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

BAKALÁŘSKÁ PRÁCE

POČÍTAČOVÁ KRIMINALITA SE ZAMĚŘENÍM NA HACKING

COMPUTER CRIMINALITY WITH THE INTENTION OF HACKING

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

2012

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, metodické vedení práce a nekonečnou trpělivost.

Abstrakt

HOLUB, O. *Počítačová kriminalita se zaměřením na hacking : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2014. 67 s. Vedoucí bakalářské práce : Mgr. Čížek Vladimír, DiS.

Klíčová slova: kybernetická kriminalita, hacking, hacker, malware, právo

Tato práce se zabývá moderní kriminalitou páchanou na poli informačních technologií. V první části práce je komplexně popisována historie kyberkriminality od jejího počátku až do 21. století. V druhé části je rozepsána historie hackerů, jejich definice, typy a nejčastěji používané nástroje. Dále práce popisuje škodlivý software sužující svět informačních technologií. Rozsáhlá část práce je věnována české legislativě a kvalifikaci jednotlivých skutkových podstat, definici kybernetické kriminality, následovně nejnovějším typům protiprávního jednání jako je spaming, cracking, sniffing, atd. Poslední část práce je věnována dotazníkovému šetření.

Abstract

HOLUB, O. *Computer criminality with the intention of hacking : bachelor thesis.* České Budějovice : The College of European and Regional Studies, 2014. 67 p. Supervisor : Mgr. Čížek Vladimír, DiS.

Key words: cyber criminality, hacking, hacker, malware, justice

This text is aimed on modern criminalitz which is obseved in fields of informatio ntechnologies. Fist part contain complexly description of history cybercriminality in begining of 21 century. Second part contains history of hackers, their definition, origin and types of techniques which they use. Next part descripe users unwanted software which impacting our wolrd of IT. Big part is aimed on law and legislative with qualification of every part of law, definition of cybernetic criminality, also new types of behaviour agaist Czech law like spamming, cracking, sniffing etc. Last part contains test qestions of typical users which facing this new type of treath.

Obsah

Úvod

Zločiny byly, jsou a budou. Téma, které zde bude rozebíráno, je kybernetická kriminalita, její minulost, současnost, hacking a zákony platné pro Českou republiku v oblasti informačních a komunikačních technologií. Kybernetická kriminalita jako taková je velmi specifická a úzká část trestné činnosti, která se rozmohla při nakupování osobních počítačů a při jejich připojování k celosvětové síti Internet. Tato situace se dostala na scénu v České Republice zejména v 90. letech 20. století, kdy se po uvolnění režimu do Československa dostávaly novinky ze zahraničí.

S výhodami, které přinášely počítače a připojení k celosvětové síti, ruku v ruce šla negativa této jedinečné technologie, a těmi jsou právě trestné činnosti v oblasti kybernetické kriminality. Nejeden člověk na vlastní kůži již zažil situaci, kdy se stal obětí nějakého škodlivého softwaru, ať to byl nějaký vir, poplašná zpráva či pokus o získání přístupových údajů k různým účtům.

Téma kybernetické kriminality a hackingu je velmi obsáhlé. Když se člověk podívá hlouběji, tak zjistí mnoho zajímavých informací, co se týká nejen vzniku, ale i současného stavu informačních a komunikačních technologií v České republice, ale i v zahraničí.

Rozšíření kybernetické kriminality poukazuje na fakt, že informovanost lidí v České republice je na velmi špatné úrovni a pro mnoho zločinců v této oblasti kriminality je velmi snadné získat citlivé údaje a následně je zužitkovat s maximální efektivitou a často bez následků. I když je legislativa České republiky neustále upravována, tak problém bude vyvstávat nadále, jelikož prioritní by měla být zejména vzdělanost lidí v oblasti informačních a komunikačních technologií, aby bylo méně příležitostí k trestné činnosti.

Po přečtení této bakalářské práce by mělo být snadnější pochopit spojitosti mezi jednotlivými aspekty počítačové kriminality, hackery, crackery a konkrétními hrozbami pro koncové uživatele.

1 Cíl a metodika bakalářské práce

Cílem práce bude obnažení problému počítačové kriminality s důrazem na problematiku hackerství, komplexní vysvětlení pojmů, které se problému týkají, sumarizace dostupných prostředků pro boj s tímto fenoménem, odhalení důvodů vzniku tohoto druhu kriminality a následný rozbor těchto důvodů s návrhy na jejich utlumení.

V bakalářské práci si vymezím následující roviny. V první teoretické části za pomoci dostupné odborné literatury se zaměřím na historii počítačové kriminality a kořeny hackingu a hackerské komunity. Pro lepší pochopení smyslu slova hacker je nutné začít u vzniku prvních počítačů a postupně probrat vývoj této velmi specifické komunity, její etiky a rozdělení. K hackerům patří hlavně činy, se kterými jsou nutně spojené i prostředky, které se pokusím popsat v jedné z kapitol. První část zakončím popisem škodlivého softwaru a možných hrozeb z něho plynoucích.

Ve druhé části se pokusím zanalyzovat dostupné legislativní prostředky České republiky, definovat kybernetickou kriminalitu jako pojem a sjednotit běžné trestné činy, kterých se mohou kyber-zločinci dopustit. Zbylou část věnuji novým typům protiprávního jednání a možnostem ochrany a postihu dle trestního zákoníku.

Třetí a poslední část věnuji výzkumu. Stanovených cílů by mělo být reálné dosáhnout za pomoci vhodně koncipovaného dotazníkového šetření. K oslovení cílové skupiny a získání potřebných informací použiji online prostředky např. vytvoření a šíření dotazníku službou Google disk. Výsledky bych zpracoval, vyhodnotil, a poté bych navrhl obecná možná řešení problému.

2 Vznik a vývoj kybernetické kriminality

Kybernetická kriminalita, co se historického vývoje týká, vychází z informačních technologií. Největší rozmach získala, když využívání osobních počítačů a jejich připojování do sítí, zejména do celosvětové sítě Internet, zaznamenalo masivní nárůst. Vytvoření celosvětové sítě bylo velkým zlomem v životě lidstva, jedná se především o kvalitu přenosu informací. Záporným bodem existence celosvětové sítě je nárůst počtu zločinců v kyberprostoru. V České republice jsme se, kvůli opožděnému zavedení a vývoji nejen informačních technologií, s kybernalitou poprvé setkali až na konci 80. let, když si obyvatelé Československa začali pořizovat první počítače.

Období 50. a 60. let

V Pensylvánii byl roku 1946 vyroben první sálový počítač pojmenovaný ENIAC. V druhé polovině 20. století si počítače značky ENIAC získaly velkou oblibu v mnoha podnicích a na univerzitách. Takové počítače ovšem zabíraly téměř celou místnost a stály desítky tisíc dolarů. Musely být provozovány v místnostech s kontrolovanou teplotou ve speciálních prosklených kukaních. Díky jejich astronomické ceně byly mnohdy nejlépe střeženým místem ve firmě, ke kterému mělo přístup jen pár vyvolených programátorů. Rozhodně se ještě nedalo mluvit o možnostech jejich kriminálního zneužití.[1] Kvůli velmi finančně a časově náročné údržbě se zasahovalo do programů. Tyto zásahy zvané hacky byly uskutečňovány, aby se zefektivnil operační systém a chod aplikací. První generací hackerů se v 60. letech stala skupina studentů Massachusetts Institute of Technology, která se k těmto počítačům dostala na univerzitě.

Období 70. let

Na základě objevu principu využití frekvence 2600 Hz u přepínače telefonních hovorů sedmiletým chlapcem Joem Engressim zjistil John Draper, že plastová píšťalka z populárních cereálií „Captain Crunch“ vydává stejný zvuk. Tato frekvence odblokovala telefonní síť AT&T a zpřístupnila bezplatné dálkové hovory, čímž se

[1] MATĚJKA, M. *Počítačová kriminalita*. Praha : Computer Press, 2002. 20 s.

zrodilo phonephreaking. Tohoto objevu využili budoucí zakladatelé Apple Computers S. Wozniak a S. Jobs k výrobě elektrického zařízení „blue box“, které proces zjednodušilo a zpřístupnilo tak volání zdarma dalším phreakerům. Klíčovou událostí 70. let bylo vynalezení prvního Bulletin Board Systemu, který majitelům PC stanice s telefonním připojením umožňoval připojit se do kyberprostoru. Firma IBM umožnila rozšíření těchto technologií uvedením osobních počítačů s možností online výměny dat na trh. Dříve bylo možné vyměňovat programy a data pouze na univerzitách a v počítačových klubech.

Období 80. let

Na přelomu 70. a 80. let díky IBM systém sítí BBS zaznamenal veliký boom a nechal by se považovat za předchůdce dnešní celosvětové sítě internet. Na server se bylo možné připojit pouze přímou volbou čísla, přičemž práci na něm umožňovalo jednoduché textové rozhraní. Systém BBS byl schopen obsloužit 5 až 10 uživatelů naráz, kapacita virtuální online paměti byla i přes 1GB a rychlost přenosu dat byla maximálně 9600bps, tedy přenos poloviny CD s kapacitou 650MB by trval asi jeden měsíc. Právě v tomto prostředí vznikla neorganizovaná skupina hackerů „Legion of Doom“, která se proslavila publikováním článků v médiích undergroundu. Další rozpuk pirátských skupin byl zaznamenán po uveřejnění novinky pro zápis digitálních dat – CD-ROM. V roce 1985 vznikla společnost Free Software Foundation, díky které se proslavil její zakladatel a také bývalý programátor v Massachusetts Institute of Technology Richard Stallman. Koncem 80. let se objevuje enormní množství hackerských skupin se zaměřením na cracking softwaru a s nimi i první viry, útoky a krádeže skrze počítačové sítě. Asi nejznámějšího počítačového červa z této doby vytvořil Robert Tappan Morris a do sítě ARPANET jej vypustil za účelem zjištění počtu připojených uživatelů. I když Morris vytvořil jednoho z prvních červů omylem, tak byl za způsobené škody stíhán a odsouzen. Do historie se zapsal i útok do sítě počítačů Digital Equipment vedený Kevinem Mitnickem. Za zmínku stojí i loupež 70 milionů z First National Bank v Chicagu pomocí počítače.[2]

[2] PAUKERTOVÁ, V. *Elektronická informační kriminalita*. [online]. Ikaros. 2006, roč. 10, č. 8 [cit. 06.05.2013]. Dostupné z WWW: <http://www.ikaros.cz/node/3554>.

Období 90. let

Charakteristický pro období 90. let je boom v šíření osobních počítačů, stejně jako operačního systému Microsoft Windows. Vývoj softwaru se rychle adaptuje směrem k nejpopulárnějšímu operačnímu systému. Protokol TCP/IP získal finální podobu a budování sítě internet se posouvá do druhé fáze. Počet připojených PC v roce 1992 překročil hranici jednoho miliónu a s tímto číslem narůstá i páchaná kriminální činnost. Připojení ČR k internetu proběhlo v roce 1991 a rozšíření mimo vědecké kruhy, a tedy přístup veřejnosti byl umožněn v roce 1993. Vznikající anonymní FTP servery a narůstající počítačová kriminalita v globálním měřítku dávají podmět pro vznik prvních zákonů na ochranu softwaru. Pachatelé z předchozích let, které představovali počítačový nadšenci, se vyvinuli v profesionály, jejichž motivací bylo vlastní obohacení. Výměnu dat podporoval fenomén P2P sítí.[3]

V USA proběhla rozsáhlá operace „Sundevil“, jejíž podstatou bylo zadržet pachatele trestné činnosti, kteří se zaměřovali na zneužívání telefonních kódů a krádeže kreditních karet. Během akce bylo zabaveno 42 počítačových serverů, na kterých běžely BBS. To však byl jen zlomek z těch, na kterých podle policejních odhadů probíhala nezákonná činnost. Jeden z největších útoků na skupiny BBS se udál v roce 1993. U skupiny BBS zvané "Fear and Loathing in Las Vegas" z Birminghamu v Alabamě provedla místní pobočka FBI a policie razii. Zaměřila se na majitele, místního lékaře zvaného "Doktor", poněvadž si za přístup ke své BBS účtoval přístupové poplatky, čímž si vlastně za kradený software nechával platit.[4] Hackeři „Data Stream“ a „Kuji“ pronikli do stovek počítačových sítí, a to včetně NASA a Korejského jaderného výzkumného institutu. Začínají se objevovat zločiny, které hacking spojují s vlastním obohacováním. Zatímco v případě Orchard Street (1993) se jednalo o minimálně zdatné podvodníky, kteří si vydělávali na živobytí prodejem ukradených přístupových kódů pro telefonní spojení nelegálním imigrantům, v případě Citibank (1994) ruská hackerská skupina vedená Vladimírem Levinem (spekuluje se i o jejím napojení na jednu z odnoží ruské mafie) pronikla do počítačů Citibank a převedla na své účty částku 10 milionů dolarů.[5] Tento zločin odstartoval novou éru

[3] PAUKERTOVÁ, V. *Elektronická informační kriminalita*. [online]. Ikaros. 2006, roč. 10, č. 8 [cit. 06.05.2013]. Dostupné z WWW: <http://www.ikaros.cz/node/3554>.
[4] CASEY, E. *Handbook of computer crime investigation*. San Diego : Academic Press, 2002. 112 s.
[5] MATĚJKA, M. *Počítačová kriminalita*. Praha : Computer Press, 2002. 24-27 s.

počítačové zločinu. Pouze šestiřádkový kód stačil hackerovi Timothy Lloydovi, aby roku 1996 způsobil škodu 10 milionů dolarů společnosti Omega Engineering. Mnohem větší škodu způsobil o pár let později David Smith, když vypustil do světa virus Melissa. Tento virus napáchl škodu 400 milionů dolarů, když napadl a vyřadil z provozu více jak 300 počítačových sítí a stal se globální hrozbou počítačů. Na přelomu století zabojovala na poli autorských práv organizace Recording Industry Association of America (RIAA), výsledkem bylo zablokování hudby spadající pod ochranu autorských práv v P2P systému Napster. Obchodní skupina Business Software Aliance určila míru používání ilegálního softwaru na 80%. Mírné změny v užívání nelegálního softwaru nastaly s šířením osvěty o pirátských kopiích a nárůstem kupní síly firem i běžných uživatelů.[6]

Čechy nezůstaly počítačové kriminality ušetřeny. K nejzávažnějším zločinům docházelo v oblasti bankovních a internetových podvodů a zneužívání osobních dat. Během 90. let bylo v Čechách zveřejněno 10 větších bankovních zločinů, které se týkaly manipulace s bankovními záznamy a až na jeden byly všechny kvalifikovány jako podvody. Vznik hackerských skupin na sebe nenechal dlouho čekat a na české scéně kyberprostoru se objevují skupiny „Binary Division“ a „CzERT“. Obě skupiny se zaměřovali na pozměňování webů, mezi jejich úspěchy řadíme nabourání webu Armády ČR a Ministerstva zdravotnictví. Noviny v té době označily hackera za démona českého internetu. Nelegální užívání software prošlo intenzivním nárůstem, kdy se hovořilo o 80% nelegálně používaného programového vybavení v České republice.[7]

Období let 2000–2013

S rokem 2000 se trend společnosti dle očekávání stále více upíná k počítačům a jejich využívání ve všech možných odvětvích. Roste závislost společnosti na počítačových sítích, stejně jako počet uživatelů internetu a s tím spojená kriminalita. Zvyšuje se počet pirátských skupin a stupeň jejich organizace. Jako příklad takových skupin je možné uvést např. PWA, RAZOR1911, SODOM, HYBRID, DOD, PRESTIGE. Na popularitě získávají praktiky typu pharming,

[6] PAUKERTOVÁ, V. *Elektronická informační kriminalita*. [online]. Ikaros. 2006, roč. 10, č. 8 [cit. 06.05.2013]. Dostupné z WWW: <http://www.ikaros.cz/node/3554>.
[7] SMEJKAL, V., et al. *Právo informačních a telekomunikačních systémů*. Praha : C. H. Beck, 2001. 502-509 s.

phishing, spamming, ransomware, DDoS či šíření malwaru a spyweru. Nelegální kopie označované jako warez jsou masivně šířeny skrze FTP servery, P2P sítě, Torrentz a warez fóra. Útoků nezůstávají ušetřeny ani giganty jako eBay, Amazon, CNN, Dell nebo Yahoo, které v roce 2000 napadl hacker MafiaBoy a vyřadil jejich servery z provozu distribuovanými útoky. Ve stejném roce vyslal do světa Onel De Guzman, filipínský student, červa s názvem ILOVEYOU. Během 10 dnů se červ rozšířil na 50 milionů PC stanic a částka na odstranění škod byla vyčíslena na 15 bilionů dolarů. Přezdívka „Solo“, pod kterou operoval hacker Gary McKinnon, se zapsala do dějin kyberprostoru mezi roky 2001 – 2002 útokem na počítačové sítě US Navy, NASA a US Army. Způsobená škoda byla vyčíslena na 700 000 dolarů a „Solo“ byl zatčen a souzen. K případu červa Blaster se vyjádřila i FBI, Jana Monroe z útvaru pro počítačové zločiny řekla: „Červi jako Blaster mohou způsobit škody za miliony dolarů a pokud napadnou některé důležité systémy, mohou dokonce ohrozit lidské životy. Proto vyšetřování těchto případů věnujeme hodně času i námahy. Počítačové zločiny jsou jednou z hlavních třech priorit FBI, hned po boji proti terorizmu a kontrašpionáži.“[8] Počítačový červ „Conficker“ v roce 2008 vzal útokem operační systémy Microsoft Windows, využívajíc chyby v systému, počítač napadl, ochromil a zpřístupnil útočníkovi. Odborníci se domnívají, že množství napadených počítačů dosahovalo až 15 milionů a napadené počítače sloužili v síti botnet k rozesílání spamu a DDos útokům. I přes vypsanou odměnu 250 000 dolarů nebyl pachatel odhalen.

Metody útočníků drží krok s dobou a stávají se mnohem sofistikovanější a rafinovanější. Vždy jsou o krok napřed před vývojáři ochranných programů a správci sítí.

Na české scéně se objevil případ společnosti Mironet s instalováním nelegálního softwaru, nebo phisingový útok na klienty Citibank. Hnutí Anonymous v roce 2012 napadlo web ODS a získalo osobní údaje tisíců členů, které následně rozeslalo redakcím s připojenou výzvou pro politiky. Výzva se týkala obchodní dohody proti padělatelství ACTA, která v ČR zatím nebyla ratifikována. Útočníci se rychle zabydleli i ve světě chytrých telefonů a našli si cestu, jak zjistit přihlašovací údaje jejich majitele např. při používání internetového bankovnictví. Vývojáři rychle reagovali a vytvořili antivirové programy i pro chytré telefony. V roce 2013 čelilo

[8] HARRIS, S., et al. *Hacking: manuál hackera*. Praha : Grada, 2008. 48 s.

mnoho významných serverů DDos útokům a následným výpadkem byly postiženy servery jako Seznam, O2, T-Mobile, dále pak zpravodajské a bankovní servery.

3 Hacker a hacking

Pojmenování "hacker" a termín "hacking" vznikl zhruba v padesátých letech dvacátého století v komunitě radioamatérů, kde se jím označoval technicky nadaný jedinec, který byl ochotný a schopný hledat nová zapojení a metody ke zlepšení výkonu a dosahu svého vysílače. Termín "hacking" byl převzat z angloamerického žargonu jezdců na koních, kde se jím označovala nenucená vyjížďka bez nějakého zřejmého cíle. Termín byl využíván na MIT ještě v časech před masovým příchodem počítačů, kde slovo "hack" označovalo často velmi jednoduchý, ale efektivní způsob řešení problému. Následovně přešel do studentského slangu a "hackem" se označovalo spáchání nějaké výtržnosti studenty MIT. Pachatel byl, stejně jako v současnosti, označován "hackerem".

S nástupem webových technologií a prvním vydáním Netscape Navigatoru se začínají objevovat první speciální hackerské nástroje, označované jako „easy-to-use“. Hacking se začíná měnit s nárůstem objemu informací dostupných na počítačových sítích a do světa hackerů začínají vstupovat i lidé bez potřebného vzdělání a vědomostí „skript-kiddies“, „lammers“ a „loosers“, zaměřující svoje úsilí do nebezpečných oblastí. Vznikají hackerské weby, kde lze volně stáhnout programy využívající bezpečnostní díry v systémech, jsou instalovány první „back-doors“, tedy utajené vstupy do systému, pomocí kterých je možno systém vzdáleně a skrytě ovládat. Mezi první rozšířené back-doors patří „Back Orifice“ vyvinutý skupinou „Cult of the Death Cow“ pro operační systémy Windows 95 a Windows 98, který se dostal na síť v roce 1998. Avšak již od poloviny devadesátých let minulého století začínají hackeři používat sofistikované nástroje pro předběžnou diagnostiku sítí a automatizaci útoků.[9]

[9] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 47-49 s.

Tab. 1: Přehled významných útoků na přelomu století[10].

Rok	Událost
1983	Počítač s kódovým označením WOPR (součást vojenského systému s označením BURGR) interpretoval hackerské vniknutí jako odpálení nepřátelské nukleární rakety. Následkem toho byla uvedena část armády do stavu vysoké pohotovosti.
1988	Morrisův „Worm“ se vymknul kontrole a napadl na 6000 počítačů. Dostal tak řadu univerzitních a vládních počítačů mimo provoz.
1988	Národní banka v Chicagu se stává obětí počítačového podvodu za 70 milionů dolarů.
1995	Ruští hackeři převedli 10 milionů dolarů z Citibank na svá konta.
1996	Hackeři napadli webové stránky významných amerických institucí – CIA, Air Force a Ministerstva spravedlnosti.
1996	U.S. General Acounting Office zveřejnil zprávu, že došlo k 250 000 útokům na počítače ministerstva obrany, z toho 65% bylo úspěšných.
1999	Skupina hackerů vydírá anglickou vládu – ovládla britský vojenský satelit a za předání kontroly požadují nemalou částku.
2000	Jeden z největších DDoS útoků postihl servery eBay, Yahoo, Amazon a další – ztráty jdou do desítek milionů dolarů.
2000	Jsou ukradeny zdrojové kódy Windows a Microsoft Office.
2001	Byl proveden útok na DNS servery. I když se podařilo zjistit útok téměř okamžitě, odstranění následků trvalo dva dny. Po celou dobu byly nepřístupné stránky firmy Microsoft.
2002	Microsoft přerušuje vývoj systému Windows, osm tisíc programátorů je vyškoleno pro oblast bezpečnosti.

V dnešní době působí některé skupiny hackerů značné problémy. Už to totiž není jen o studentech, kteří projevují své dovednosti na akademické půdě, ale jedná se i o věci celosvětového významu, což zapříčinilo změnu pohledu na hackery. Stále je k takové dovednosti potřeba vysoký stupeň odbornosti, ale už je na hackery pohlíženo jako na lidi, kteří škodí. Za tuto změnu nesou zodpovědnost zejména komerční firmy,

[10] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 49 s.

neboť základní činností hackerů je odhalování nedostatků komerčních projektů, což snižuje dosažený zisk postižených firem.

Na druhou stranu je nutné dodat, že přes veškeré a někdy oprávněné výhrady je činnost hackerů velmi důležitá a bez jejich znalostí bychom se museli potýkat s různými problémy jako špatné zabezpečení počítačů. I když tento způsob vynucování nápravy na zlepšování bezpečnosti sítí a kvality programů není zrovna korektní a někdy i nezákonný, tak by bez něj byly naše počítače mnohem otevřenější a snadno zranitelné. A nevznikl by ani tržní segment bezpečnostních technologií, který je nemalým zdrojem příjmů pro mnohé technologicky vyspělé firmy.

Kriminální podsvětí vyhledává hackery pro svá nová pole působnosti. Nejčastěji jsou hackeři členy skupin organizovaného zločinu působících v oblasti porušování autorských práv. Hackerské schopnosti však kriminální podhoubí využívá i při volbě a přizpůsobení využívaných technologií pro komunikaci, předávání zpráv a sledování aktivit vytipovaných cílů. V tomto okamžiku však hacker přestává být hackerem a stává se jedním z členů kriminálního podsvětí.[11]

3.1 Definice Hackera

V definici hackera hrají obrovskou roli i média a masové sdělovací prostředky. Jejich nevědomost a honba za sledovaností mnohdy hackera představují v nejhorším možném světle, a to jako kriminálníka, který se nabourává do zabezpečených informačních systému, krade hesla, identity a především provádí neautorizované bezhotovostní transakce. Tuto milnou prezentaci média zakotvili do vědomí prostých lidí a úplně zapomněli na pojmenování a hlavně správný termín pro většinu výše zmíněných aktivit, kterým je „cracker“.

Podle hnutí Anonymous je:

- Hacker termín s nejasnou definicí, jenž se v kontextu Anonymous používá k označení lidí, kteří se díky svým technickým znalostem dokáží nabourávat do počítačových sítí (viz také hesla „black hat“

[11] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 49-50 s.

a „white hat“). V širším slova smyslu může označovat také počítačové nadšence nebo programátory, kteří se rádi šťourají v interních systémech a vymýšlejí různé „zlepšováky“ nebo nové systémy.

- Hacktivista složenina slov „hacker“ a „aktivista“ odkazující na někoho, kdo se pomocí elektronických nástrojů snaží šířit politické nebo sociologické poselství. Hacktivisté mohou sahat po různých metodách, přičemž mezi ty méně legální patří DDoS útoky, hanobení webových stránek či zveřejňování utajených dat.[12]

Policejní definice označuje hackera jako osobu, která proniká do chráněných systémů, přičemž jejím cílem je prokázat vlastní kvality bez toho, aby měli zájem na získání nebo zničení informací obsažených v systému. Za nejdůležitější je překonání ochranné bariéry, což je považováno za zábavu, dobrodružství či „sportovní nadšení“, a to bez nároku na veřejné uznání. Hackerům stačí uspokojení z toho, když se o jejich činu hovoří alespoň ve vlastní komunitě. Hacking je jejich koníčkem, u počítače dokážou vysedávat dlouhé hodiny a získaná data nebo programy využívají pouze pro svoji potřebu nebo pro potřebu svých přátel.

Sami hackeři se většinou vidí jako uživatelé velmi dobře vybavení technologickými znalostmi, které zpravidla získali samostudiem. Uspokojení nacházejí v objevování skrytých detailů informačních a telekomunikačních systémů, především v oblasti jejich bezpečnosti a zranitelnosti. Milují praktické, rychlé a sofistikované programování, nikoliv však přehledné a uspořádané. Jsou to lidé s kreativním myšlením, kteří se nedají přimět ke stereotypní práci s počítačem.[13]

3.2 Hackerská komunita a etika

Základem je víra, že sdílení informací je správné a dobré a je etickou povinností hackerů dělit se o své poznatky psaním open-source kódů a usnadňováním přístupu k informacím a počítačovým zdrojům v maximální možné míře. K čemuž se

[12] OLSON, P. *Jsme Anonymous: uvnitř hackerského světa Anonymous, LulzSec a globální internetové vzpoury*. Praha : Práh, 2012. 490-491 s.
[13] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 51 s.

hlásí většina hackerů a někteří z nich navíc rozšiřují o myšlenku volně dostupných informacích, a to i na úkor autorských a patentových práv.

Dalším bodem je přesvědčení, že infiltrace systému pro zábavu a získání zkušeností je eticky v pořádku, pokud nedojde k poškození, zcizení, nebo narušení dat, či porušení jejich utajení. Tento bod je možné rozdělit na dva kroky, které významně dělí komunitu:

1. Infiltrace systému.
2. Zaslání informace o průniku správci systému s návrhem na její zabezpečení.

CERT Coordination Center je organizace založena roku 1988, která sleduje bezpečnost na internetu. Od svého vzniku prošla nemalým vývojem a v dnešní době má významnou roli. Tato organizace v roce 2000 vydala standardy pro nahlašování bezpečnostních chyb, která vypadá takto:

- 45 dnů po ohlášení chyby CERT/CC budou všechny informace o chybě zveřejněny, a to i tehdy, když do té doby výrobce nepřijde se záplatou nebo jiným řešením. Jedinou výjimkou budou výjimečně vážné hrozby nebo scénáře, které by vyžadovaly změnu standardu.
- CERT/CC na chybu okamžitě po jejím oznámení upozorní výrobce, aby mohl co nejrychleji začít pracovat na řešení.
- Společně s popisem problému předá CERT/CC výrobci i jméno osoby, která chybu našla. Výjimkou budou případy, u kterých tato osoba výslovně požádá o anonymitu.
- Během 45denní lhůty bude CERT/CC nálezce chyby průběžně informovat o jejím stavu, ale neprozradí žádné důvěrné informace.

Viceprezident firmy Symantec řekl, že se každý týden objeví zhruba padesát nových bezpečnostních chyb. Schopnosti hackerů neustále rostou - dříve trvalo nalezení praktického útoku na nově objevenou chybu měsíce, dnes stačí dny nebo týdny. Červ Blaster byl vypuštěn měsíc poté, co byla ohlášena jím zneužívaná chyba v systému DCOM. Červovi Witty. A trvalo zneužití příslušné kritické chyby řádově hodiny.[14]

[14] HARRIS, S., et al. *Hacking: manuál hackera*. Praha : Grada, 2008. 60-62 s.

3.3 Dělení hackerů

Prvním rozlišovacím prvkem je motivace hackera. Rozlišujeme, zdali se jedná o čistě technologickou výzvu, nebo se jedná o vidinu zisku z ilegální činnosti. Toto hledisko umožňuje rozlišit dvě základní skupiny:

- Hackery
- Crackery

Toto dělení je poněkud černobílé a lze rozšířit. Poté se jedná o tzv. kloboukové dělení, které zahrnuje i třetí alternativu a dle mého názoru je i výstižnější. Ona třetí varianta poukazuje na prolínání jednotlivých skupin:

1. White hats česky „bílé klobouky“ jsou hackeři, kteří se sice dokáží nabourat do počítačové sítě a ukrást informace, nicméně tyto své znalosti používají jen k tomu, aby firmám a webovým stránkám pomohli lépe se zabezpečit.
2. Black hats v češtině „černé klobouky“, jsou hackeři, kteří využívají znalosti programování ke škodlivým účelům, například hanobení cizích webových stránek nebo kradení databází s osobními údaji uživatelů za účelem prodeje někomu dalšímu. Black hat hackerům se někdy říká i „crackeři“.[15]
3. „Greyhats“ se pohybují na pomezí obou skupin, jak již jejich název „šedé klobouky“ napovídá. 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 přechodným stadiem rodícího se hackera, který nemá ujasněn svůj budoucí úkol.

[15] OLSON, P. *Jsme Anonymous: uvnitř hackerského světa Anonymous, LulzSec a globální internetové vzpoury*. Praha : Práh, 2012. 490-494 s.

Toto dělení je odvozeno od klobouků hlavních hrdinů ve westernech. Obvykle kladný hrdina míval světlý nebo bílý klobouk, zatímco záporný hrdina se vyznačoval tmavou, nejčastěji černou barvou klobouku.[16]

Shrnutím předcházejících poznatků a základních charakteristik je možné vytvořit nejvýznamnější skupiny hackerů:

- Kriminální hackeři, neboli crackeři. Jejich motivací je zisk za každou cenu. Cíle zahrnují většinou servery velkých firem nebo institucí a často se jedná o organizované a izolované skupiny spojené s kriminálním podsvětím. Do této skupiny můžeme zařadit i individua zneužívající hackerské metody pro teroristické aktivity.
- Profesionální hackeři, které je možné rozdělit podle předcházející kloboukové typologie na „Whitehats“, „Greyhats“ a „Black hats“.
- Nespokojení zaměstnanci, kteří tvoří jednu z nejnebezpečnějších skupin hackerských aktivit.
- Ideologičtí hackeři patří k fanaticky zaměřeným skupinám internetových aktivistů, kteří používají internetu k šíření a prosazování svých politických nebo ideologických cílů. Jejich aktivity obvykle souvisí s nějakou významnou událostí ve světové politice nebo ekonomice. Často se označují jako „haktivisté“ a bývají zahrnováni do kyberteroristických skupin.
- Skripťáčci (skript kiddies) je hanlivý termín označující někoho, kdo by se rád považoval za black hat hackera, ale kdo zatím k napadání počítačových sítí používá jen známé a volně dostupné webové nástroje nebo skripty. Skripťáčci si mnohdy prostřednictvím hackování chtějí vydobýt víc respektu mezi kamarády.[17]

[16] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 54-55 s.
[17] OLSON, P. *Jsme Anonymous: uvnitř hackerského světa Anonymous, LulzSec a globální internetové vzpoury*. Praha: Práh, 2012. 493 s.

3.4 Hackerské nástroje

Sebelepší hacker se neobejde bez nástrojů, které jeho úkony ulehčují, zrychlují a do jisté míry i automatizují. Úspěšnost útoku nezávisí pouze na použitých nástrojích, ale stále je zapotřebí plně kvalifikovaného, zkušenostmi a znalostmi nabytého operátora, který dané nástroje umí efektivně využít. V opačném případě se jedná o již zmíněné skripťáčky. Nejčastěji používané nástroje lze rozdělit následovně:

- Hardwarové nástroje, kam patří např. techniky hledání bezpečnostních děr v čipových kartách, nebo již zmíněné blue-boxy, kterými se dodnes označují technická zařízení pro neoprávněný přístup.
- Softwarové neboli programové nástroje, které v hackerské komunitě převažují.
- Sociální inženýrství neboli techniky zneužití lidského elementu.[18]

Vývoj nástrojů

V průběhu let se hackerské nástroje vyvíjely, a to od prostého hádání hesla obsluhy počítače, přes první backdoory využívající slabin síťových protokolů, až po první skutečný síťový útok na dostupnost služby tzv. Denial of Service.

Současně se složitostí přípravy vlastního útoku se objevují nástroje vybavené grafickým rozhraním a zavádí se automatizace některých kroků založená buď na náhodné volbě dalšího kroku, nebo na analýze odezvy cíle útoku.

Při neustále se zvyšující kvalitě útoků a k nim potřebných nástrojů neúměrně klesá úroveň znalostí útočníka pro provedení útoku. A to jen díky pokročilým nástrojům vytvářeným a volně distribuovaným špičkovými hackery, nebo programátorskými skupinami napojenými na kriminální podsvětí.

Program pro využití slabiny v systému se nazývá exploit a jeho vývoj lze popsat několika kroky:

- Pokročilí hackeři zjistí novou slabinu systému.
- Programování a distribuce nástroje pro využití slabiny.

[18] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 59 s.

- Ostatní hackeři využívají nástroj. V tuto chvíli má exploit pouze omezené využití a jak se šíří komunitou tak se zdokonaluje.
- Vznik automatických exploitů. Takový program stačí pouze stáhnout a spustit, což je dokonalý nástroj pro skript-kiddies.
- Vrcholem vývoje je výroba nových exploitů využívajících stejnou slabinu a jejich široké využití. V tuto chvíli nastupují dodavatelé operačních systémů a výrobci antivirových programů, kteří mají za úkol vydat patch, či jiným způsobem slabinu odstranit. Čímž exploit ztrácí smysl a soustředění hackerů se obrací k jiné nově objevené slabině.

Toto je běžný a neustále se opakující cyklus hrozby a protiopatření, který doprovází celou bezpečnostní problematiku v informatice. A protože útočník je vždy o krok před správcem systému a pravděpodobně se nikdy nepodaří, aby tomu bylo naopak, je tento životní cyklus základním rytmem boje s kybernetickými útoky.

Prolamovače hesel

Jeden z nejstarších hackerských nástrojů používaných k prolomení ochrany statický heslem. Základními druhy útoků jsou:

- "Dictionary attack", které využívají vlastní databázi k nalezení správného hesla.
- "Brute force attack", které generují všechny kombinace potřebné délky z vybraných znaků a porovnávají je s hledaným heslem.

Na internetu je nespočet volně dostupných prolamovačů, které se liší kvalitou obsahu slovníku, grafickým rozhraním, nastavitelností parametrů prolamování a hlavně rychlostí prověřování hesel, která se u kvalitních programů může vyšplhat až k milionu hesel za jedinou sekundu. Rychlost prolamování nejvýznamněji ovlivňuji následující faktory:

- Kapacita hardwaru.
- Typ souboru.
- Lokace dat nebo souboru (LAN, ONLINE, nebo HDD).
- Struktura zakódovaného souboru.

Tab. 2 Odhady doby práce prolamovače podle typu hesla[19].

Kombinace použitá pro heslo	Odhad doby práce prolamovače
4 velká a malá písmena a číslice v libovolné kombinaci	Několik sekund
5 velkých a malých písmen a číslice v libovolné kombinaci	cca 15 minut
8 velkých nebo malých písmen	cca 58 hodin
8 velkých a malých písmen v libovolné kombinaci	cca 21 měsíců
8 velkých a malých písmen a číslice v libovolné kombinaci	cca 7 let
10 velkých a malých písmen a číslice v libovolné kombinaci	cca 26984 let

Jak lze z tabulky vyčíst, je bezpečnější používat delší heslo obsahující více druhů znaků.

Backdoors

Je oblíbený hackerský nástroj tzv. zadní vrátka, které umožňují vzdálené ovládání počítače po instalaci škodlivého kódu. Kompromitované PC stanice slouží hackrům k podnikání útoků a též jako ochrana před odhalením skutečného útočníka. Kvalita hackera se může měřit i počtem kompromitovaných strojů, které má k dispozici.

Kvalitní backdoor lze jen těžko zjistit, zvláště pokud není často používán, a hackerovi poskytuje úplnou kontrolu nad kompromitovaným strojem. Komunikace mezi nástrojem uvnitř kompromitovaného počítače a hackerem se uskutečňuje pomocí nástrojem spuštěné služby na portu s vysokým číslem např. 12345, nebo je maskován jako standardní služba např. http (webový přístup). Moderní backdoors mají zdokonalenou komunikaci a využívají většinou protokolů některých interaktivních nástrojů komunikace jako je IRC, ICQ nebo MSN messenger.[20]

Příkladem nástroje používaného pro backdoor od roku 1998 je Back Orifice, který ve své původní verzi umožňoval úplnou kontrolu nad operačními systémy Windows 95 a 98. Pozdější upravené verze byly schopné kompromitovat i Windows NT a 2000. Schopnost tohoto nástroje maskovat se v tabulce běžících procesů jako „explorer.exe“, ho činila obtížně detekovatelným.

---

[19] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 63 s.

[20] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 63 s.

Skenery

Zjišťují stav portů a na nich běžících služeb, čímž útočníkovi předají základní informace o cílovém počítači. Zachycení takového skenu může předpovídat přípravy na útok ze strany hackera. Princip skenu se dá popsat takto:

1. Odeslání nějaké sondy, např. paket SYN (firstsent „synchonize“ packet).
2. Poznačení toho, co a kam jsem poslal.
3. Trpělivé čekání na to, až (a jestli) se něco vrátí, a naděje, že se z této návratové informace něco dozvím o svém cíli.

Rychlost skenování není nějak závratná. Neustálý koloběh odesílání paketů a čekání na odpovědi celý proces zdržuje. Proto v roce 2002 zveřejnil Dan Kaminsky, známý též jako Effugas, svůj bezstavový TCP port skener „scanrand“ a další jeho součásti. Jeho přednost spočívala v rychlosti skenování. Nalezení osmi tisíc webových serverů na síti třídy B, což je přes 65 tisíc strojů, mu trvalo pouhé čtyři sekundy. Takovéto rychlosti bylo možné dosáhnout jistým porušení principu skenování. Jednoduše řečeno, scanrand se po spuštění skenu rozdělí na dva samostatné procesy – odesílání a přijímání packetů, čímž ušetří čas při čekání na odpověď a nemusí držet v paměti zbytečné množství informací.

Techniky skenů:

- TCP spojení - třícestný protokol pro plné navázaní spojení
- TCP SYN sken - zpola navázané spojení
- TCP FIN sken - pro Unixové servery
- TCP XmassTree sken - zjišťování uzavřených portů kombinací packetů FIN, URG a PUSH
- TCP Null sken - zjišťování uzavřených portů paketem s nulovými návěštími
- TCP ACK sken - k mapování filtrů firewallu
- TCP Windows sken - využívá anomálie při oznamování velikosti TCP okna
- TCP RPC sken - na detekci otevřených RPC portů u systému Unix
- UDP sken - pomalý a méně přesný sken pro zjišťování otevřených portů[21]

[21] SCAMBRAY, J. *Hacking bez tajemství: Windows 9x, Me, NT a 2000, NetWare, Unix*. Praha : Computer Press, 2001. 38-39 s.

Debuggery

Nástroje určené pro analýzu softwaru a používané jak k ladění nového programu, tak i při hledání chyby využitelné k výrobě exploitu. Jsou neodmyslitelnou pomůckou každého hackera. Slouží jim jako kontrola správné funkce exploitu, tedy ověřuje správnou funkci kódu. Výhodou debuggeru je poskytnutí přesného snímku stavu programu při vzniku výjimky. Práce s tímto nástrojem vyžaduje hodně zásahů operátora a tím se nehodí k automatizovanému testování.

Sniffery

Program odvozený od anglického slova „sniff", což v českém jazyce znamená „čmuchat", slouží k odposlouchávání síťového provozu. Nejedná se přímo o nástroj útoku, spíše o prostředek ke shromažďování informací potřebných pro přípravu útoku. Pro dosažení chtěných informací je důležité správné umístění snifferu v síti.

Práce snifferu je jednoduchá, přepne síťové rozhraní do tzv. promiskuitního módu, a tak přijímá všechny pakety, které se na síti pohybují, bez jakékoliv filtrace. Tyto pakety jsou zaznamenávány a dále analyzovány. Součástí analýzy je vydělení datové části s obsahem přenášené zprávy. Tak je možno odposlechnout komunikaci v síti, zachytit otevřeně přenášená hesla, nebo jiné citlivé údaje.

Jednodušší sniffery jsou schopny vypisovat zachycené údaje pouze v hexadecimální, nebo znakové formě. Speciálně zaměřené, nebo profesionální sniffery už jsou schopny složit celý průběh relace a zobrazit ji v běžné formě, např. emailovou komunikaci.[22]

Rootkity

Byly odvozeny od účtu pro správu unixových operačních systémů, který se jmenuje „root". To ovšem neznamená, že rootkit lze použít pouze pro operační systém Unix. Od roku 1999, kdy Greg Hoglund vytvořil první známý rootkit určený pro Windows NT, jsou tyto nástroje široce používány a žádný operační systém před nimi není v bezpečí.

Rootkit se skládá ze dvou částí, a to přenašeče a nákladu. Přenašeč zneužije nějaké bezpečnostní chyby nebo nepozornosti uživatele a spustí náklad. Ten má

[22] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 64-65 s.

u většiny moderních rootkitů obvykle podobu jaderného modulu, takže se přidá do jádra systému a začne s úklidem stop.

Krátký popis funkcí rootkitu:

1. Úprava jádra je prvním a základním krokem. Obvykle začíná přesměrováním API nebo načtením jaderného modulu s příponou „sys“.
2. Skrývání souborů a adresářů. A to pomocí datových proudů ADS (Alternate Data Streams), kompresí, šifrováním, nebo také označováním souborů jako vadné bloky disku. Budoucnost takovéto hry na schovávanou je možnost využít k maskování jinou dostupnou paměť pro zapisování, např. grafického procesoru.
3. Skrývání procesů. Bez spuštění procesu se rootkit neobejde, a tak spuštěný proces většina rootkitů odpojí ze seznamu aktivních procesů, čímž proces z většiny obyčejných API úspěšně zmizí.
4. Skrývání portů. Rootkity obvykle komunikují po síti, a tak potřebují utajit i otevřené síťové TCP a UDP porty.
5. Skrývání klíčů registru. Díky velikosti a nepřehlednosti registru je poměrně snadné v něm cokoliv schovat. Stačí to jen umístit do správné větve a šikovně pojmenovat.
6. Skrývání uživatelů a skupin. Jakmile se stane rootkit součástí jádra, tak může libovolně nastavit práva jednotlivých uživatelů i skupin tak, aby pro ostatní byl nedostupný.
7. Odposlech klávesnice je řešený speciálním programem vloženým do přihlašovacího procesu Windows, nebo malým programem, který události z klávesnice zachytí už blízko hardwaru.
8. Backdoor. Zadní vrátka slouží k opětovné infikaci systému v případě částečného odhalení.

Většina rootkitů používá kombinaci několika technik, aby se v případě částečného odhalení nebo selhání v počítači udržela. Jako příklad pravděpodobně nejoblíbenějšího rootkitu je možné uvést Hacker Defender zkráceně hxdef.

Operační systém kompromitovaný rootkitem se stává nedůvěryhodným a doporučený postup je zálohovat čistá data a systém nainstalovat znovu. Protože

při hlubší infiltraci rootkitu v systému už nepomohu ani antivirové programy nebo systémy detekce narušení.[23]

Trojské koně

Trojské koně patří mezi nejoblíbenější hackerský nástroj současnosti. Jedná se o software, který se vydává za něco jiného, než ve skutečnosti je, např. může být součástí nové hry, či zajímavé utility. Používají se na nejrůznější účely, od pouhého monitorování činnosti cílového počítače a instalace backdooru, až po zneužití pro rozesílání spamu, či DDoS útokům. Jednou z funkcí je i odesílání citlivých údajů na určená sběrná místa. Existují velice povedené nástroje, které spojí kód trojského koně s nosným programem a přibalí k němu instrukce pro rozbalování.[24]

Denial of Service

Nástroje potlačení služby, zkráceně DoS, jsou používány k odstřižení cílového stroje nebo celého systému od vnější sítě tím, že je cílová síťová i výpočetní kapacita počítače zahlcena. V roce 2000 tento nástroj zaznamenal inovaci ve formě Distributed Denial of Service. Distribuovaný se mu říká pro jeho obrovský výpočetní potenciál, účastní se ho totiž více počítačů. V případě útoku na servery Yahoo!, eBay. CNN a několik dalších internetových firem se DDoS útoku účastnilo tisíce počítačů. Nedílnou součástí jsou i tzv. zombie sítě, neboli kompromitované počítače ovládané hackery, které podle některých odhadů čítají až 140 tisíc strojů. Tolik výpočetního a síťového výkonu je samozřejmě velice žádaný artikl, který rádi využijí spameři, vyděrači a řada dalších lidí. A tím se z jednoduchých DoS útoků stala noční můra pro internetové firmy.

Starší typy DoS si vystačily s jedním nebo několika málo pakety a fungují na těchto principech:

- Příliš velké pakety. V minulosti stačilo pouhých 65 kilobajtů k tomu, aby byl operační systém vyřazen z provozu.
- Překrývající se rozdělené pakety byly kamenem úrazu pro některé v minulosti používané operační systémy, které na ně reagovaly pádem, nebo vyčerpáním systémových prostředků.

---

23 SCAMBRAY, J. *Hacking bez tajemství: Windows 2000*. Praha : Computer Press, 2003. 178 s.

24 JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 67 s.

- Zaplavení smyčky. Spojení služeb chargen a echo vytvoří nekonečnou smyčku, ve které se některé Unixové systémy spolehlivě utopily. Novější variace využívají TCP/IP pakety se zdrojovou i cílovou adresou nastavenou na adresu oběti.
- Nukery zneužívaly chybu ve Windows, díky které se operační systém složil po přijetí urgentního paketu.
- Drobení paketů umožňuje protokol TCP/IP. Jejich opětovné sestavení pak samozřejmě nějakou dobu trvá, takže je vhodné rozdělit paket na co největší možný počet částí. Systém oběti pak selhává na nedostatek výpočetní kapacity.
- NetBIOS/SMB jsou licencované síťové protokoly Microsoftu, které byly využívány k odstřihnutí počítače s operačním systémem Windows od místní sítě.[25]

Všechny zmíněné možnosti lze vzájemně kombinovat a za pomoci skriptů použít i naráz. Útěchou pro správce sítí je, že většina z výše zmíněných chyb byla již opravena, a tak se mohou soustředit na hrozby nové. Těmi jsou DDoS útoky a pro jejich uskutečnění je zapotřebí nástroje zvaný „bot“ (např. populární TribeFlood Network). Automatizovaný program vzniklý z vypůjčených IRC skriptů a určený pro vzdálené ovládání jednotlivých počítačů, které jsou součástí zombie sítě, nebo také botnetu. Tyto nástroje pracují na principech odesílání SYN, UDP, ICMP a Smurf paketů. Cílem takového distribuovaného útoku pak může být infrastruktura oběti, nebo aplikační logika.[26]

3.5 Malware a další

Malware je podle Ministerstva vnitra ČR souhrnný pojem pro jakýkoli software, který při svém spuštění zahájí činnost ke škodě systému, ve kterém se nachází. Jeho vnější projevy mohou být časovány, nebo reagovat na konkrétní naprogramovanou spouštěcí událost, např. na okamžik, kdy oprávněný uživatel otevře

[25] MCCLURE, S., SCAMBRAY, J., KURTZ, G. *Hacking bez záhad*. 5. dopl. vyd. Praha : Grada, 2007. 389 s.
[26] SCAMBRAY, J. *Hacking bez tajemství: webové aplikace*. Brno : Computer Press, 2003. 293 s.

zprávu v rámci elektronické pošty. V následující části bude uveden stručný přehled škodlivého softwaru.[27]

Infoware

Může být specifikován jako aplikace pro informatickou podporu klasických bojových akcí, respektive jako soubor aktivit, které slouží k ochraně, vytěžení, poškození, potlačení, nebo zničení informací nebo informačních zdrojů, s cílem dosáhnout významné výhody v boji nebo vítězství nad konkrétním protivníkem. Pojem infoware nelze zaměňovat s termínem infowar, tj. informační válka.

Spyware

Jsou to programy, skrytě monitorující chování oprávněného uživatele počítače nebo systému. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, respektive distribuoval. Takové programy jsou často na cílový počítač nainstalovány spolu s jiným programem (utilita, počítačová hra), s jehož funkcí však nesouvisí.

Adware (advertising supported software)

Je software, jehož cílem je předání reklamního sdělení, a to i proti vůli uživatele systému.

Vir

Podmnožina malware. Parazitující soubor, který se připojí k určitým programům nebo systémovým oblastem, které pozmění. Může se nekontrolovatelně rozšiřovat, nebo po svém spuštění zahájit destrukční proceduru (poškození, změnu či zničení dat, degradaci funkce operačního systému, stahování dalšího malware atd.). Existují viry, které mohou zároveň plnit funkci trojského koně a vytvářet backdoor do napadeného systému. Počátek šíření počítačového viru může být distribuován v prostoru ohnisek, vytvořených na již kompromitovaných (zavirovaných) počítačích, což nesmírně urychluje celý proces šíření infekce.[28]

Dělení počítačových virů:

A. Podle umístění do paměti

---

[27] *Základní definice, vztahující se k tématu kybernetické bezpečnosti*. [online]. Praha, 2009, [cit. 2013-08-03]. Dostupné z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>.

[28] *Základní definice, vztahující se k tématu kybernetické bezpečnosti*. [online]. Praha, 2009, [cit. 2013-08-03]. Dostupné z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>.

1. Rezidentní - po skončení své činnosti zůstává v paměti
2. Nerezidentní - po skončení své činnosti nezůstává v paměti

B. Podle cíle infekce
   1. Spustitelné soubory s příponami COM, EXE, BIN, SYS, OVL
   2. Bootový virus - nahradí boot sektor disku a tabulku rozdělení disku
   3. Klastrové viry - upravují FAT či NTFS tabulku

C. Podle chování virů
   1. Worm (Červ) - rozmnožující se vir
   2. Stealth vir - maskující se vir
   3. Polymorfní vir - mutující viry
   4. Trojan Horse (Trojský kůň) - destruktivní program[29]

Červ

Autonomní program, schopný vytvářet své kopie, které rozesílá do dalších počítačových systémů (sítí), kde vyvíjí další činnost, pro kterou byl naprogramován. Často slouží ke hledání bezpečnostních skulin v systémech nebo v poštovních programech.

Přesměrovávače (re-dial, „pharming crimeware“)

Podmnožina malware. Programy, jejichž úkolem je přesměrovat uživatele na určité stránky namísto těch, které původně hodlal navštívit. Na takových stránkách dochází k instalaci dalšího crimeware (viru), nebo touto cestou dojde ke značnému zvýšení poplatku za připojení k Internetu (prostřednictvím telefonních linek se zvýšeným tarifem).[30]

[29] POŽÁR, J. *Informační bezpečnost*. Plzeň: Aleš Čeněk s.r.o., 2005, 216-218 s.

[30] *Základní definice, vztahující se k tématu kybernetické bezpečnosti.* [online]. Praha, 2009, [cit. 2013-08-03]. Dostupné z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>.

4 Legislativa

Současný stav české i evropské legislativy v oblasti informačních a komunikačních technologií není důkladně připraven na moderní nástroje kriminálního podsvětí. Jednotlivé trhliny jsou "záplatovány" případ od případu a celkové koncepční pojetí této oblasti se teprve rodí. O moc lépe na tom není ani legislativa zámořská, která však díky své odlišné právní metodice, spočívající na právních precedentech a dodatcích ústavy, má pro jednotlivé incidenty již své vzory a nekompromisní trestní taxy.

Na přelomu století vedla potřeba harmonizovat právní úpravy na mezinárodní úrovni k vytvoření Úmluvy o počítačové kriminalitě. Jedinečnost této Úmluvy se projevuje v její komplexnosti a v okruhu signatářů. Úmluva se zabývá nejen definicemi některých trestných činů v kyberprostoru, ale obsahuje též závazky k přijetí procesních opatření nezbytných k zajištění důkazů, odhalení a potrestání pachatelů, jakož i závazky v oblasti mezinárodní spolupráce. Ke dni 10. července 2008 Úmluvu podepsalo 45 států, z nichž ji však ratifikovalo jen 23.[31] V ČR zatím úmluva nebyla ratifikována.

4.1 Legislativa v ČR

Nejčastěji uplatňované zákony z oblastí informatiky a telekomunikací jsou :

- Občanský zákoník - č. 40/1964 Sb.[32] je zásadní předpis pro označení vlastnického práva a zároveň definuje právnickou a fyzickou osobu.
- Obchodní zákoník - č. 513/1991 Sb. [33] upravuje smluvní vztahy, postavení podnikatelů, obchodní závazkové vztahy a podobné vztahy.
- Zákon o elektronických komunikacích č. 127/2005 Sb. [34] zahrnuje dodržování telekomunikačního tajemství a zabývá se nezákonným chováním v prostředí počítačové sítě.

---

31 GŘIVNA, T., POLČÁK, R., ed. *Kyberkriminalita a právo*. Praha : Auditorium, 2008. 162 s.

32 AION CS. *Předpis č. 40/1964 Sb.: Občanský zákoník.* [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: <http://www.zakonyprolidi.cz/cs/1964-40>.

33 AION CS. *Předpis č. 513/1991 Sb.: Obchodní zákoník.* [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: <http://www.zakonyprolidi.cz/cs/1991-513>.

- Autorský zákon č. 121/2000 Sb. [35] určuje, že program se stává duševním vlastnictvím a je chráněn jako např. literární dílo.
- Zákon o ochraně osobních údajů č. 101/2000 Sb.[36]
- Trestní zákon č. 40/2009 Sb.[37] ve své poslední úpravě a s ním související předpisy by měly sloužit jako represivní nástroj v okamžiku prokázaného porušení některého zákonného předpisu, které spadá do sféry trestní odpovědnosti. Bohužel, v těchto případech je mnohdy výklad zákona takový, že některé typické kriminální delikty v počítačovém prostředí se jenom velmi obtížně začleňují do stávající osnovy zákona. Rovněž dokazovací procedura je v těchto případech většinou složitá, neboť procesní dokazování je stavěno na klasických důkazních metodách.

4.2 Definice kybernetické kriminality

Kybernetická kriminalita, označovaná v anglické literatuře mnohdy jako "IT crime" nebo "cybercrime", znamená jakýkoliv čin směřující k narušení nebo zneužití počítače nebo počítačového systému a informací v něm obsažených. Oficiální definicí počítačové kriminality existuje celá řada, avšak většina z nich vychází z podstaty uvedené výše. Podle materiálu OSN, který se zabývá počítačovou kriminalitou, jsou jejím obsahem *"Tradiční zločinné aktivity jako krádež, podvod nebo padělání, tedy činy trestné ve většině zemí na světě. Počítač rovněž tvoří prostředí pro nové činy spočívající ve zneužití počítačů, které jsou nebo by měly být ve své podstatě trestné."* Ve stejném materiálu se OSN snaží odlišit dva základní případy - náhodné a neúmyslné použití počítače, které vede ke vzniku škody, a úmyslné použití počítače jako nástroje nebo předmětu kriminálního deliktu.

---

34 AION CS. *Předpis č. 127/2005 Sb.: Zákon o elektronických komunikacích.* [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: <http://www.zakonyprolidi.cz/cs/2005-127>.

35 AION CS. *Předpis č. 121/2000 Sb.: Autorský zákon.* [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: <http:// http://www.zakonyprolidi.cz/cs/2000-121 >.

36 AION CS. *Předpis č. 101/2000 Sb.: Zákon o ochraně osobních údajů.* [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: < http://www.zakonyprolidi.cz/cs/2000-101>.

37 AION CS. *Předpis č. 40/2009 Sb.: Zákon trestní zákoník.* [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: < http://www.zakonyprolidi.cz/cs/2009-40>.

4.2.1 Klasifikace podle dopadu konkrétního skutku[38]

Na základě prostudované dostupné literatury jsem se ztotožnil s klasifikací podle napadeného chráněného zájmu. Můžeme pak rozeznat:

a. Trestný čin proti osobě, kam patří útok proti pověsti, pomluva, vydírání, obtěžování, krádež identity, nenáležité nakládání s osobními údaji, atd. Příkladem může být situace, kdy je digitální prostředek využit pro úpravu audiovizuálních projevů. Výsledek může být situace, kdy je projev řečníka upraven tak, že zvuk i obraz plně korespondují, i když se původní projev nesl ve zcela jiném duchu. V tomto konkrétním případě se jedná o důležitý prostředek psychologického útoku, podkopávající důvěru v konkrétního mluvčího.
b. Další možnosti, kterými je např. klamavá reklama, nebo naopak šíření nepravdivých informací poškozujících protivníka mohou využít jak veřejně přístupné mediálními prostředky, tak i přímo protivníkův informační systém, který byl jinými prostředky předem kompromitován.
c. Trestný čin proti veřejnému zájmu, veřejnému pořádku nebo mravnosti, kam můžeme zahrnout pobuřování, šíření poplašné zprávy, kybernetický terorismus, politicky motivovaná špionáž, šíření nelegální pornografie, šíření nenávisti, schvalování zločinu a nabádání k němu nebo propagaci toxikomanie, atd.
d. Trestný čin proti vlastnictví, kde můžeme rozeznat případy:
    1. Kdy je přímým dopadem činu další obohacení se na úkor poškozeného (odčerpávání majetku z účtu nebo využívání služby na účet poškozeného). Škoda může být i značně vysoká, pokud je platba vázána na objem dat nebo čas.
    2. Kdy je následkem činu "úspora" nákladů útočníka, která by byla ziskem postiženého (investice do koupě software, audiovizuálních nahrávek, atd.), sem patří především porušování autorských práv, defraudace dat, atd.
    3. Kdy zisk útočníka a ztráta poškozeného spočívá v dalším nezákonném šíření neoprávněně získaných dat: software, audiovizuálních nahrávek, atd., ať již za úplatu nebo bez ní; do této oblasti spadá i průmyslová

[38] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 92-93 s.

špionáž uskutečněná prostřednictvím informatických prostředků (krádež výsledků výzkumu, patentů, marketingových strategií apod.).

4. Kdy je škoda napadeného subjektu odvozena od vratného či nevratného zničení, poškození či pozměnění jeho dat (sabotáž, vandalizmus). Informace tak nemůže být spolehlivě použita pro účel, ke kterému je určena. Často jsou přitom změněna pouze některá data, a to v obtížně rozlišitelných detailech, útok se tedy projeví až s určitým zpožděním.
5. Kdy je škoda napadeného subjektu založena na tom, že jeho služba není dostupná (Denial of Service resp. Denial of Access). Útok zabrání autorizovanému přístupu ke zdrojům, nebo způsobí zpoždění časově kritických operací. Tento typ útoku je používán např. pro potlačení konkurenčních serverů a provedení vyžaduje široce koordinovanou akci většího počtu počítačů.
6. Kdy je škoda založena na zneužití informace, která byla neoprávněně získána z informačních a komunikačních sítí v reálném světě (např. informace o trase přepravy velkých finančních prostředků).

Toto členění je více obecné a přehledné. Je potřeba počítat s prolínáním jednotlivých skupin.

4.3 Nové typy protiprávního jednání

S nástupem nových technologií se objevují nové a obtížněji zařaditelné druhy trestné činnosti. Pro příklad zde uvedu ty nejvýznamnější.

Hacking

Označení hackingu v původním slova smyslu za trestný čin není jednoduché. Problém nastává ve chvíli, kdy se určuje výše škody, nebo se zjišťuje, zda si je správce systému vědom průniku, ztráty, nebo poškození dat. Odměnou a zároveň motivací útočníka je uznání hackerské komunity a osobní úspěch na poli informačních technologií.

Hacking je možné definovat jako úmyslné vniknutí do zabezpečeného počítačového systému prolomením jeho ochrany jinou, než běžnou cestou. Právo v této oblasti zatím není příliš upravené, a proto je jeho uplatňování obtížné. Bylo by

možno použít ustanovení §228 TZ, který hovoří o poškození nebo zneužití záznamu na nosiči informací. Zdá se, že pokud nedojde ke škodě, nikomu není způsobena újma, nebo hacker či třetí osoba nemá z průniku do systému neoprávněný prospěch, pak podstata tohoto trestného činu je nenaplněna.

Kybernetické výpalné

Je trestná činnost založená na hrozbě a následném vydírání oběti za účelem obohacení se. Díky internetu a webovým prezentacím získává tento delikt nový rozměr. V tomto případě vyděrač využívá neznalost oběti, nedostatečné zabezpečení systému a dat, nebo jiné informace o oběti, které by mohl prezentovat v prostředí internetu. Strach z hrozby napadení např. internetového obchodu je oprávněný, a proto by majitel webu, jehož podnikatelská činnost by mohla být významně ovlivněna nedostupností služby, by měl investovat do analýzy rizik a možností zabezpečení.

Pokud jde o právní hodnocení trestného činu, připadá zde možnost uplatnění §175 TZ, tedy stejného jako při klasickém trestném činu vydírání, s možností rozšíření o §228 TZ.

Šíření materiálů se závadným obsahem

Díky novým možnostem šíření informací získávají pozornost i běžné trestné činy jako šíření materiálů s extremistickým obsahem, dětskou pornografií a podobnými obsahy. Novinka tví tedy ve vykonávání činnosti za pomoci nového média. Odpovědnost za obsah materiálu přebírá jeho poskytovatel. V trestním řízení lze uplatnit §191 TZ, §192 TZ nebo §355 TZ a horní sazba odnětí svobody je až na 3 roky.[39]

Zneužití internetových stránek

Pomluva, jako jeden z nejstarších trestných činů dostal díky novému masovému sdělovacímu prostředku další rozměr. V našem trestním zákoně označená §206. Vyhodnocení pomluvy je ztíženo vysokým množstvím podnětů, což je způsobeno snadný zneužitím internetu prakticky kýmkoliv. Pomluva prezentovaná na internetu je hodnocena podle již zmíněného §184 TZ, a protože čin je spáchán

[39] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 102-103 s.

pomocí "sdělovacího prostředku", jedná se tedy o kvalifikovanou skutkovou podstatu, je nutno počítat s dvouletou horní hranicí trestní sazby.[40]

Příkladem trestného činu pomluvy může být např. zveřejnění pohoršujících fotografií spolu s telefonním číslem na webu erotické seznamky, vytvořit web za účel veřejného prezentování názorů autora o oběti, s možným doplněním smyšlených komentářů třetích stran. Mnoho aktéru se domnívá, že pobyt na internetu je anonymní, nicméně opak je pravdou a tím je odhalení neopatrného autora velice reálné.

Spamming

Pod pojmem spamming se rozumí rozesílání nevyžádané elektronické pošty obvykle s reklamním obsahem. Tento typ nepříjemného přímého marketingu, který obtěžuje zejména tam, kde doba připojení nebo objem přenesených dat je účtováno, je starý jako elektronická pošta sama. Spammeři získávají elektronické adresy nejrůznějšími způsoby ze zdrojů, jako jsou chaty, IRC, ICQ, registrační stránky pro služby "zdarma", z webových stránek, elektronické inzerce a mnoha dalších.

Stejně jako tomu je u škodlivého softwaru, tak i spameři jsou o krok napřed před vývojáři ochrany proti spamu, a proto žádné řešení ochrany není trvalé. Podle testu poskytovatelů emailových služeb zdarma z roku 2008 má nejhorší integrovanou ochranu proti spamu tiscali.cz, volny.cz a seznam.cz. Opakem je tomu u Gmailu, který se považuje za špičku na poli freemailů. Existuje i mnoho programů, které chrání proti spamu dodatečně. Příkladem externí ochrany proti spamu jsou placené i free programy jako Spamhilator, SPAMfighter, MailWasher a SpamPal. Podle posledních výzkumů lze očekávat, že objem spamu v elektronické poště překročí v krátké době devadesátiprocentní hranici.

Problematiky spamu se dotýkají zákony č. 127/2005 Sb. O elektronických komunikacích[41], č. 480/2004 Sb. O některých službách informační společnosti[42] a č.

---

40 JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 102-103 s.

41 AION CS. *Předpis č. 127/2005 Sb.: Zákon o elektronických komunikacích.* [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: <http://www.zakonyprolidi.cz/cs/2005-127>.

42 ČESKO. *Zákon č. 480/2004 Sb.: Zákon o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)*. [online]. MVČR, © 2014, [cit 2014-01-09]. Dostupné z WWW: < http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=480/2004%20&typeLaw=zakon&what=Cislo_zakona_smlouvy>.

40/2009 Sb. Trestní zákoník.[43] Výše zmíněné zákony popisují problematiku od získávání emailových adres, přes poskytovatele připojení, až po rozesílání obchodních sdělení potažmo spamu. Při prokázání škody při odstraňování spamu a odhalení viníka lze uložit pokutu až do výše dvou milionů Kč.

Warez

Nebo také nelegální nakládání s díly podléhajícím autorským zákonům. Do této kategorie spadá hudba, filmy, programy, počítačové hry, aplikace a cracky. Pro výměnu těchto dat slouží převážně P2P sítě, webová fóra a uložiště, FTP servery a Bittorrenty.

V ČR všeobecně platí, že je legální stahovat hudbu a filmy pro osobní potřebu. Software je možné legálně stahovat, ovšem jeho používání je omezeno. Šíření takovýchto dat je nelegální a jsou jím porušována autorská práva, která jsou chráněna trestním zákonem. Trestem za jejich porušení může být odnětí věci, peněžitý trest, nebo i odnětí svobody až na 5 let.

Počítačoví piráti pracují v organizovaných skupinách jako elitní obchodní jednotky, které se dělí na:

- Dodavatele - všemi dostupnými způsoby shání placený software v nejnovější verzi a bez virů před oficiálním vydáním
- Crackery - obcházejí a nabourávají protipirátské ochrany softwaru
- Kurýry - nahrávají nový warez na FTP servery a plní požadavky uživatelů serveru
- Baliče - rozdělují warez do více souborů pro snažší upload a následný download
- Koordinátory - dohlížejí na průběh procesu a dodržení podmínek pro vydání[44]

[43] AION CS. *Předpis č. 40/2009 Sb.: Zákon trestní zákoník.* [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: < http://www.zakonyprolidi.cz/cs/2009-40>.
[44] CRAIG, P., HONICK, R. *Softwarové pirátství bez záhad*. Přeložil Tomáš HLAVÁČ. Praha : Grada, 2008. 35-105 s.

Cracking

Je výraz pro prolamování hesel, nabourávání se do systémů a obcházení ochranných prvků. Všeobecným cílem crackingu je neoprávněné použití produktů a jiných cenných dat.

Základní typy ochrany softwaru:

- Registrační číslo (seriál number)
- Časové omezení (time limit)
- Registrační soubor (key file)
- Program ve Visual Basicu nebo Delphi - zvýšení bezpečnosti použitím nepřehledného programovacího jazyka
- Hardwarový klíč (dongle)
- Kontrola originálního CD (CD-Check)
- Demo - omezené funkce programu
- Komerční ochrany - používané na dekomprimování před samotným spuštěním aplikace
- Další typy ochrany - např FLEXlm[45]

K odblokování softwaru existuje mnoho metod např. debugování a reverzní inženýrství. Cracking neslouží pouze k vytváření warez, ale též je to metoda, jak se dostat k důležitým informacím skrze ochranné prvky cílového systému. Jednou ze základních ochran systému je heslování. Metodou pro odhalení hesla je password cracking, které dle složitosti hesla používá techniky jako:

- Hádání hesla ze slovníku nejpoužívanějších hesel
- Hádání hesla pomocí hrubé síly zadáváním různých kombinací znaků
- Použití algoritmů snažících se o zpětnou rekonstrukci hesla ze zakódovaného řetězce

Trestní klasifikace tohoto typu činnosti může být velmi rozličná. Pokud právnické nebo fyzické osobě, která je vlastníkem systému, vůči němuž je útok crackingem prováděn, nevznikla prokazatelná škoda, může být od stíhání zcela

[45] ČERVEŇ, P. *Cracking a jak se proti němu bránit*. Praha : Computer Press, 2001. 13 s.

upuštěno. V ostatních případech se obvykle jedná o porušení autorského práva, nebo poškození či zneužití záznamu na nosiči informací.

Sniffing

Jedná se o neoprávněnou činnost "odposlouchávání", která bývá předzvěstí další ilegální akce ze strany útočníka. Toto jednání naplňuje skutkovou podstatu §182 TZ - porušování tajemství dopravovaných zpráv. V případě poskytnutí získaných údajů třetí straně je trestní sazba až 2 roky.

Bohužel dopadení pachatele takového činu a prokázání viny je velice obtížné.

5 Výzkum

Cílem výzkumu je stanovit míru povědomí respondentů v oblasti dostupné a používané ochrany před malwarem, jejich zkušenost s hackery a malwarem a také reakce na určité typy útoku. Pro dosažení optimálních výsledků byla zvolena metoda kvantitativního výzkumu.

Pro svůj kvantitativní výzkum si stanovuji tyto hypotézy:

1. Osoba hackera je veřejností všeobecně vnímána jako zločinec, který páchá rozsáhle škody, nebo se snaží obohatit se na úkor druhých a jen malá skupina lidí jej bude vnímat odlišně.
2. Dnešní uživatelé PC nejsou dostatečně informování o možných bezpečnostních hrozbách.

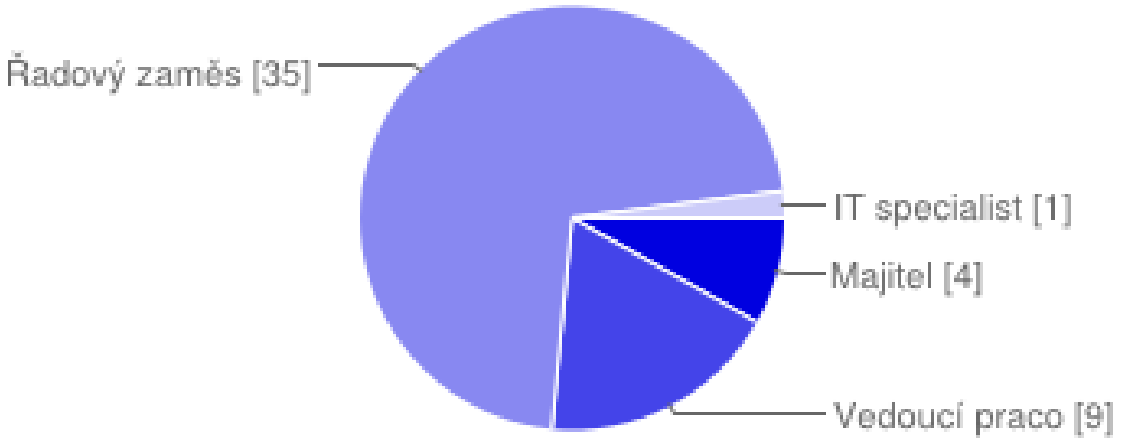
Při sestavování dotazníku jsem se soustředil na běžné problémy, se kterými se uživatel PC může setkat a snažil jsem se vystihnout to nejdůležitější a nejzákladnější, čemu by obsluha PC měla věnovat svou pozornost. Zároveň jsem několik otázek věnoval na konto informovanosti o potencionálních hrozbách. Zvolil jsem i základní otázky určující věk, pohlaví a postavení ve firmě, což ve výsledku umožňuje několik možností posouzení odpovědí.

Takto sestavený dotazník o 18 otázkách byl zacílen na menší a střední firmy, respektive na jejich zaměstnance, pracovníky či majitele. Dotazníkové šetření bylo rozšířeno anonymním uživatelům službou Google disk a získané odpovědi byly protříděny na 50 použitelných odpovědí pro výzkum.

5.1 Výsledky a popis výsledků dotazníkového šetření

Otázka č. 1: Jakou pozici ve firmě zastáváte?

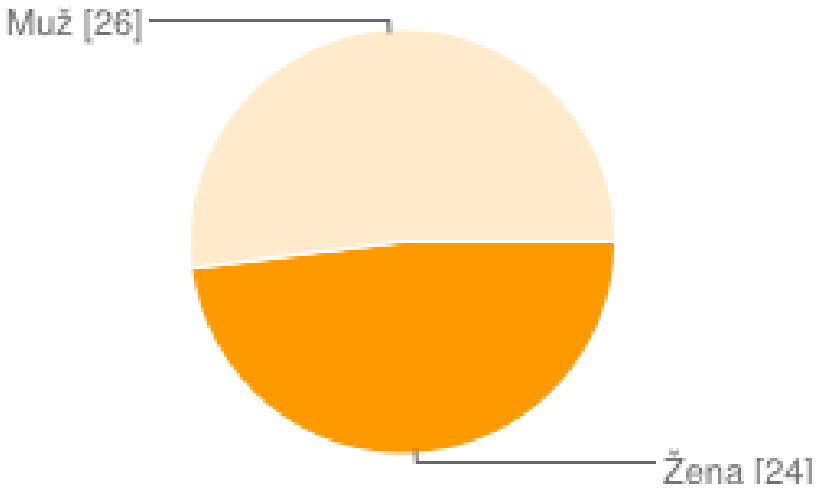
***Graf č. 1 Četnost respondentů z hlediska pracovní pozice ve firmě*[46].**



Mezi respondenty jsou zejména řadoví zaměstnanci (71%), kteří tvoří téměř 3/4 dotazovaných. Na druhou stranu nejméně zastoupení mají IT specialisté a to pouhá 2%. Po IT specialistech jsou majitelé s 8% a vedoucí pracovníci s 18%.

Otázka č. 2: Jakého jste pohlaví?

***Graf č. 2 Četnost respondentů z hlediska pohlaví*[47].**

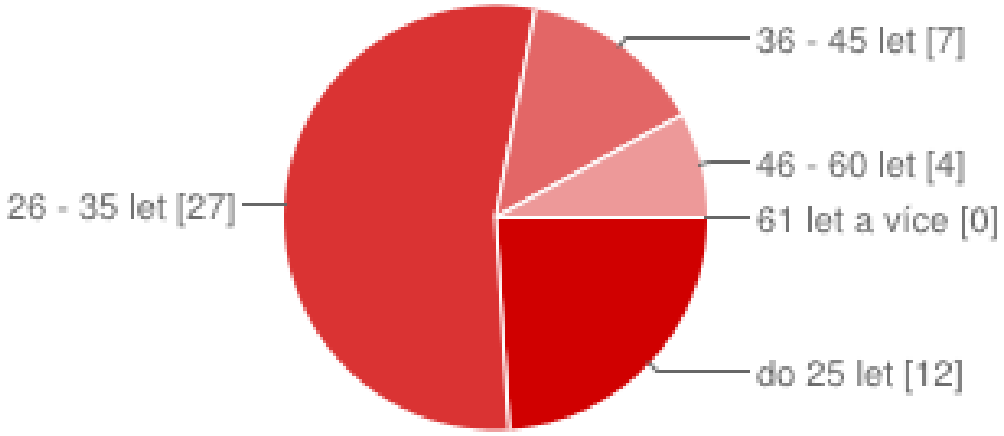


[46] Vlastní tvorba.
[47] Vlastní tvorba.

Ze získaných hodnot lze usoudit, že poměr dotazovaných mužů a žen je podobný. Mezi respondenty bylo o 4 % více mužů (52%). Žen tedy bylo 48 %.

Otázka č. 3: Kolik je Vám let?

***Graf č. 3 Četnost respondentů z hlediska stáří*[48].**

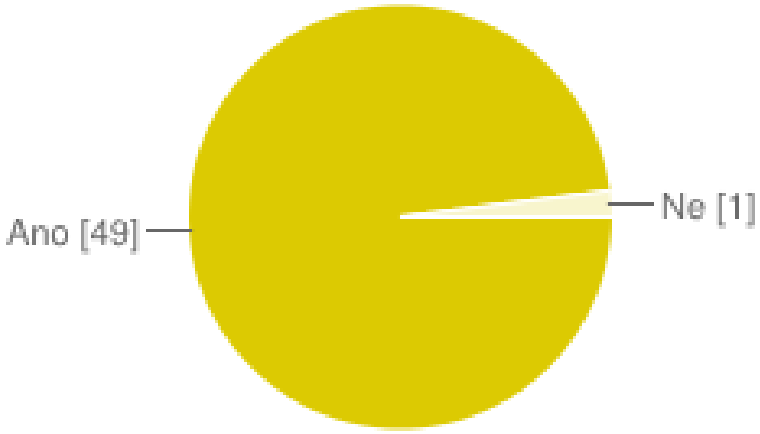


Souhrn odpovědí od respondentů ukazuje, že nejvíce odpovědí je od lidí ve věku 26 – 35 let (54%), kterých dle výsledků odpovědělo více než polovina. Na druhou stranu nejméně odpověděli respondenti ve věku 46 – 60 let (8%), když opomeneme skupinu 61 let a více, tuto odpověď žádný respondent nezvolil. Necelou čtvrtinu odpovědí získala věková skupina do 25 let (24%). Ve skupině 36 – 45 let byla zaznamenána sedmina (14%) odpovědí.

[48] Vlastní tvorba.

Otázka č. 4: Je Váš počítač připojen k Internetu nebo k jiné síti?

Graf č. 4 Četnost respondentů z hlediska dostupnosti připojení k internetu[49].

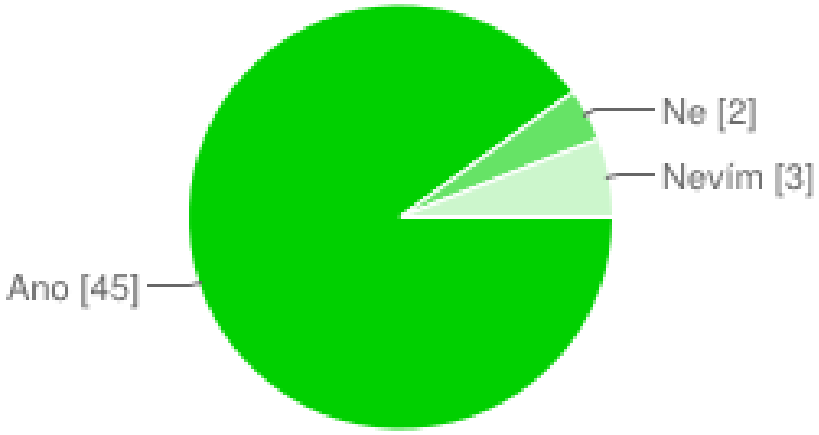


Dle odpovědí lze usoudit, že většina respondentů má připojený počítač k síti. Téměř všichni bez dvou procent používají počítač připojený k Internetu nebo jiné síti.

Otázka č. 5: Je Váš počítač chráněn pomocí antivirového programu, pokud ano, jakým?

Cílem této otázky bylo zjistit, zda jsou respondenti obezřetní, co se týká chránění jejich počítačů pomocí antivirového programu.

Graf č. 5 Četnost respondentů z hlediska používání antivirového programu[50].



[49] Vlastní tvorba.
[50] Vlastní tvorba.

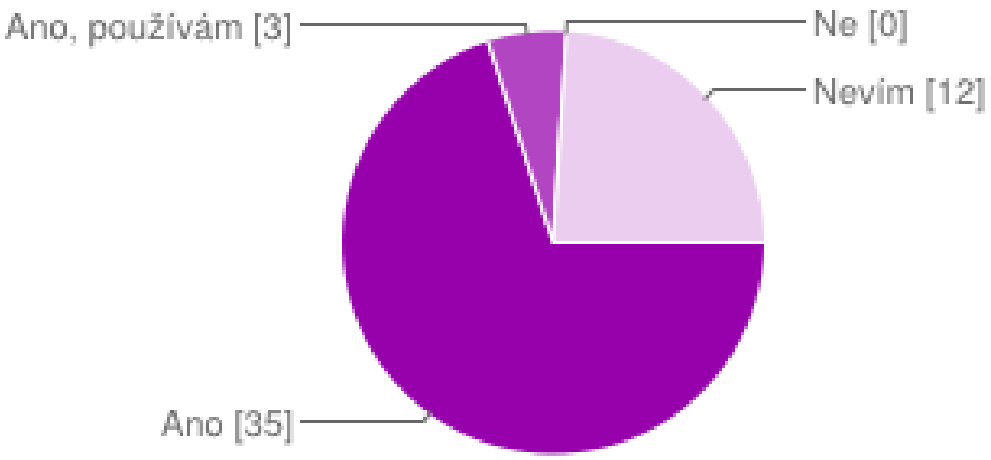
Dle získaných odpovědí je možné posoudit, že většina respondentů (90%) svůj počítač chrání. Pouhá 4 % respondentů není obezřetná a svůj počítač nechrání pomocí antivirového programu. Co je ovšem zajímavé, že se našli i tací, kteří zvolili odpověď „nevím“ (6%), což znamená, že mohou ohrozit v případě výskytu viru nejen svůj počítač a svá data, ale i data a počítače v podnikové síti.

Odpovědi respondentů: Avast, Windows, Firefox, AVG, nod 32, norton, Symantec, ESET Smart Security, Microsoft Security Essentials, Eset, Kaspersky, MS Essetial.

Z doplňující otázky je patrné, že respondenti využívají celou škálu antivirových řešení včetně placených verzí s rozšířenými možnostmi komplexní ochrany systému. Nad jednou z odpovědí se ještě pozastavím, odpověď FIREFOX je zcela špatně, protože dotazovaný zvolil místo antivirového programu internetový prohlížeč (řadový zaměstnanec - muž - věk mezi 25 až 36 lety).

Otázka č. 6: Je Váš počítač chráněný pomocí firewallu?

Graf č. 6 Četnost respondentů z hlediska používání firewallu[51].



Necelé 3/4 (70%) respondentů odpověděly, že používají k ochraně svého počítače firewall. Zároveň jedna čtvrtina respondentů (24%) odpověděla, že neví, zda

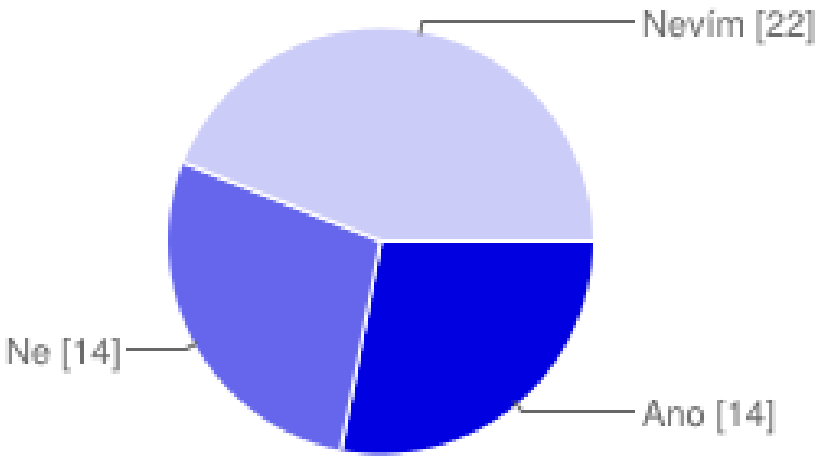
[51] Vlastní tvorba.

je jejich počítač chráněn tímto způsobem. A pouhých 6 % respondentů odpovědělo, že používají komplexní řešení.

Poměrně vysoký počet odpovědí "Nevím" značí jasnou mezeru v informovanosti, která se více projevila u žen (9), a to napříč pracovními pozicemi, nejvíce však u řadových zaměstnankyň (7). Stejnou odpověď zvolili i 3 muži z pozice řadový zaměstnanec.

Otázka č. 7: Používáte k ochraně PC i jiný software kromě výše zmíněných, pokud ano, jaký?

Graf č. 7 Četnost respondentů z hlediska používání další ochrany PC[52].



Získané hodnoty nám ukázaly, že necelá polovina respondentů (44%) na otázku „Používáte k ochraně PC i jiný software kromě výše zmíněných?“ odpověděla, že neví. Zbylé dvě odpovědi „Ano“ a „Ne“ získaly stejné množství procent a to 28%.

Odpovědi respondentů: McAfee, Ccleaner, Sbybot, proxy, web content filtering, spybot sandD.

Tato otázka byla náročnější a projevilo se to vyšším počtem respondentů s odpovědí "Nevím" oproti předchozí otázce. Jako příčinu bych označil skutečnost,

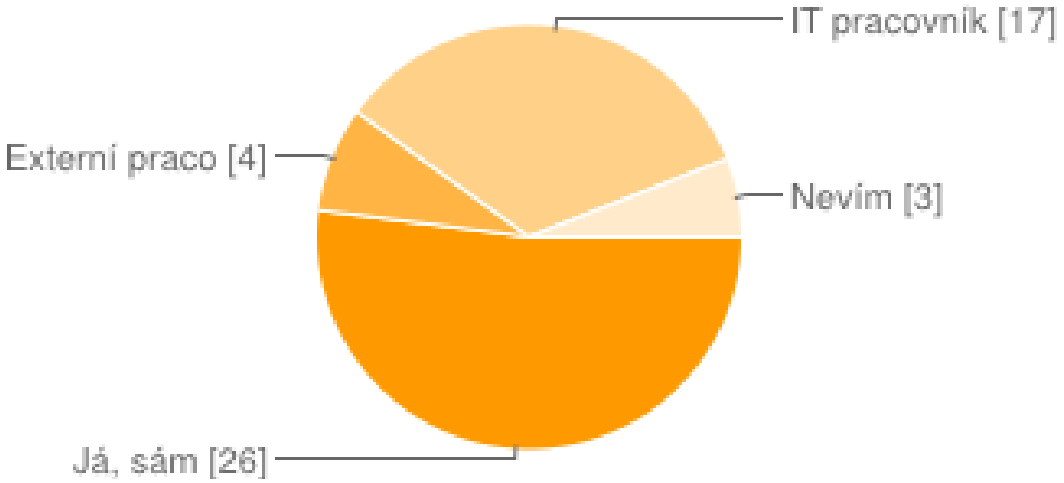
[52] Vlastní tvorba.

že výše zmíněné programy používají více zkušení uživatelé, nebo uživatelé instruovaní IT techniky.

Otázka č. 8: Kdo se stará o aktualizace operačního systému?

Tato otázka mapovala, kdo se respondentům stará o aktualizaci operačního systému počítače.

Graf č. 8 Četnost respondentů z hlediska spravování aktualizací OS[53].



Dle získaných hodnot můžeme říct, že více než polovina respondentů (52%) se stará o aktualizaci operačního systému sama. Ale třetina respondentů (34%) má pro tuto funkci ve své firmě IT specialistu. Tam kde nemají vlastního IT specialistu, tuto funkci vykonává externí pracovník, což se týká 8% respondentů. Poslední možností byla odpověď „Nevím“, kterou zvolilo 6% respondentů.

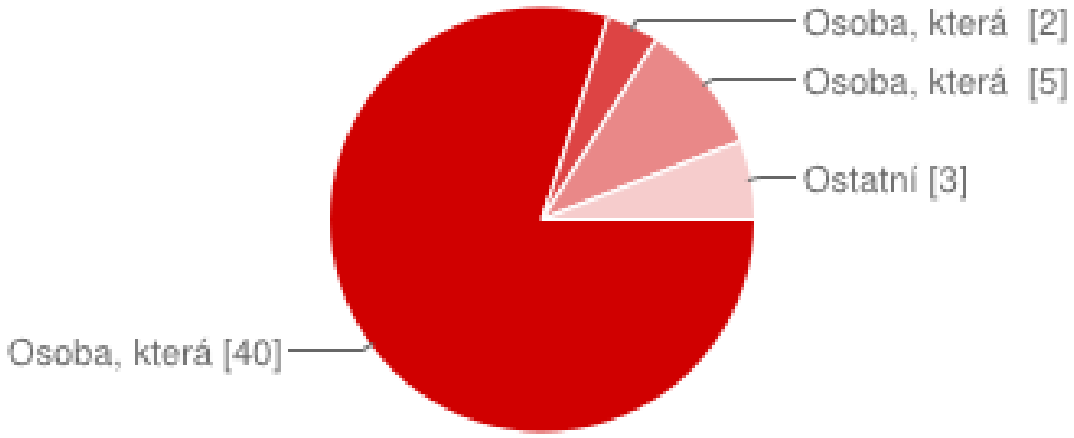
Odpovědi na tuto otázku s porovnáním ostatních údajů naznačují, že i tam běžná věc jako aktualizace OS je podstupována profesionálům, a to ve více jak 40% případů. Takto vysoké číslo přivádí k zamyšlení, zda jsou uživatelé pohodlní, neznalí, nebo jen nemají přístup k této akci skrze omezená práva správce sítě.

[53] Vlastní tvorba.

Otázka č. 9: Co pro Vás znamená označení HACKER?

Tato otázka mapovala názor respondentů na lidi, které označujeme jako Hackery.

Graf č. 9 Četnost respondentů na téma kdo je to hacker[54].



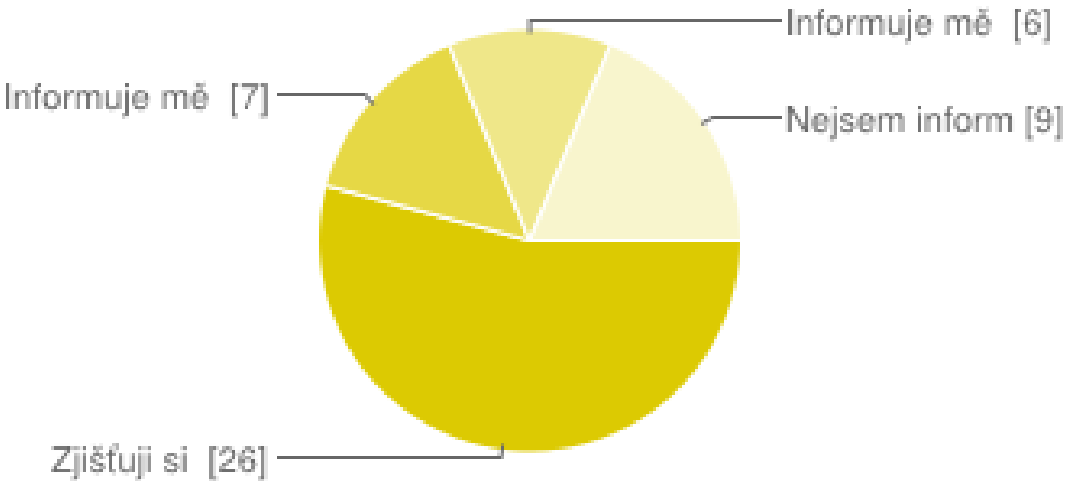
Tento graf jasně ukazuje, že přesně 4/5 respondentů si myslí, že Hacker škodí různými způsoby skrze internet. Na druhé straně pouhá 4% respondentů Hackera považují za člověka spravujícího rozsáhlé sítě a starajícího se o jejich chod. Správnou představu o osobě, kterou označujeme slovem Hacker, mělo pouhých 10% respondentů, podle kterých to je osoba detekující bezpečnostní hrozby a následně je ohlásí správci sítě. Zbývající odpověď ostatní vybralo 6% respondentů.

Dle etického hlediska jsem zvolil jako správnou odpověď "osoba detekující bezpečnostní hrozby a následně je ohlásí správci sítě", která označuje tzv. White hats. Dle očekávaní většina respondentů zvolila médii zkreslenou podobu hackera a tudíž se i potvrdila jedna z hypotéz.

[54] Vlastní tvorba.

Otázka č. 10: Jakým způsobem jste školeni o nových bezpečnostních hrozbách?

Graf č. 10 Četnost respondentů z hlediska informovanosti o nových hrozbách[55].



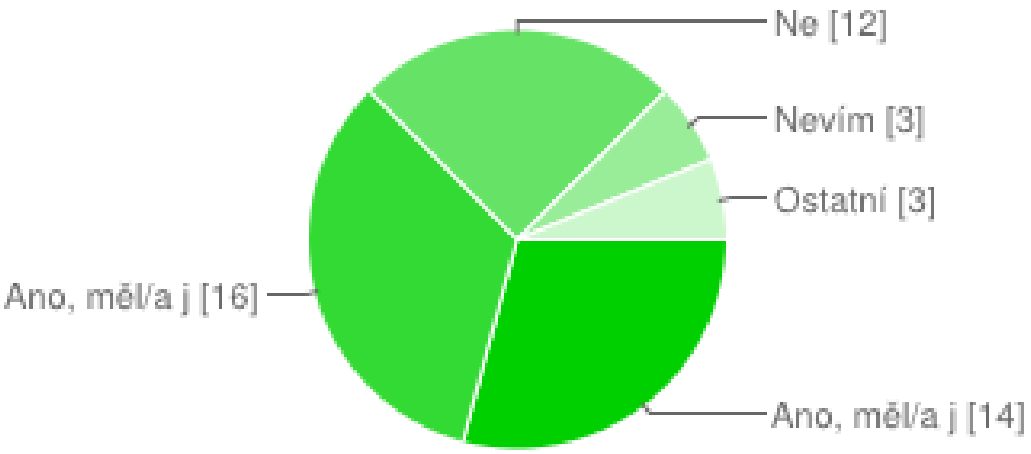
Více než polovina respondentů (54%) si zjišťuje novinky sama. Naproti tomu 13 % respondentů je informována od vedoucího a 15 % respondentů získává novinky od pracovníka specializované firmy. Co je ale zajímavé, že necelá pětina (19%) dotazovaných není informována.

Porovnáním stáří dotazovaných kdy skoro 80% je ve věku 25-35 let a 20% neinformovaných dotazovaných naznačuje jistou závislost. A to snižující se zájem o nové potencionální hrozby se zvyšujícím se věkem. Tato skutečnost je částečně zapříčiněna opožděným rozmachem IT technologií na území České republiky.

[55] Vlastní tvorba.

Otázka č. 11: Stal/a jste se někdy obětí nějakého škodlivého softwaru?

Graf č. 11 Četnost respondentů z hlediska setkání se s škodlivým softwarem[56].

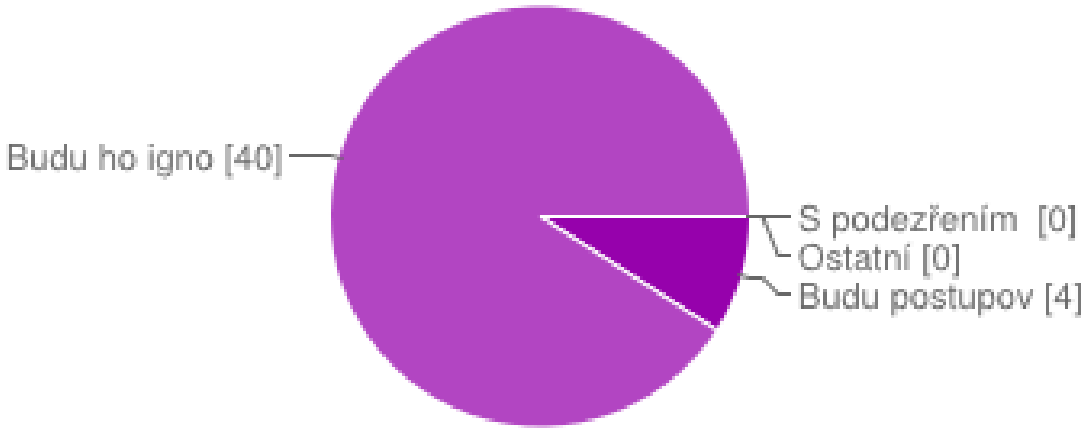


U této otázky nejvíce (33%) respondentů odpovědělo, že měli problém s trojským koněm, naproti tomu nejméně respondentů nevědělo, zda byli obětí nějakého škodlivého softwaru nebo nějakého jiného nezmíněného softwaru, v obou případech se jednalo o 6 % dotazovaných. Přesně čtvrtina (25%) respondentů se nikdy nestala obětí škodlivého softwaru a 29% dotazovaných mělo problém s virem.

[56] Vlastní tvorba.

Otázka č. 12: Jak se zachováte jako klient zmíněné instituce při obdržení následujícího emailu?

***Graf č. 12 Četnost respondentů z hlediska reakce na podvodný email*[57].**



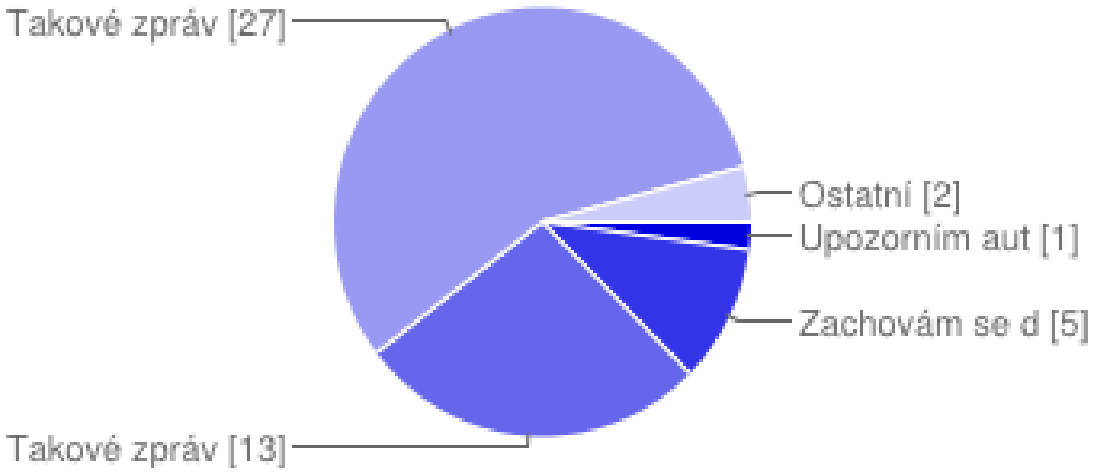
Valná většina (91%) respondentů si vybrala odpověď, že takovou zprávu budou ignorovat, zbývajících 9% dotazovaných by v takovém případě postupovalo dle instrukcí. Zbylé dvě odpovědi si nezvolil žádný respondent.

Přirozená obezřetnost většinu respondentů vedla ke správné odpovědi, otázkou zůstává, zda-li by se zachovali stejně, kdyby email obsahoval jiné znění. Takovýto email je jedna z možností, jak se může hacker s označení black hat dostat k osobním financím oběti, která poslušně následuje nabídnuté kroky.

[57] Vlastní tvorba.

Otázka č. 13: Jak se zachováte při obdržení HOAXU?

Graf č. 13 Četnost respondentů z hlediska reakce na HOAX[58].



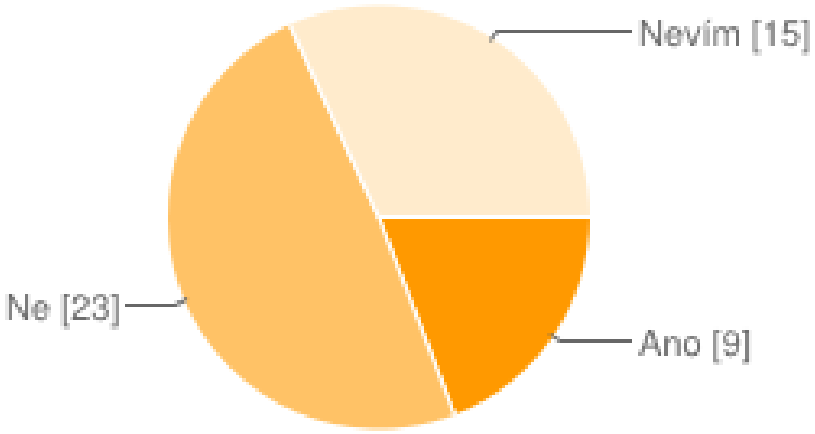
Ze získaných odpovědí plyne, že více jak polovina (56%) respondentů by tento typ zprávy ignorovala. Oproti tomu pouhé 2% dotazovaných by upozornili autora, že se jedná o HOAX a požádali ho, aby ho dál nešířil. Čtyři procenta dotazovaných zvolila odpověď ostatní. Jedna desetina (10%) respondentů by se zachovala dle instrukcí a poslala zprávu dál. A přibližně čtvrtina (27%) dotazovaných takové zprávy nečte, protože mohou obsahovat viry.

I v tomto případě drtivá většina dotazovaných zvolila ignorovat zprávu. Někteří sice z mylné představy, že zpráva obsahuje viry, čímž potvrdili mou domněnku o nedostatečné informovanosti. Zrovna v případě hoaxu existuje mnoho stránek vysvětlující tento pojem i rady jak se zachovat při jeho obdržení.

[58] Vlastní tvorba.

Otázka č. 14: Setkal jste se někdy s útokem typu DDoS?

Graf č. 14 Četnost respondentů, kteří se setkali s DDoS útokem[59].



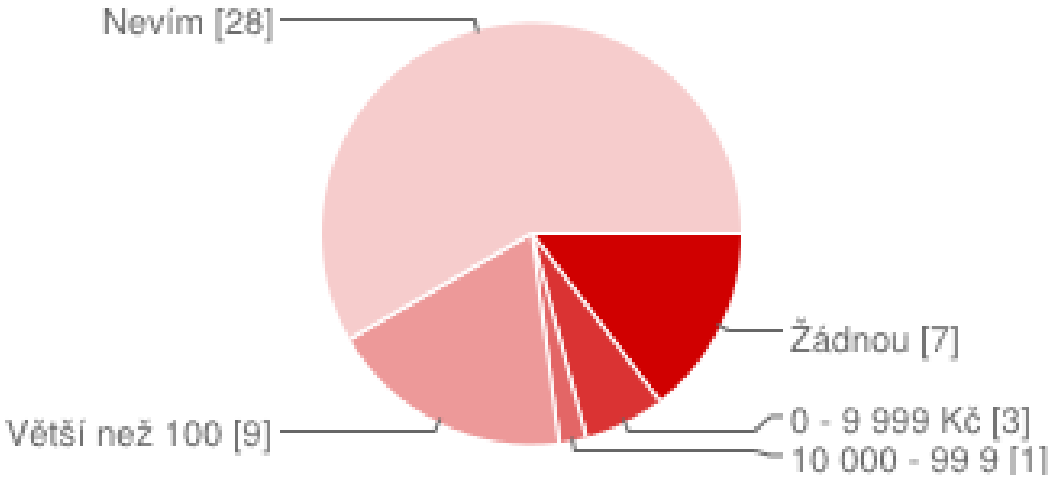
Po zhodnocení odpovědí je více než jasné, že necelá polovina (49%) respondentů se nikdy nesetkala s útokem typu DDoS. Naproti tomu necelá pětina (19%) dotazovaných tuto zkušenost již má. Mezi respondenty se našlo 32% lidí, kteří nevěděli, zda se s útokem tohoto typu setkali.

Odpovědi na tuto otázku nejsou překvapením a kopírují skladbu použitého vzorku respondentů. I přes vysvětlení, které otázku doplňovalo si mnoho dotazovaných pravděpodobně ani neuvědomovalo, že se s tímto typem útoku mohlo setkat v běžném životě. V roce 2013 se pod palbu paketů dostalo několik velikých institucí v České republice, jako weby mobilních operátorů a vládních organizací. Mnozí se jistě setkali i s výpadkem online služeb finančních institucí.

[59] Vlastní tvorba.

Otázka č. 15: Jak vysokou finanční ztrátu by zaznamenala Vaše firma v případě úspěšného DDoS útoku?

Graf č. 15 Četnost respondentů z hlediska finanční ztráty při nedostupnosti služby[60].



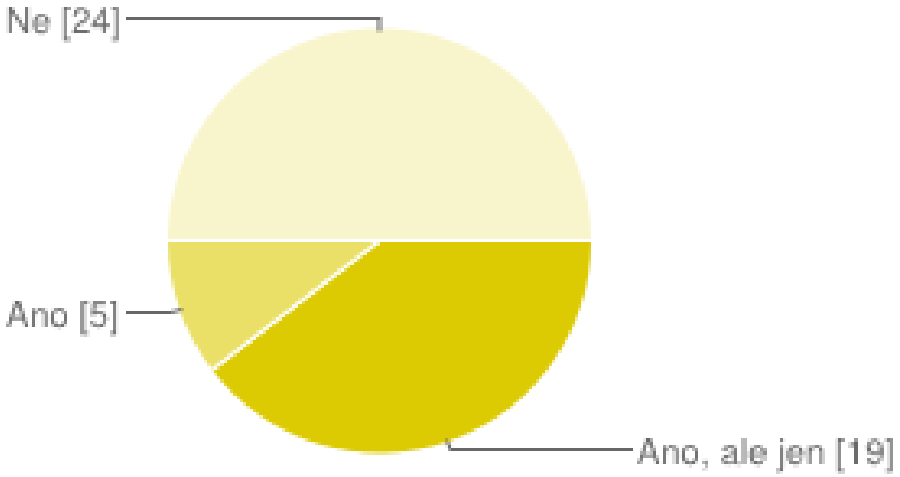
Více jak polovina (58%) respondentů si není vědoma nebo nedokáže odhadnout, jakou ztrátu by zaznamenala firma, ve které pracující. Žádnou ztrátu by nezaznamenaly firmy zaměstnávající 15% z dotazovaných. Možnost, že by firmu, ve které dotazovaní pracují, postihla minimální ztráta od 0 až do 9 999 Kč, zvolilo 6 % respondentů. Pro variantu větší ztráty v rozsahu 10 000 – 99 999 Kč se rozhodla pouhá dvě procenta. A poslední variantu, že by firmu, kde respondent pracuje, postihla ztráta větší než 100 000 Kč, zvolilo 19% tázaných.

Z historických záznamů je patrné, že veliké společnosti jako eBay a Amazon, které své služby nabízejí výhradně online v případě úspěšného DDoS útoku zaznamenají nevyčíslitelné ztráty. V případě menších a středních firem by cílem útoku byl pravděpodobně e-shop, prezentační web, online formuláře, nebo architektura sítě.

[60] Vlastní tvorba.

Otázka č. 16: Používáte nějaký nelegální software?

Graf č. 16 Četnost respondentů z hlediska používání ilegálního SW[61].



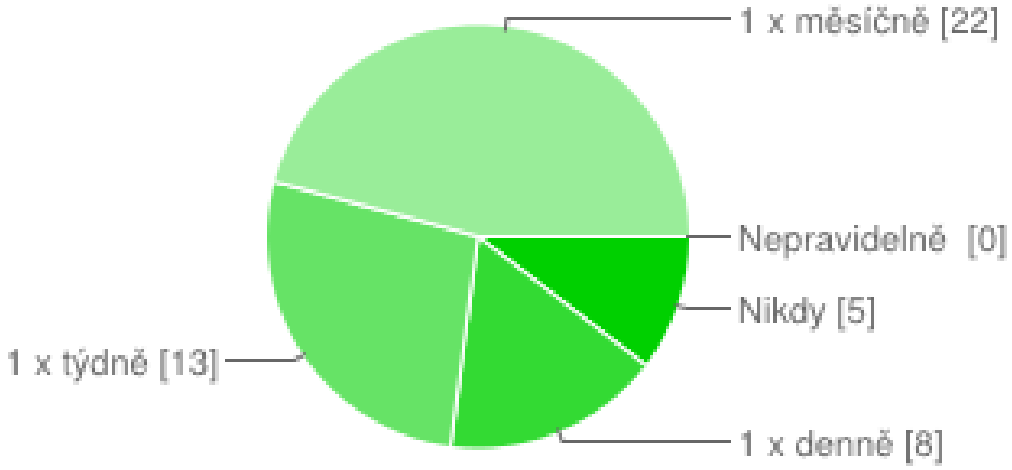
Dle získaných odpovědí můžeme usoudit, že polovina (50%) respondentů nepoužívá nelegální software. Oproti tomu pouhých 10 % dotazovaných používá nějaký nelegální software a zbývajících 40% tázaných používá nějaký nelegální software pouze pro soukromé účely.

Otázka ohledně warez jasně ukazuje na stav ilegálně používaného softwaru. Když pominu otázku autorských práv a zaměřím se na bezpečnostní problémy, tak se vnoříme do koloběhu událostí kdy crackerská skupina získá program např. pomocí metody sociálního inženýrství, crackne ochranné prvky a okamžitě jej zpřístupní warez komunitě. V tuto chvíli může využít black hat hacker uživateli oblíbeného programu k šíření škodlivého software, který si po stažení programu uživatel nainstaluje spolu s kýženým programem a hacker v tu chvíli získá pomocí backdooru neomezený přístup a kontrolu nad počítačem, případně nad celou sítí.

[61] Vlastní tvorba.

Otázka č. 17: Jak často provádí kontrolu dat antivirovým programem?

Graf č. 17 Četnost respondentů z hlediska četnosti kontroly antivirem[62].



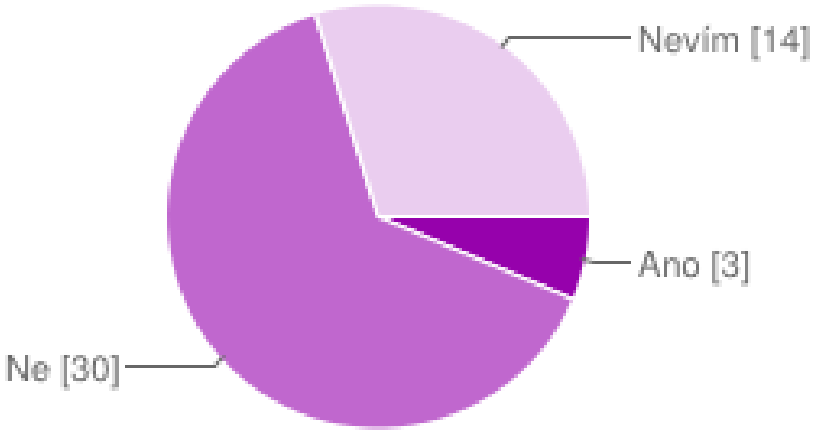
Ze získaných odpovědí vyplývá, že nejvíce (46%) respondentů provádí kontrolu dat antivirovým programem minimálně jednou měsíčně. Na druhou stranu žádný respondent nezvolil odpověď Nepravidelně – méně než jednou měsíčně. Svá data nikdy nekontroluje až 10% dotazovaných. Další z možností, že si respondenti kontrolují svá data jednou denně, zvolilo 17% tázaných. A zbývající variantu, že svá data kontrolují jednou týdně, si vybralo 27% dotazovaných.

Výsledné údaje přesně korespondují s odpověďmi na téma používání antivirového programu. Respondenti přistupují k pravidelným kontrolám zodpovědně a snaží se tak předejít případnému rozšíření infekce.

[62] Vlastní tvorba.

Otázka č. 18: Setkal/a jste se někdy s praktikou zvanou sociální inženýrství, pokud ano s jakou?

Graf č. 18 Četnost respondentů z hlediska setkání se s sociálním inženýrstvím[63].



Dle získaných odpovědí je jasné, že více jak polovina (64%) respondentů se nikdy nesetkala s praktikou zvanou sociální inženýrství. Oproti tomu pouhých 6 % dotazovaných má zkušenost se zmíněnou praktikou. Zbývající respondenti (32%) zvolili možnost nevím.

Odpovědi respondentů: fishing, předstírání jiné identity, pretexting.

Vyhodnocení hypotéz

První hypotéza se potvrdila, když 80% všech dotazovaných vybralo záporné hodnocení označení hacker, jakožto osobu škodící skrze internet. Skupina dotazovaných se k osobě hackera vyjádřila dle vládnoucího názoru široké veřejnosti, který je silně zmanipulován médii a všeobecnou neinformovaností. Skutečnost, že hacker může napomáhat odhalovat bezpečnostní hrozby vědělo pouze 10% respondentů, z toho 3 ženy ve vedení firmy a dva muži na postu řadový pracovník.

Druhá hypotéza se nepotvrdila, když pouze 19% dotazovaných uvedlo, že nejsou informovaní. Čekal jsem výslednou hodnotu vyšší než 30%. Pozitivní výsledek byl ovlivněn zejména aktivním zjišťováním novinek samotnými respondenty.

[63] Vlastní tvorba.

Zajímavostí je, že u otázek úzce spojených s informovaností, tedy u otázek zabývajících se běžnou ochranou proti malwaru odpovídali "nevím" až měrou 44%.

Závěr

Cílem bakalářské práce je přiblížit problematiku počítačové kriminality a hackerské komunity jako takové. Co se problematiky hackerů týče, tak je to dozajisté velice sporný bod, jehož řešení se liší s ohledem na skupinu, která ho posuzuje. Po prostudování dostupné odborné literatury i výsledků výzkumu se přikláním k variantě, že osoba hackera má více pozitiv než negativ, čímž se liším od názoru široké veřejnosti i většiny dotazovaných. Jako příklad uvedu nepřehlédnutelnou část trhu se softwarem na ochranu OS, které zaměstnává a živý masu lidí, a to od programátorů vyvíjející tento software až po IT techniky, kteří se živí servisem pro malé firmy a koncové uživatele. Ať už aktivně, nebo pasivně se osoba hackera podílí na efektivnější tvorbě softwarových záplat OS a programů, což opět vytváří poptávku na trhu práce a zároveň nutí obrovské giganty, aby koncovým zákazníkům nabízely stále kvalitnější služby. Dříve či později si většina hackerů projde svým vývojem a dozraje do podoby, která je společnosti prospěšná.

Veliká propast se s ohledem na zákony dotýkající se problematiky počítačové kriminality nachází v dokazování, a to je dlouhodobý problém nejen u zločinů páchaných v kyberprostoru. I když legislativa reaguje na realitu a trendy se značným zpožděním, tak je možné najít trestně právní úpravu pro všechny uvedené trestné činy ze cyber prostředí.

I díky anonymnímu dotazníku lze usoudit, že lidé v České republice jsou nedostatečně informovaní, co se týká nebezpečí a hrozeb při používání počítače a jeho připojení k síti. A při ochraně svých dat jsou často nerozvážní a lehkomyslní. Pro většinu lidí znamená počítač a připojení k síti samozřejmost, ale ochrana dat, která by měla být prioritní, je velmi zanedbána. Kvůli tomu se mnoho lidí stává obětí nějakého škodlivého softwaru, nebo jiných praktik. Je velice zajímavé, kolik respondentů uvedlo, že používá vědomě ilegální software, přičemž právě ten bývá zdrojem malwaru a koloběhu následných problémů.

Na druhou stranu je potřeba připustit, že v klíčových otázkách se většina respondentů zachovala dle zdravého rozumu a nespadla do připravené léčky.

Seznam použitých zdrojů

TIŠTĚNÉ ZDROJE

1. CASEY, E. *Handbook of computer crime investigation*. San Diego : Academic Press, 2002. 448 s. ISBN 0-12-163103-6.
2. CRAIG, P., HONICK, R. *Softwarové pirátství bez záhad*. Přeložil Tomáš HLAVÁČ. Praha : Grada, 2008. 212 s. ISBN 978-80-247-1765-4.
3. ČERVEŇ, P. *Cracking a jak se proti němu bránit*. Praha : Computer Press, 2001. 205 s. ISBN 80-7226-382-X.
4. GŘIVNA, T., POLČÁK, R., ed. *Kyberkriminalita a právo*. Praha : Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.
5. HARRIS, S., et al. *Hacking: manuál hackera*. Praha : Grada, 2008. 399 s. ISBN 978-80-247-1346-5.
6. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada, 2007. 284 s. ISBN 978-80-247-1561-2.
7. MATĚJKA, M. *Počítačová kriminalita*. Praha : Computer Press, 2002. 106 s. ISBN 80-7226-419-2.
8. MCCLURE, S., SCAMBRAY, J., KURTZ, G. *Hacking bez záhad*. 5. dopl. vyd. Praha : Grada, 2007. 520 s. ISBN 978-80-247-1502-5.
9. OLSON, P. *Jsme Anonymous: uvnitř hackerského světa Anonymous, LulzSec a globální internetové vzpoury*. Praha : Práh, 2012. 494 s. ISBN 978-80-7252-400-6.
10. POŽÁR, J. *Informační bezpečnost*. Plzeň : Aleš Čeněk s.r.o., 2005. 309 s. ISBN 80-868-9838-5.
11. SCAMBRAY, J. *Hacking bez tajemství: Windows 9x, Me, NT a 2000, NetWare, Unix*. Praha : Computer Press, 2001. 592 s. ISBN 80-7226-549-0.
12. SCAMBRAY, J. *Hacking bez tajemství: Windows 2000*. Praha : Computer Press, 2003. 461 s. ISBN 80-7226-781-7.

13. SCAMBRAY, J. *Hacking bez tajemství: webové aplikace*. Brno : Computer Press, 2003. 328 s. ISBN 80-7226-769-8.
14. SMEJKAL, V., et al. *Právo informačních a telekomunikačních systémů*. Praha : C. H. Beck, 2001. 542 s. ISBN 80-717-9552-6.

ELEKTRONICKÉ ZDROJE

1. *Základní definice, vztahující se k tématu kybernetické bezpečnosti.* [online]. Praha, 2009, [cit. 2013-08-03]. Dostupné z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>.
2. PAUKERTOVÁ, V. *Elektronická informační kriminalita*. [online]. Ikaros. 2006, roč. 10, č. 8 [cit. 06.05.2013]. Dostupné z WWW: <http://www.ikaros.cz/node/3554>.
3. AION CS. *Předpis č. 127/2005 Sb.: Zákon o elektronických komunikacích.* [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: <http://www.zakonyprolidi.cz/cs/2005-127>.
4. AION CS. *Předpis č. 121/2000 Sb.: Autorský zákon.* [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: <http:// http://www.zakonyprolidi.cz/cs/2000-121 >.
5. AION CS. *Předpis č. 101/2000 Sb.: Zákon o ochraně osobních údajů*. [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: < http://www.zakonyprolidi.cz/cs/2000-101>.
6. AION CS. *Předpis č. 40/2009 Sb.: Zákon trestní zákoník.* [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: < http://www.zakonyprolidi.cz/cs/2009-40>.
7. AION CS. *Předpis č. 40/1964 Sb.: Občanský zákoník.* [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: <http://www.zakonyprolidi.cz/cs/1964-40>.
8. AION CS. *Předpis č. 513/1991 Sb.: Obchodní zákoník.* [online]. AION CS, © 2010 - 2013, [cit 2013-12-09]. Dostupné z WWW: <http://www.zakonyprolidi.cz/cs/1991-513>.
9. ČESKO. *Zákon č. 480/2004 Sb.: Zákon o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách*

informační společnosti). [online]. MVČR, © 2014, [cit 2014-01-09]. Dostupné z WWW: < http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=480/2004%20&typeLaw=zakon&what=Cislo_zakona_smlouvy>.

Seznam tabulek a grafů

Přílohy

Příloha č. 1: Použitý dotazník.

Umíte se bránit?

Jakou pozici ve firmě zastáváte?

- Majitel
- Vedoucí pracovník
- Řadový zaměstnanec
- IT specialista

Jakého jste pohlaví?

- Žena
- Muž

Kolik Vám je let?

- do 25 let
- 26 - 35 let
- 36 - 45 let
- 46 - 60 let
- 61 let a více

Je Váš počítač připojen k Internetu nebo k jiné síti?

- Ano
- Ne

Je Váš počítač chráněn pomocí antivirového programu? Pokud ano, tak jaký?

- Ano
- Ne
- Nevím

Je Váš počítač chráněný pomocí firewallu?

- Ano

- Ano, používám komplexní řešení
- Ne
- Nevím

Používáte k ochraně PC i jiný software kromě výše zmíněných? Pokud ano, tak jaký?

- Ano
- Ne
- Nevím

Kdo se stará o aktualizace operačního systému?

- Já, sám
- Externí pracovník
- IT pracovník naší firmy
- Nevím

Co pro Vás znamená označení HACKER?

- Osoba, která různými způsoby škodí skrze internet
- Osoba, která spravuje rozsáhlé sítě a stará se o jejich chod
- Osoba, která detekuje bezpečnostní hrozby a následně je ohlásí správci sítě

Jakým způsobem jste školeni o nových bezpečnostních hrozbách?

- Zjišťuji si novinky sám
- Informuje mě pracovník specializované firmy
- Informuje mě můj vedoucí
- Nejsem informovaný

Stal/a jste se někdy obětí nějakého škodlivého softwaru?

- Ano, měl/a jsem problém s virem
- Ano, měl/a jsem problém s trojským koněm
- Ne
- Nevím

Jak se zachováte jako klient zmíněné instituce při obdržení následujícího emailu?

Text: Vazeni klienti, radi bychom Vas upozornili na novou verzi podvodneho e-mailu (tzv. phishingu). Nova verze e-mailu ma jako ty predesle vzbudit dojem, ze byla odeslana z e-mailove adresy Ceske sporitelny, tentokrat vsak z oficialni e-mailove adresy banky csas@csas.cz. Obsahuje odkaz v tele na udajne webove stranky internetoveho bankovnictvi banky a uzivatel je vyzvan k prihlaseni, tedy zadani osobnich bankovnich udaju. Prosim, verifikujte tuto emailovou adresu kliknutim na spojeni nize: http://www.csas.cz/banka/appmanager/portal/banka Verifikovaci spojeni je platne do 24 hodin.

- Budu postupovat dle instrukcí
- Budu ho ignorovat
- S podezřením na phising email nahlásím příslušné instituci

Jak se zachováte při obdržení HOAXU?

Text: V pátek začne Facebook používat vaše fotky v reklamách, které se objeví na stránkách profilu Vašich kontaktů. Je to legální a je to zmiňováno v drobném písmu, když jste si vytvářeli účet. Abyste se vyhnuli takovéto nezvané publicitě, jděte na: Účet, Nastavení účtu, pak klikněte na záložku Reklamy na Facebooku a vyberte "nikdo" v rolovacím menu. A pak uložte změny. Zkopírujte text do "statusu". ŠIŘTE INFO DÁL.

- Upozorním autora emailu, že se jedná o HOAX a požádám ho, aby ho dál nešířil
- Zachovám se dle instrukcí a zprávu pošlu dál
- Takové zprávy raději nečtu, mohou obsahovat viry
- Takové zprávy ignoruji

Setkal jste se někdy s útokem typu DDoS?

Text: Denial of Service (česky odmítnutí služby) je útok zahlcením obrovským množstvím dat, při kterém dochází k nefunkčnosti a nedostupnosti internetové služby nebo stránky pro ostatní uživatele.

- Ano
- Ne
- Nevím

Jak vysokou finanční ztrátu by zaznamenala Vaše firma v případě úspěšného DDoS útoku?

- Žádnou
- 0 - 9 999 Kč
- 10 000 - 99 999 Kč
- Větší než 100 000 Kč
- Nevím

Používáte nějaký nelegální software?

- Ano, ale jen pro soukromé účely
- Ano
- Ne

Jak často provádí kontrolu dat antivirovým programem?

- Nikdy
- 1 x denně
- 1 x týdně
- 1 x měsíčně
- Nepravidelně - méně než 1 x měsíčně

Setkal/a jste se někdy s praktikou zvanou sociální inženýrství? Pokud ano, tak s jakou?

Text: Sociální inženýrství je způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace, a to bez osobního kontaktu s útočníkem.

- Ano
- Ne
- Nevím