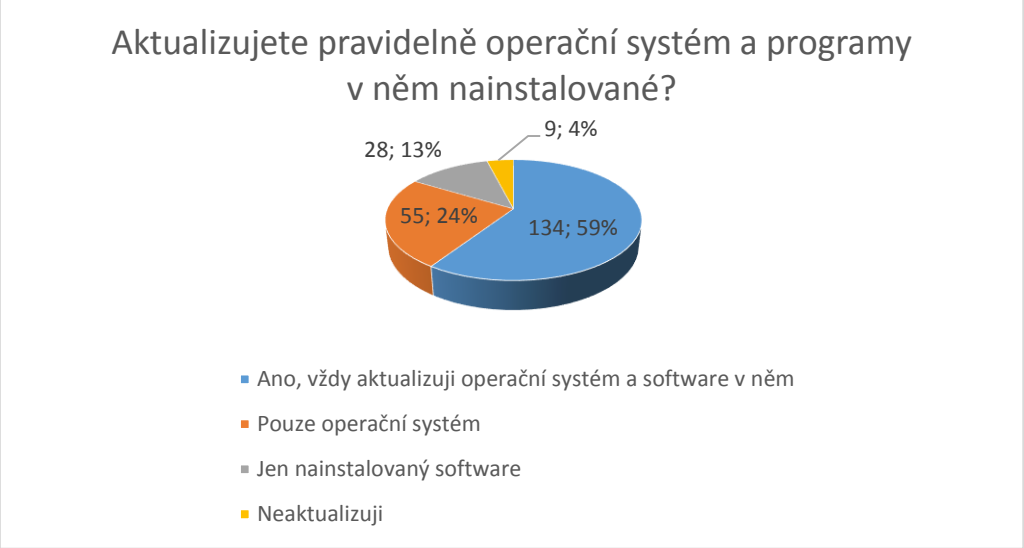
Smysl otázky je jednoznačný. Má za cíl zjistit, jestli uživatelé dbají na pravidelnou aktualizaci operačního systému a softwaru implementovaného v počítači nebo v jiném informačním zařízení.

Praxe dokládá fakt o skutečnosti, že většina bezpečnostích „skulin“ v operačních systémech a v softwaru je nalezena až poté, co jsou uvedeny na trh nebo při dlouhodobějším užívání.

Výsledky průzkumu přinesl pohled, kdy 134 respondentů vždy aktualizuje operační systém a software v něm, 55 aktualizuje pouze operační systém, 28 aktualizuje pouze software. A celkem 4% procenta riskují a neaktualizují operační systém ani jiný software.

Za připomínku stojí prohlášení firmy Microsoft o ukončení podpory Windows XP dne 8. dubna 2014. Znamená to, že nebude nadále poskytovat opravné aktualizace, a tudíž počítač s Windows XP připojený k internetu může být snáze ohrožen bezpečnostními hrozbami.[63]

Graf 10: aktualizace[64]



[63] WINDOWS. End support help. *Windows.microsoft.com* [online]. © 2014 [cit. 2014-4-20]. Dostupné z WWW: < http://windows.microsoft.com/cs-cz/windows/end-support-help>.

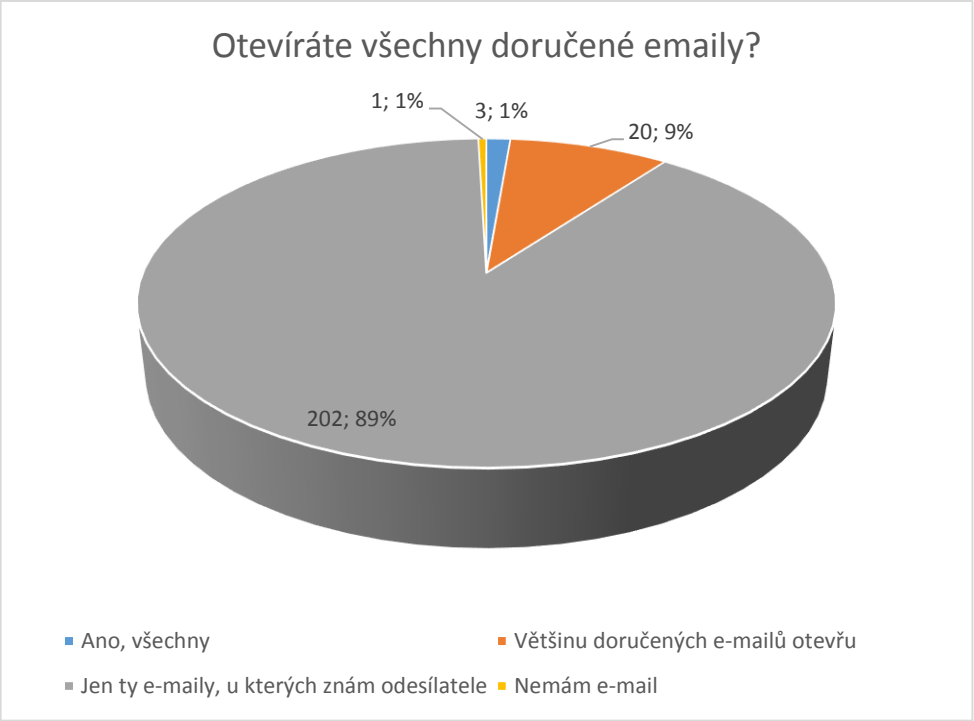
[64] Vlastní zdroj

11. Otevíráte všechny doručené emaily?

Anonymní emaily se objevují stále více a více. Mají nejrůznější podobu a obsah, ovšem cíl je stejný. Většinou jde o klamání uživatelů a získání důvěry, a ti třeba podlehnou a uvěří. Ti pak v emailu například otevřou nevhodnou přílohu, či vyplní citlivé údaje. Výsledkem je poté zavirovaný počítač, ztráta dat, či zmizení finančních prostředků z peněžního účtu.[65]

Na základě výše zmíněných faktech dojdeme ke zjištění, že drtivá většina dotázaných má ponětí o hrozbách, možno skrývajících se v e-mailových zprávách s pochybným údajem o odesílateli, a snaží se jim vyhnout. Tedy 202 uživatelů otevírá jen ty zprávy, u kterých znají původce. Většinu e-mailů otevře 20 dotázaných a 3 z dotázaných otevírá veškerou doručenou poštu. Ovšem nejlépe se chrání před infikovanými zprávami 1, ten e-mail nemá.

Graf 11: otevírání emailů[66]



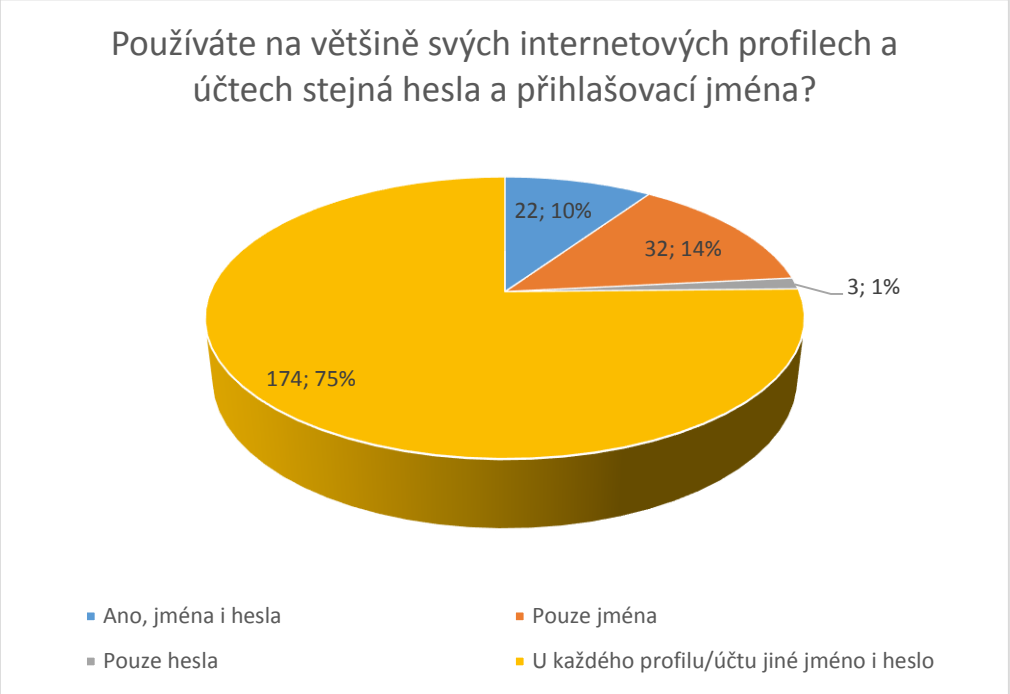
[65] KRAJSKÉ ŘEDITELSTVÍ POLICIE. *Zpravodajství.* Policie.cz [online]. © 2014 [cit. 2014-6-1]. Dostupné z WWW: < http://www.policie.cz/clanek/nenechte-se-zmast-podvodnymi-maily.aspx>.

[66] Vlastní zdroj

12. Používáte na většině svých internetových profilech nebo účtech stejná hesla a přihlašovací jména?

V internetové prostředí většina uživatelů má vytvořený alespoň jeden profil nebo účet. V tomto ohledu ani nezáleží na jakém serveru má daný uživatel účet vytvořený, či spíše na použitých autentizačních údajích, za pomoci nichž se na konkrétní profil nebo účet přihlašuje. Jednoduché volby hesla, mohou být například prolomeny slovníkovým útokem. Naštěstí ¾ dotázaných používá různé kombinace přihlašovacích údajů, tudíž nejsou vystaveni tak velkému riziku kompromitace údajů na dalších účtech/profilech.

Graf 12: hesla a přihlašovací jména[67]

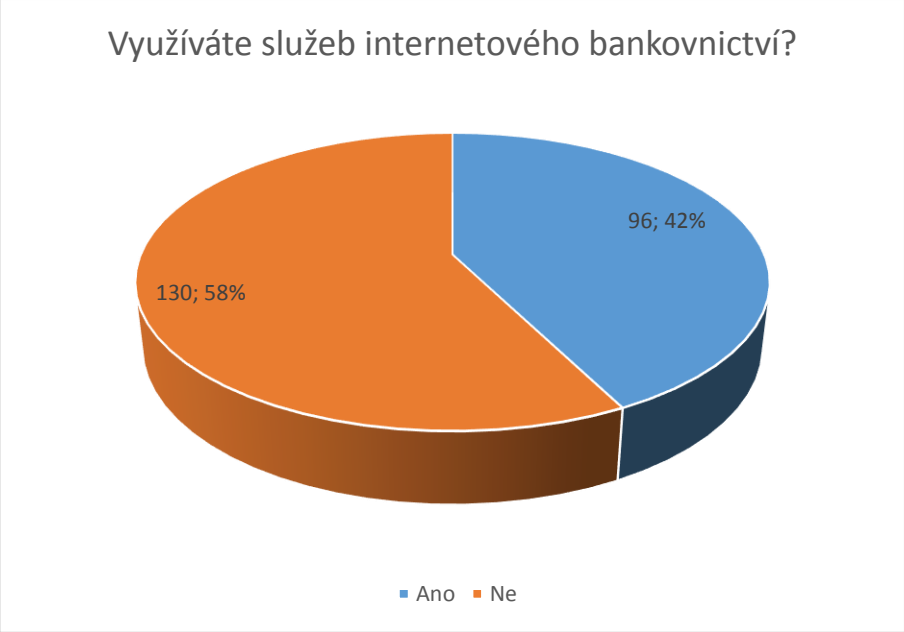


[67] Vlastní zdroj

13. Využíváte k placení internetové bankovnictví?

Útoky hackerů často směřují k prolomení systému, za účelem získání údajů o bankovních účtech poškozeného. Údaje hackeři mohou poskytnout crackerům za úplatu, a ti (vycházíme-li z definice pojmu cracker) účty nabourávají a peníze převádí na jiné, zejména na své účty.

Graf 13: internetové bankovnictví[68]



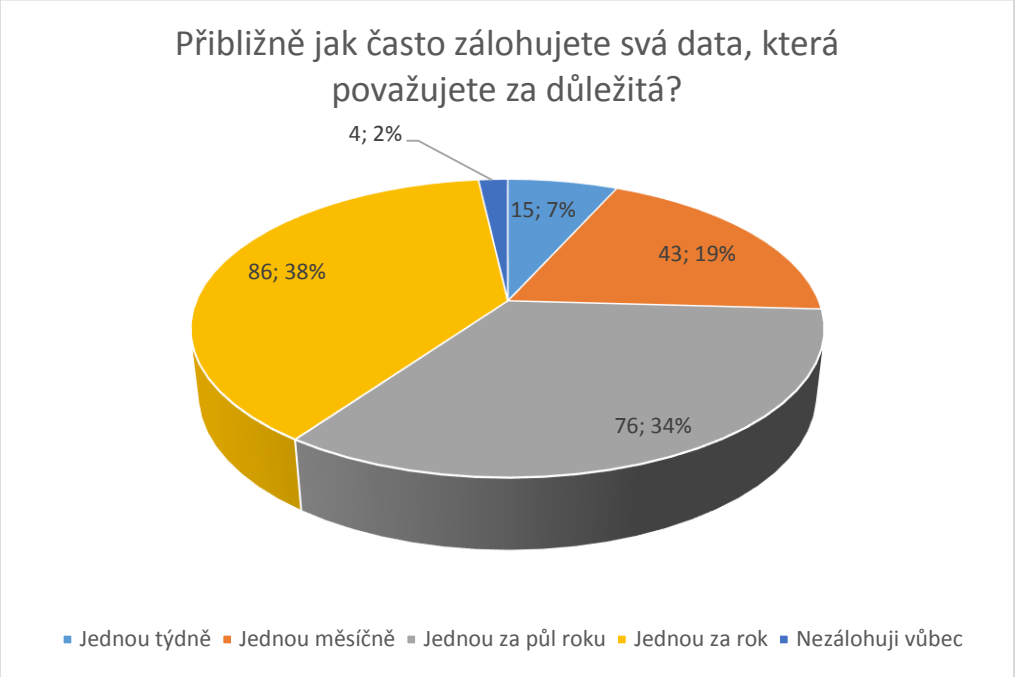
[68] Vlastní zdroj

14. Přibližně jak často zálohujete svá data, která považujete za důležitá?

Zálohu dat je vhodné provádět v časových cyklech v závislosti na důležitosti s nakládanými údaji či uloženými daty.

Průzkum ukázal, že 15 dotázaných svá důležitá data zálohuje alespoň jednou týdně, 19% z dotázaných zálohuje jednou měsíčně. Nejvíce dotázaných provádí zálohu jednou za rok, a těch co neprovádí zálohu, jsou pouze 2%.

Graf 14: záloha dat uživatelů[69]



[69] Vlastní zdroj

ZÁVĚR

Cílem bakalářské práce bylo přiblížit počítačovou kriminalitu, a to konkrétně hacking. Počítačová kriminalita patří téměř na vrchol hospodářské kriminality, jelikož velký rozmach výpočetní techniky způsobil, že se k těmto nástrojům dostanou i lidé, jejichž záměry jsou: ničit, krást a škodit, a to vše za celkově nízké pořizovací náklady.

Do první kapitoly spadají pojmy důležité pro pochopení problematiky. Byly zde detailně porovnáni subjekty hacker a cracker. Analýzou informací z odborných publikací, týkající se informačních a komunikačních technologií, docházíme k překvapivému závěru, že původně hacker měl pomoci při nalézání důmyslných řešení a při odhalování bezpečnostních nedostatků v softwarových produktech. Cracker na rozdíl od hackera využívá výpočetní techniku zejména pro páchání škod a k vlastnímu obohacení. V masmédiích dochází k záměnám mezi uváděnými subjekty.

Páchání trestné činnosti na informačních a komunikačních technologiích v České republice reguluje trestní zákoník č. 40 z roku 2009. Proti starému zákoníku č. 140 z roku 1961 byl doplněn o další skutky. Doplněné skutkové podstaty vychází především z Úmluvy o počítačové kriminalitě. Americké federální právo počítačovou kriminalitu postihuje zejména na základě: zákona o přístupových zařízeních, zákona o počítačových podvodech, zákona o soukromé elektronické komunikaci a zákona o vylepšení počítačové bezpečnosti.

Obětí počítačové kriminality může být téměř každý připojený uživatel k Internetu, jelikož důmyslnost praktik a technik soudobých hackerů/crackerů přesahuje hranice znalostí většiny lidí i těch, kteří pracují s informačními technologiemi. Při analýze bezpečnostních opatření bylo zjištěno, že neexistuje stoprocentní ochrana před kybernetickými narušiteli, tedy když bereme v úvahu fakt, že počítač či jiné informační zařízení přistupuje k Internetu.

Penetrační testování se hodí zejména pro firmy, které využívají informační a komunikační technologie a uchovávají v systémech citlivá nebo důležitá data. Tichý penetrační test může ověřit i připravenost IT personálu a odhalit i nedostatky v rámci interního prostředí firmy či organizace. Při použití penetrační testů je třeba dbát na to, že žádný test vám nezajistí stoprocentní ochranu. Často jsou testy velice vytěžující, a to ať po znalostní stránce nebo po stránce finanční.

Kvantitativní šetření prokázalo, že většina dotazovaných má určité povědomí o bezpečnostních rizicích a snaží se před nimi alespoň částečně bránit. Z vlastního šetření vycházejí následující doporučení pro běžné uživatele.

Níže doporučená opatření mají preventivní charakter:

Přihlašovací jména a hesla – V tomto ohledu doporučuji, ať už uživatelé využívají jakýkoliv profil či účet na internetu, aby při zřizování jednotlivých účtů nebo profilů dbali na správnou volbu přihlašovacího jména a hesla. Minimální počet by měl být 8 znaků, a to v kombinaci velkých a malých písmen, čísel, či jiných znaků. Útočníkovi je tím znesnadněn nebo alespoň oddálen přístup k dalším profilům nebo účtům.

Aktualizace operačního systému a software – Pravidelná aktualizace sice nezajistí bezchybnost, ale odstraní dosud zjištěné nedostatky a snižuje pravděpodobnost napadení daného zařízení. Je tedy vhodné u softwarového vybavení nakonfigurovat automatickou aktualizaci, přičemž je rovněž vhodné provádět kontrolu aktualizací manuálně. V případě operačního systému Windows Vista a výše, doporučuji zapnout Windows Update, jenž zvládá automatickou kontrolu a implementaci aktualizací.

Pravidelná kontrola před nežádoucím softwarem – Kontrolu a eliminaci škodlivého software, zajistíme především kvalitní antivirovou ochranou, doporučuji spíše placenou licenci. Antivirovou ochranu je vhodné použít v kombinaci se scannery, detekující spyware, malware, phising a další hrozby.

Záloha dat – Zde je doporučení, aby záloha dat byla prováděna pravidelně a v kratších časových úsecích. Zálohu dat především provádíme za pomoci jiného

média, než na kterém se data připravená k záloze nachází (např. flash disk, externí pevný disk, cloudové úložiště a další).

Účet bez administrátorský práv – Zřízením uživatelského účtu, bez privilegovaných práv zajistíme, že v případě nabourání do systému nebudou automaticky administrátorská práva převzata útočníky.

Napadené společnosti nebo napadení uživatelé by měli informovat buď Národní centrum kybernetické bezpečnosti, nebo sdružení CZ.NIC. Národní centrum kybernetické bezpečnosti se stará o kybernetické zabezpečení státní správy a kritické infrastruktury, do níž patří například energetické nebo vodovodní sítě. CZ.NIC pak zabezpečuje ostatní komerční sféru.[70]

Splnění hypotéz:

Hypotéza 1: Počet respondentů, kteří jsou obeznámeni s problematikou hackingu je celkem 63%, tudíž hypotéza je splněna.

Hypotéza 2: Počet respondentů, kteří chrání počítač antivirem, je celkem 73% procent, z toho vychází, že hypotéza nebyla splněna.

[70] E15. Zprávy. *E15.cz* [online]. © 2014 [cit. 2014-2-6]. Dostupné z WWW: < http://zpravy.e15.cz/byznys/finance-a-bankovnictvi/do-boje-s-hackery-se-zapoji-bezpecnostni-urad-963107>.

SEZNAM POUŽITÝCH ZDROJŮ

Literární zdroje

1. CINKALS, R. Úvod do technik využívaných pro šifrování harddisku. *Hackin9*. 2008, č. 1, 45 s. ISSN 1214-7710.
2. ERICKSON, J. Hacking - umění exploitace. Brno : Zoner Press, 2008. 544 s. ISBN 978-80-7413-022-9
3. HARRIS, S., HARPER, A., EAGLE, CH., JONATHAN, N., LESTER, M. *Hacking: manuál hackera*. 1. vyd. Praha : Grada, 2008, 400 s. ISBN 978-80-247-1346-5.
4. MIKO, K. Nebezpečí zvané hacking. *CIO Business World.* 2003. č.8, 52 s. ISSN 1803-7321.
5. SELECKÝ, M. *Penetrační testy a exploatace.* Brno : Computer Press, 2012. 646 s. EAN 9788072266449.
6. SCAMBRAY, J., MCCLURE, S., KURTZ, G. *Hacking bez tajemství.* 2. aktualizované vydání. Praha : Computer Press, 2002. 625 s. ISBN 80-7226-644-6.
7. SMEJKAL, V. *Internet a §§§*. 2. aktualizované, přepracované a rozšířené vydání. Praha : Grada Publishing, 2001, s. 151-152. ISBN 8024700581.
8. VANTUCH, P. *Trestní zákoník s komentářem.* Olomouc : ANAG, 2011. 1386 s. ISBN 978-80-7263-677-8.

Legislativní dokumenty

1. ČESKO. Úmluva o počítačové kriminalitě. In *Sbírka mezinárodních smluv, Česká republika.* 2013, částka 56, s. 10790
2. ČESKO. Vládní návrh zákona z roku 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dostupné z WWW:< http://www.govcert.cz/download/nodeid-577/>.
3. ČESKO. Vládní návrh, kterým se předkládá Parlamentu České republiky k vyslovení souhlasu s ratifikací Úmluva o počítačové kriminalitě. In *Senátní tisk č.28* [online]. Senát, © 2014 [cit. 2014-4-16]. Dostupné z WWW:<

http://www.senat.cz/xqw/xervlet/pssenat/historie?action=detail&value=3266 >.

4. ČESKO. Zákon č. 140 ze dne 29. listopadu 1961 trestní zákon. In *Sbírka zákonů České republiky.* 2002, částka 146, s. 8093. Dostupné také z WWW:< http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=2002&typeLaw=zakon&What=Rok&stranka=6 >.
5. UNITED STATES. Copyright act of 1976. Copyright Law of the United States [online]. [cit. 2014-1-11]. Dostupný z WWW:< http://www.copyright.gov/title17/circ92.pdf>.

Elektronické zdroje

1. BUDAI, D. Sociální inženýrství v praxi: Když si hacker o heslo prostě řekne. In *CNEWS* [online]. 2.4.2012, [cit. 2014-3-15]. Dostupné z WWW: < http://www.cnews.cz/socialni-inzenyrstvi-v-praxi-kdyz-si-hacker-o-heslo-proste-rekne >.
2. BEDNÁŘ, V. Principy a postupy sociálního inženýrství. In *ICT security: nezávislý odborný on-line magazín* [online]. [cit. 2014-5-9]. Dostupné z WWW: <http://www.ictsecurity.cz/odborne-clanky/principy-a-postupy-socialniho-inzenyrstvi.html>.
3. *Clever and Smart* [online]. [cit. 2014-5-20]. Dostupný z WWW: < http://www.cleverandsmart.cz/integrita/>.
4. *Czech national team* [online]. [cit. 2014-5-6]. Dostupné z WWW: < http://www.czechnationalteam.cz/view.php?cisloclanku=2007090003>.
5. E15. Zprávy. *E15.cz* [online]. © 2014 [cit. 2014-2-6]. Dostupné z WWW: < http://zpravy.e15.cz/byznys/finance-a-bankovnictvi/do-boje-s-hackery-se-zapoji-bezpecnostni-urad-963107>.
6. Hacker. In *Wikipedia: the free encyclopedia* [online]. St. Petersburg (Florida): Wikipedia Foundation, 11.12.2006, poslední aktualizace 30.5.2014 [cit. 2014-5-30]. Dostupné <http://cs.wikipedia.org/wiki/Hacker>.
7. JIROVSKÝ, V., HNÍK, V., KRULÍK, O. Základní definice, vztahující se k tématu kybernetických hrozeb. In Ministerstvo vnitra České republiky. *Informační kriminalita* [online]. Praha : MVČR, 2008 [cit. 2013-12-

20]. Dostupné z WWW: <http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/zakladni_info.pdf >.

8. KRAJSKÉ ŘEDITELSTVÍ POLICIE. *Zpravodajství.* Policie.cz [online]. © 2014 [cit. 2014-6-1]. Dostupné z WWW: < http://www.policie.cz/clanek/nenechte-se-zmast-podvodnymi-maily.aspx>.
9. *MANAGEMENT MANIA* [online]. [cit. 2014-5-20]. Dostupný z WWW: < https://managementmania.com/cs/dostupnost-availability>.
10. MINISTR. J. *Informatika: informační bezpečnost* [online]. [cit. 2014-5-1]. Dostupný z WWW: < http://www.ivsosoom.cz/_doc_download.php?idd=15>.
11. *NCKB* [online]. [cit. 2014-2-2]. Dostupný z WWW:< http://www.govcert.cz/cs/legislativa/legislativa/>.
12. *Owasp* [Online]. Last modified on 31 January 2014 [cit. 2014-3-21]. Dostupný z WWW< https://www.owasp.org/index.php/Main_Page>.
13. OWASP. OWASP Testing guide v3.0. In *OWASP: OWASP Testing Projects* [online]. [cit. 2014-4-14], United States. Dostupné z WWW: < http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf>.
14. *Pakoš* [online]. [cit. 2013-12-20]. Dostupný z WWW< http://pakos.cz/co-je-to-hacking>.
15. *PCWorld* [online]. [cit. 2014-5-2]. Dostupné z WWW: < http://pcworld.cz/software/jak-prolomit-temer-kazde-heslo-i-9930>.
16. *Počítačová bezpečnost a ochrana dat* [Online]. [cit. 2014-1-10]. Dostupný z WWW:<http://marlib.cmsps.cz/bezpecnost/bezpecnost.html/>.
17. POČÍTAČ PRO KAŽDÉHO. *Firewally* [online]. © 2014 [cit. 2015-5-14]. Dostupné z WWW: < http://ppk.chip.cz/cs/novinky/ppk-13-2014-vychazi-9-cervna-2014.html>.
18. *Právní rádce* [online]. [cit. 2014-2-1]. Dostupný z WWW:< http://pravniradce.ihned.cz/c1-37865090-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>
19. *Svět sítí* [Online]. 2000-2014 [cit. 2014-3-10]. Dostupný z WWW:< http://www.svetsiti.cz/clanek.asp?cid=Penetracni-testy-v-bezpecnostni-analyze-informacniho-systemu-28102007/>.

20. *Systém online* [online]. [cit. 2014-5-18]. Dostupný z WWW: < http://www.systemonline.cz/clanky/informacni-bezpecnost-pojem-ne-znamy.htm>.
21. *Trustica* [Online]. 2002-2009 [cit. 2014-3-15]. Dostupný z WWW< http://www.trustica.cz/penetracni-testy/>.
22. *T-soft* [online]. [cit. 2014-5-21]. Dostupný z WWW: < https://www.tsoft.cz/slovnik-pojmu>.
23. WINDOWS. End support help. *Windows.microsoft.com* [online]. © 2014 [cit. 2014-4-20]. Dostupné z WWW: < http://windows.microsoft.com/cs-cz/windows/end-support-help>.

SEZNAM ZKRATEK

ACTA – obchodní dohoda proti padělkům

EU- Evropská unie

DMZ – Demilitarizovaná zóna

HDD – Hard disk drive neboli pevný disk

ICT – Informační a komunikační technologie

NCKB – Národní centrum kybernetické bezpečnosti

PC – Personal computer neboli „osobní počítač“

OS – Operační systém

SEZNAM TABULEK, GRAFŮ A OBRÁZKŮ

SEZNAM PŘÍLOH

Příloha I.

Dotazník – Počítačová kriminalita

Získaná data budou použita v bakalářské práci o počítačové kriminalitě se zaměřením na hacking. Výstupní data mají ukázat povědomí uživatelů počítačů o tomto poměrně novém fenoménu a rizicích, vázaných s ním. Vyplnění dotazníku je anonymní.

Děkuji za vyplnění

Jakub Kažimír, student Vysoké školy evropských a regionálních studií.

1. Váš věk
    - Do 15 let
    - 16 – 30
    - 31 – 50
    - nad 50

2. Máte vlastní počítač?
    - Ano
    - Ne, sdílím ho s rodinou
    - Chodím do internetové kavárny
    - Půjčuji si od známých

3. Kolik hodin denně trávíte u počítače?
    - Méně než 1
    - 1-2
    - 2-4
    - 4-6
    - 6 a více

4. Slyšeli jste někdy o hackingu?
    - Určitě ano
    - Spíše ano

- Spíše ne
- Určitě ne

5. Myslíte si, že původně hacking sloužil k obohacení?
    - Ano
    - Ne

6. Myslíte si, že děláte s počítačem něco nelegálního?
    - Ano
    - Spíše ano
    - Spíše ne
    - Ne

7. Slyšeli jste o hnutí Anonymous?
    - Ano, vím, co dělají
    - Jen jsem o nich slyšel, ale nevím, co dělají
    - Ne, nikdy

8. Jaký operační systém nejčastěji používáte?
    - Windows
    - GNU/Linux
    - Mac OS X
    - Android
    - Jiný

9. Používáte na počítači placenou antivirovou ochranu?
    - Ano
    - Ne
    - Nevím

10. Aktualizujete pravidelně operační systém a programy v něm nainstalované?
    - Ano, vždy aktualizuji operační systém a software v něm
    - Pouze operační systém

- Jen nainstalovaný software
- Neaktualizuji

11. Otevíráte všechny doručené e-maily?
    - Ano, všechny
    - Většinu doručených e-mailů otevřu
    - Jen ty e-maily, u kterých znám odesílatele
    - Nemám e-mail

12. Používáte na většině svých internetových profilech a účtech stejná hesla a přihlašovací jména?
    - Ano, jména i hesla
    - Pouze jména
    - Pouze hesla
    - U každého profilu/účtu jiné jméno i heslo

13. Využíváte k placení internetové bankovnictví?
    - Ano
    - Ne

14. Přibližně jak často zálohujete svá data, která považujete za důležitá?
    - Jednou týdně
    - Jednou měsíčně
    - Jednou za půl roku
    - Jednou ročně
    - Nezálohují vůbec

Děkuji Vám za vyplnění dotazníku a přeji hezký zbytek dne.