Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra statistiky

Diplomová práce

Počítačová kriminalita

Bc. Vítězslav Chochola

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra statistiky

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Vítězslav Chochola

Hospodářská politika a správa

Název práce
Počítačová kriminalita

Anglický název
Computer crime

Cíle práce

Cílem práce je posouzení informační společnosti z pohledu obezřetnosti při používání informačních technologií, upozornění na podceňování zabezpečení dat a důvěřivost vůči zdrojům informací či přímo hrozícího nebezpečí elektronické kriminality, a to i z pohledu vyšetřování takovýchto činů.

Metodika

S využitím vlastní práce i dostupných záznamů pracovišť státní správy , zabývajících se počítačovou kriminalitou vyjádřit podceňování nebezpečí kriminality. Získané údaje budou analyzovány vhodnými statistickými postupy.

Rozsah textové části

cca 60 stran

Klíčová slova

elektronická média, Informační společnost, Internet, kriminalita, trestný čin, vyšetřování, zabezpečení dat

---

Doporučené zdroje informací

CEJPEK, J. Informace, komunikace a myšlení. 2. vyd. Praha: Karolinum, 2005. ISBN 80-246-1037-X.
HULANOVÁ, L. Internetová kriminalita páchaná na dětech. 1. vyd. Praha: Triton, 2012. ISBN 978-80-7387-545-9.
Identity in the Information Society [online], ročníky 2008-2010. ISSN: 1876-0678. Dostupné z: http://www.springer.
KALAMÁR, Š. a J. POŽÁR. Vybrané aspekty informační bezpečnosti.1. vyd. Praha: PAČR, 2010. ISBN 978-80-7251-339-0.
KOLOUCH, J. Trestněprávní ochrana před kybernetickou kriminalitou. 1. vyd. Praha: PAČR, 2013. ISBN 978-80-7251-402-1.
MUSIL, M. Elektronická média v informační společnosti. 1. vyd. Praha: Votobia, 2003. ISBN 80-7220-157-3.
PROKEŠ, J. Člověk a počítač aneb svítání digitální kultury. 1. vyd. Tišnov: Sursum, 2000. ISBN 80-85799-82-0.
SMEJKAL, V. Internet a §§§. 1. vyd. Praha: Grada Publishing, 2001. ISBN 80-247-0058-1.

Vedoucí práce

RNDr. Jan Grosz

Elektronicky schváleno dne 15. 10. 2014

prof. Ing. Libuše Svatošová, CSc.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2014

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 06. 02. 2015

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Počítačová kriminalita" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30.3.2015 _____

Poděkování

Rád bych touto cestou poděkoval panu RNDr. Janu Groszovi za odborné vedení práce a podnětné připomínky. Mé poděkování patří i rodině a všem, kteří mi umožnili se této práci věnovat.

Počítačová kriminalita

Computer Crime

Souhrn

Práce se zabývá počítačovou kriminalitou v České republice. Hlavním cílem je nalezení souvislosti mezi jejím nárůstem a chováním uživatelů Internetu.

Tvoří ji základní přehled těch nejčastějších oblastí kriminality, seznamuje se stručnou historií technologií obsahující první projevy související kriminality. Následuje hlavní část, která je analýzou chování uživatelů, zpracované na základě empirického výzkumu.

Ten se zaměřil na používání běžně dostupných bezpečnostních prostředků a znalost některých důležitých prvků internetové komunikace. U souvisejících otázek zjišťuje závislosti zjištěných výsledků. Empirická část dále sleduje dosavadní průběh počtu případů počítačové kriminality v České republice a na základě něj za použití statistické metody odhaduje budoucí vývoj.

Zjištění z empirické části je dále sumarizováno v závěrečné části a na základě nalezení slabých míst české uživatelské základny jsou navrhována opatření, která mohou úspěšnost pachatelů počítačové kriminality zmírnit.

Průběžně je práce doprovázena případy z kazuistiky, jejichž účelem je přiblížit závažnost a reálné dopady podceňování bezpečnosti používání Internetu.

Klíčová slova: informační a komunikační technologie, počítačová kriminalita, Internet, zabezpečení dat, bezpečné chování, bezpečnostní software, přenos dat, vývoj kriminality, kazuistika, pravidla bezpečného chování

Summary

This diploma thesis deals with cybercrime in the Czech Republic. The main objective is to find the connection between the increase of cybercrime and the behavior of Internet users.

It comprises a basic overview of some of the most common areas of criminal activities. It also introduces a brief history of technologies and first manifestations of related criminal activity. In the main part, which is behavior analysis, based on empirical research. This research is focused on using commercially available security resources and knowledge of some important elements of Internet communication. For related questions it detects dependence of the results. The empirical part follows the current course and amount of cyber crime cases in the Czech Republic and then with use of statistical method estimates its following course.

The findings of the empirical part is further summarized in the final section and after the weaknesses of Czech user base are identified it proposes measures that may be successful in mitigation of cyber criminality.

Throughtout the work there are examples from case studies designed to ephasize the seriousness and real impacts of underestimating the safety rules for Internet users.

Keywords: Information and communications technology, Computer crime, Internet, Data security, Safe demeanour, Security software, Data transfer, Crime rate, Casuistry, Safe demeanour rules

Obsah

1. Úvod

Mezi fenomény současné doby lze jednoznačně zařadit informační technologie. Jen málokterý technický směr našel své uplatnění tak rychle a masově jako právě tyto technologie. To je způsobeno především širokou možností jejich využití a mírou zefektivnění oblastí, které posunuly dopředu za krátké období oproti předchozím snahám. V poslední době slouží stále více také k zábavě lidí. Dalším zásadním milníkem bylo vynalezení Internetu, který k výše popisovanému masovému rozšíření značnou měrou přispěl. Vědečtí pracovníci, kterým se v laboratořích podařilo přimět dva počítače ke komunikaci, jistě nečekali, že se výsledek jejich práce během několika málo let promění v neuvěřitelnou globální záležitost propojující zařízení i v těch nejzazších koutech světa, a že stojí u zrodu jednoho z největších a nejpřínosnějších vynálezů poslední doby.

Není cílem této práce popisovat všechny možnosti, které dnes informační technologie a Internet nabízí. Jejich každodenní využívání se stalo součástí našich životů. Možnosti tohoto využití jsou většině moderní populace známy a nemalá část je i využívá. V dnešní době téměř již zapomínáme, že Internet nebyl vždy samozřejmostí. Proto je vhodné uvést několik základních změn, díky kterým došlo z pohledu lidstva k podstatným zásahům do jeho života. V této souvislosti se hojně setkáváme s termínem Informační společnost. IT a Internet tedy především zásadně změnily přístup běžných lidí k informacím, což umožnilo rychlejší vývoj celé společnosti. Porovnáme-li přístup k informacím v době před půl stoletím a dříve s tím dnešním, povšimneme si zásadního rozdílu, který se zdá být díky naprosto samozřejmému každodennímu využívání Internetu téměř neuvěřitelný. Přístup k literatuře byl pro běžného člověka ve vzdálenější minulosti značně omezen. Protože písemné informace byly přístupné pouze úzkému okruhu převážně městské populace, k předávání informací docházelo především z generace na generaci. Tímto způsobem neměla společnost možnost být opravdu dobře informována. K tomu lze do kontrastu postavit dnešní, i díky Internetu globální svět, kdy stačí k vyhledání a seznámení se s často i několik minut čerstvými informacemi doslova pár vteřin.

Díky masovému rozšíření dostupnosti informací ale nutně přicházejí i rizika, která mohou vést ke zneužití informací. Na tato rizika je nutné reagovat zodpovědným chováním, kterému je právě tato práce věnována. Přínos provázanosti moderní společnosti s technologiemi se může při nezodpovědném chování přeměnit v problémy, osobní

tragédie či dokonce katastrofy. Přestože je bezpečnosti věnována poměrně značná mediální pozornost, stále se dozvídáme o nových a nových případech zneužívání technologií.

Tato práce má za úkol na základě prozkoumání chování uživatelů odhalit příčiny, proč ke zneužívání opětovně dochází. Následně s přispěním kazuistiky policejní praxe pak zjišťuje způsoby, jak ke zneužívání dochází a vyvozuje možnosti, jak těmto případům předcházet, či alespoň jejich účinky omezit. Stále četnější informace o nárůstu počítačové kriminality a škod jí způsobených nás vedou k domněnce, že schopnost reagovat na hrozby počítačové kriminality stále více zaostává za snahou zločinců tuto kriminalitu páchat. Počet kroků, o něž jsou pachatelé před obrannými mechanismy, se stále zvyšuje. Chování uživatelů proto souvisí s mapováním trendu počítačové kriminality a stává se tak její součástí.

Práce je rozdělena do tří hlavních částí. První má uvést čtenáře do problematiky počítačové kriminality z hlediska oblastí, které jsou s běžným užíváním Internetu nejčastěji spojeny. Dále pak provede stručné seznámení s historií technických prostředků doprovázené popisem prvních projevů počítačové kriminality.

Následuje empirická část, která se zabývá výsledky provedeného výzkumu mapujícího úroveň bezpečnosti chování uživatelů Internetu, včetně aplikace statistických metod na zjištěné výsledky, doprovázené krátkými komentáři.

Třetí část pak sumarizuje skutečnosti zjištěné v empirické části a pokouší se zformulovat doporučení v reakci na odhalené nedostatky v bezpečném chování.

2. Cíl práce a metodika

Nežádoucí zneužívání informačních technologií pro napadání uživatelů je součástí běžného života, kterou nelze zcela eliminovat. Jak uvede následující kapitola, vývoj technologií je těmito nežádoucími jevy doprovázen prakticky od svého vzniku. Vynalézavost útočníků nezná mezí a nezbývá, než se jejich útokům bránit. Každý posun ve vývoji technologií kromě své užitné hodnoty nabízí i nové příležitosti útočníkům a tak je nutné investovat čas i peníze do obrany. To se ve skutečnosti samozřejmě děje a tyto snahy tvoří samostatnou oblast vývoje, na které se podílí množství firem i jednotlivců. Dá se říci, že tvoří samostatný obor v oblasti informačních a komunikačních technologií. Stejně jako jakýkoliv obor, je i tento odkázán na schopnost a ochotu jej aplikovat uživateli, a to především aplikovat účinně. To vyžaduje orientaci v problematice a povědomí o možnostech obrany.

Literatury, která se zabývá vytvořením přehledu počítačové kriminality rozřazením do skupin je mnoho a účel této práce není ji rozšiřovat. Snaží se poukázat na ty nejčastější, zasazené do konkrétního uživatelského prostředí. Cílem práce je tedy s využitím provedeného empirického výzkumu, vlastních zdrojů zkoumání a získaných údajů z jiných kriminalistických pracovišť, analyzovat běžné chování uživatelů výpočetní a komunikační techniky, odhalit jeho slabá místa a identifikovat příčiny chování, které mají za následek uživatele Internetu jako oběti trestné činnosti. Práce se snaží analyzovat především chování uživatelů, jejichž vybraný vzorek v sobě zahrnuje běžnou skladbu úrovně počítačové gramotnosti, tzn. od uživatelů Internetu spíše podprůměrných znalostí výpočetní a komunikační techniky, přes nejhojněji zastoupenou skupinu běžných uživatelů s povědomím o užívaných standardech v oblasti informačních technologií až po reprezentanty odborné veřejnosti. Vzorek byl pořízen v prostředí, u něhož lze předpokládat skladbu obdobnou většinové ekonomicky aktivní populaci.

Samotný empirický výzkum byl proveden formou kvantitativního dotazníkového výzkumu na vzorku 152 respondentů, kterým byl předložen dotazník s 18 otázkami, uvedenými v příloze této práce. Otázky byly sestaveny na základě řešené problematiky v oblasti bezpečnosti chování běžných uživatelů Internetu. Byly kladeny především ve spojitosti s prostředky, jejichž užívání lze v současné době pokládat za běžné nebo je jejich existence většině běžných uživatelů Internetu známá. Respondenti byli ze skupiny

o věkovém rozmezí 21 - 60 let v rozsahu vzdělání středoškolského s maturitou až vysokoškolského. Výběr takovéto skupiny vycházel kromě její dostupnosti i z předpokladu, že jakožto aktivní uživatel výpočetní techniky v zaměstnání je uživatelem informačních technologií i v soukromém životě a tudíž je vysoká pravděpodobnost porozumění otázkám v dotazníku.

Respondenti byli instruováni, že otázky jsou zaměřené na bezpečnost používání soukromých zařízení a tedy se na služební telefony či počítači nevztahují. Tím mělo být docíleno zmapování přístrojů, nad jejichž nastavením a provozem mají plnou moc. Ti, kteří nemají vlastní počítač nebo mobilní telefon, byli z průzkumu vyřazeni.

Otázky byly formulovány tak, aby vyčerpávajícím způsobem umožnily zmapovat běžné chování uživatelů při používání technologií s Internetem. Převážně se dotazují na technické prostředky, běžně používané jak k připojení, tak k samotnému užívání. Nad rámec tématu byla položena otázka na kurzy a školení v oblasti bezpečnosti, aby bylo možné potvrdit či vyvrátit domněnku o nedostatečném systému vzdělávání v této oblasti.

Výsledky byly zpracovány v tabulkovém procesoru, odpovědi byly procentuálně vyhodnoceny a pro potřeby nalezení vícenásobné shody souvisejících ukazatelů byla použita odpovídající funkce, vracející počet záznamů vyhovujících více kritériím současně. Z těch byly dále vytvořeny kontingenční tabulky a vypočítány síly závislosti mezi jednotlivými aspekty chování. Ostatní odpovědi jsou popsány základními popisnými charakteristikami ve formě grafického vyjádření absolutních a relativních četností, doprovázenými komentáři.

Z výsledků tohoto průzkumu se pak pokusíme nalézt souvislosti a z nich vyvodit závěry a doporučení, které by mohly úspěšnost útočníků při jejich snahách zkomplikovat, případně dopady jejich pokusů alespoň zmírnit.

Pohybuji se v prostřední komunity zabývající se odhalováním počítačové kriminality i dalších trestných činů, které jsou technologiemi doprovázeny. Konkrétně se jedná o znalecké pracoviště Vojenské policie, jehož jsem zaměstnancem. Díky tomu mohu použít data jak z vlastní práce, tak i policejních útvarů, které se touto činností zabývají. S pomocí jejich i vlastních dat budou vytvořeny statistiky o změnách počtu řešených případů v oblasti informačních technologií i poznatky v oblasti zabezpečení zkoumaných

elektronických zařízení. Z těchto podkladů vytvoříme přehledný grafický trend v této oblasti a statistickou metodou časových řad odhadnout další vývoj.

Pro bližší znázornění problematiky pak budou některá témata doplněna případy z kazuistiky. Ty mají za cíl přiblížit skutečné dopady především uživatelům, kteří zabezpečení svých přístrojů podceňují. Mají též čtenáři ukázat, jak jednoduše se může stát terčem kybernetického kriminálního činu v případě své neobezřetnosti a jaké mohou mít takové útoky následky.

3. Přehled řešené problematiky

3.1. Terminologie a názvosloví

Aby bylo možné se tímto tématem zabývat, je vhodné provést stručné seznámení s některým názvoslovím, zjednodušenými principy fungování vybraných informačních technologií, celosvětovou sítí Internet atd. Do tématu počítačové kriminality je vhodné zahrnout i historii technologií, ve které můžeme spatřovat pokusy o elektronickou kriminalitu, pevně spojené s jejím vývojem. Protože se nejedná o práci technického zaměření, jsou zde zmíněny jen nejvýznamnější milníky a velice letmé seznámení s vybranými základními principy a to především ve vztahu k tématu této práce. Vzhledem ke spojení technologií se současnou společností budou výrazy a termíny použité v práci mnohým potenciálním čtenářům již známy.

Informační technologie (IT) – výraz vyjadřující elektronické přístroje se schopností zpracovávat informace a provádět s nimi operace. Informační technologie používané pro komunikaci jsou označovány jako Informační a komunikační technologie (ICT). Komunikací myslíme v tomto případě především výměnu informací. V současné době je namístě i v souvislosti s počítačovou kriminalitou hovořit o ICT, protože informace a komunikace jsou velmi úzce spjaty a samostatná elektronická zařízení, která nejsou s okolím nijak propojena, se stávají spíše okrajovou záležitostí. Mezi ICT tak lze kromě počítačů připojených k Internetu či jiné síti a chytrých mobilních telefonů, zařadit i klasické mobilní telefony, fungující v digitálních sítích. Při komunikaci v síti totiž dochází k výměně mnoha informací (například identifikace zařízení nebo informace o poloze vůči vysílači) a služby jako je hovor nebo SMS v digitální síti není nic jiného než přenos digitálních dat.

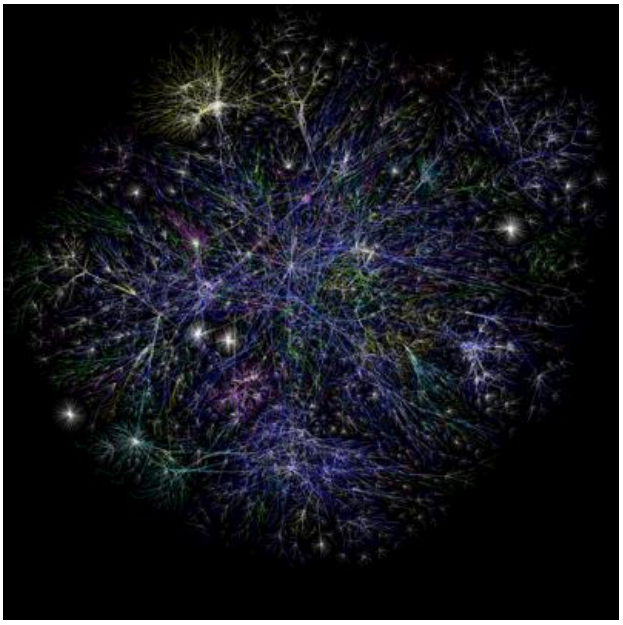
Provázanost lidské činnosti s ICT je často vyjádřena termínem Informační společnost. Jedná se o *„Společnost založenou na integraci informačních a komunikačních technologií do všech oblastí společenského života v takové míře, že zásadně mění společenské vztahy a procesy. Nárůst informačních zdrojů a komunikačních toků vzrůstá do té míry, že ho nelze zvládat dosavadními informačními a komunikačními*

technologiemi.“[1] Tento termín zahrnuje všechny vyspělé státy světa včetně České republiky a ve většině rozvojových zemí můžeme směřování k informační společnosti pozorovat téměř v přímém přenosu. Zde je vhodné podotknout, že pozorovat výše zmíněné směřování můžeme právě proto, že již součástí informační společnosti jsme. Informační společnost přináší v mnohých oblastech zkvalitnění života. Mezi nejvýznamnější přínosy patří efektivita trhu, který je díky rychlým odezvám a jednoduššímu mapování potřeb zákazníků schopen reagovat přímo na subjektivní potřeby zákazníka, zjednodušuje firmám organizaci a řízení, efektivnější reklamu a přímé propojení se zákazníkem atd. Jednotlivci pak umožňuje pomocí elektronické komunikace a digitálních formulářů rychleji jednat s úřady, využívat výše uvedených výhod digitálního trhu a ušetřit tak volný čas, který může zajímavěji zužitkovat díky větší informovanosti o možných volnočasových aktivitách. Nebo může své schopnosti využít jinak, protože *„Informatizace společnosti velmi výrazně zvětšuje objem potenciálních informací. Umožňuje vytvářet na stále větších plochách obrovské, dříve netušené zásobárny zaznamenaných znalostí a zkušeností, stále většími rychlostmi je podle předem stanovených hledisek třídit a vyvolávat z nich ty, o nichž se domníváme, že je potřebujeme.“*[2] To nám umožňuje zvyšovat efektivitu práce jak v profesionální oblasti, tak mimo ni.

Jedním z podstatných prostředků umožňující stupeň integrace informační společnosti je Internet. Jedná se o unikátní systém propojených jednotek pomocí uzlů (zařízení) do celosvětového systému, ve kterém má každá jednotka svůj specifický název (IP adresu). Z důvodu uživatelské přívětivosti jsou tyto adresy vyjadřovány adresami slovními, které jsou při zadání uživatelem pomocí DNS[3] překládány zpět do adres specifických číselných. Jedná se o decentralizovaný systém, díky čemuž je eliminována centrální zranitelnost. Samotný výraz Internet vyjadřuje síť umožňující komunikaci mezi členy prostřednictvím protokolů. Tyto protokoly jsou využívání pro služby fungující na Internetu jako je elektronická pošta, WWW stránky (multimediální obsah), přenosy souborů atd.

---

[1] JONÁK, Z., *Informační společnost*. [on-line], dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000468&local_base=KTD.
[2] CEJPEK, J., *Informace, komunikace a myšlení…*, s. 106
[3] Domain Name System – systém doménových jmen, jehož úkolem je převádět doménová jména na IP adresy – JIRÁSEK, P., NOVÁK, L., POŽÁR, J., *Výkladový slovník kybernetické bezpečnosti,* s. 25-26



Obr. č. 1 - Grafické znázornění části Internetu.[4]

Budeme-li se zabývat počítačovou kriminalitou, pro kterou lze použít i výraz kybernetická kriminalita, je vhodné popsat, co je kyberprostor. Jedná se o termín bezprostředně spojený se sítí Internet. Ten díky své podstatě vytváří dynamický systém vázaný na hardware, avšak vytvářející těžko definovatelný a prakticky neomezený kyberprostor – jedná se tedy o virtuální realitu, nemající konec ani začátek.[5]

3.2. Počítačová kriminalita

Existuje mnoho definic počítačové kriminality, ze všech lze ale odvodit jakousi střední variantu a tou je označení pro trestné činy páchané pomocí ICT či přímo proti ICT zaměřené. Technologie umožňují jak nové typy trestných činů, tak především ulehčují či zdokonalují tradiční činy, které zároveň jsou, či spíše byly páchány v minulosti složitějším způsobem.[6] Typickým příkladem je falšování dokladů, písemností a cenin. Specifikem počítačové trestné činnosti je i absence některých prvků klasické kriminality jako je násilí, ohrožení zdraví, či použití zbraně. Dalším specifikem jsou značné újmy ve formě

[4] THE OPTE PROJECT, *The Internet,* [on-line], dostupné z http://www.opte.org/maps/
[5] KOLOUCH, J., VOLEVECKÝ, P., *Trestněprávní ochrana před kybernetickou kriminalitou*, s. 13
[6] MATĚJKA, M., *Počítačová kriminalita*, s. 6

peněžních škod nebo zneužití osobních informací.[7] EUROPOL pak počítačovou kriminalitu rozděluje na:[8]

1) útoky proti počítačovému hardwaru a softwaru (například botnety, malware, narušení sítě),
2) finanční kriminální činy (on-line podvod, on-line vniknutí do finančních služeb, phishing),
3) zneužití (týká se především mladých lidí – falšování identity, pornografie).

V České republice byla počítačová kriminalita podle definice starého trestního zákona č. 140/1961 Sb. velmi strohá. Celou problematiku shrnovala do paragrafu 257 a):

(1) Kdo získá přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch

a) takových informací neoprávněně užije,

b) informace zničí, poškodí, změní nebo učiní neupotřebitelnými, nebo

c) učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení,

bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.

Tato formulace je ve vztahu k roku účinnosti trestního zákona pochopitelná, avšak vzhledem k absenci novelizací a současnému stavu dění ve světě informačních technologií silně nedostačující. Při tvorbě nového trestního zákoníku č. 40/2009 byla tato oblast zahrnuta v širším záběru. Pro přehled si uvedeme nejdůležitější paragrafy, které se počítačovou kriminalitou zabývají v současně platném zákonném předpise s jejich popisem, majícím charakterizovat postižitelné skutky počítačové kriminality:[9]

§ 182 Porušení tajemství dopravovaných zpráv

Jedná o rozšíření listovního tajemství o zprávy, obsahující digitální data a to jak ve formě datových, textových, hlasových, zvukových či obrazových zpráv, posílaných

[7] POŽÁR, J., KALAMÁR, Š., POKORNÝ, V. *Základy teorie informační bezpečnosti*, s. 129-130
[8] INTERPOL, *Cybercrime*, [on-line], dostupné z: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
[9] Trestní zákoník (Zákon č. 40/2009 Sb.)

prostřednictvím sítě elektronických komunikací (odst. 1 b)), tak o formulaci trestnosti porušení tajemství neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího počítačová data (odst. 1 c))

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

Tento paragraf se zabývá přístupem k počítačovému systému nebo k jeho části překonáváním bezpečnostních opatření, čímž tuto činnost kvalifikuje jako přečin i bez spáchání dalších škod. Tím mění i přístup k počítačové kriminalitě, který byl uveden ve starém trestním zákoně, který definoval trestnou činnosti pouze ve spojení se zneužitím dat nebo způsobenými škodami, vyplývajících z jejich získání (odst. 1). Další odstavec se zabývá neoprávněným užitím, smazáním, změnou či jiným poškozením dat, dále padělaním, neoprávněným vložením, zásahem do programového a technického vybavení atd.

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

Tento paragraf řeší mimo jiné častou kriminalitu ve formě snah o získání přístupu do počítačových systémů. Lze jím obsáhnout velmi častý výskyt podvodných e-mailových zpráv, vytvořených právě za účelem vylákání citlivých, nejen přístupových údajů. Kromě získání postihuje i další nakládání s těmito údaji jako je uvedení do oběhu, dovoz/vývoz, nabízení, zprostředkování, prodej, přechovávání atd. Kromě přístupových údajů se zabývá i vlastnictvím nástrojů a prostředků, které k tomuto účelu slouží. Jinými slovy lze aplikovat i na škodlivé kódy, aplikace, prolamovače hesel apod.

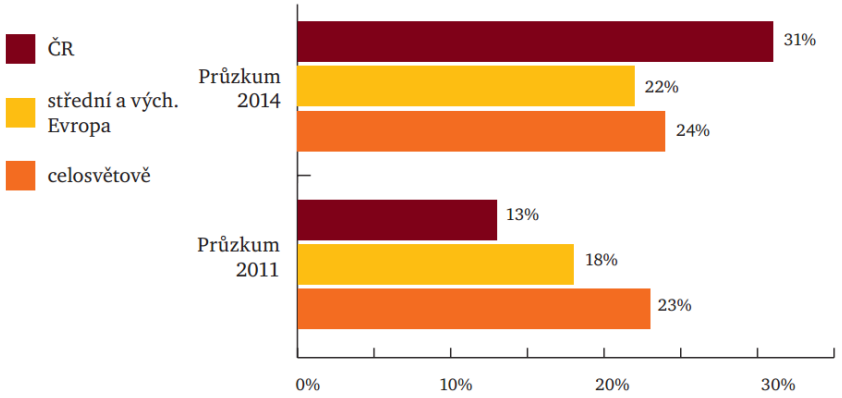
§ 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

Paragraf pro činy z nedbalosti, z porušení povinnosti, postavení nebo funkce, vyplývající ze zákona nebo smluvně převzaté.

§ 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi

Tento paragraf není vztažen přímo na počítačovou kriminalitu a řeší porušování autorského práva obecně. S ohledem na skutečnost, že toto porušování je především

doménou Internetu, je vhodné jej do výčtu uvést. Dalším argumentem pro uvedení je i vysoká četnost využívání znaleckých pracovišť pro prověřování této trestné činnosti. Analogicky to platí i pro ustanovení o výrobě, držení a distribuci dětské pornografie a dalších obdobných trestných činů. Neméně důležitým paragrafem, často uváděným v souvislosti s počítačovou kriminalitou, je podvod. Podíl jeho spáchání v počítačové formě narůstá a tento podíl je v České republice ve srovnání s okolním světem vyšší. I to je signál ke zvýšení pozornosti věnované bezpečnému používání ICT.



Graf č. 1 - Podíl počítačové kriminality na spáchaných podvodech.[10]

Řešení na úrovni legislativy jednotlivých států se vzhledem k jejímu častému mezinárodnímu charakteru ukazuje jako silně nedostačující a nekompatibilní a tak vyvstala potřeba řešit počítačovou kriminalitu na vyšší úrovni a podpořit mezinárodní spolupráci. Z nám blízkého prostředí i vzhledem k implementaci mezinárodního práva do právních norem ČR přísluší především úroveň Evropské unie.

Rada Evropy a další státy, které podepsaly Úmluvu o počítačové kriminalitě v Budapešti dne 23.11.2001 dělí dle prvního oddílu boj s kriminalitou do čtyř oblastí[11], které mají být přijaty na vnitrostátní úrovni:

1) Trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů (nezákonný přístup, odposlech, zasahování do dat a systémů, zneužívání zařízení).
2) Trestné činy vztahující se k počítači.

[10] PWC, *Celosvětový průzkum hospodářské kriminality 2014,* [on-line], dostupné z: http://www.pwc.com/cz/cs/hospodarska-kriminalita/assets/pdf/global-economic-crime-survey-2014-cz.pdf
[11] COUNCIL OF EUROPE. *Convention on Cybercrime,* [on-line], dostupné z: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

3) Trestné činy se vztahem k obsahu počítače.
4) Trestné činy porušování autorského práva a souvisejících práv spáchané s využitím počítače.

V druhé oblasti trestné činy související s počítačem rozděluje na počítačové padělání a počítačový podvod. Třetí část je věnována dětské pornografii a další pojednává o porušování autorského práva. Následující části se zabývají praktickým prováděním boje proti počítačové kriminalitě.

Dne 28.1.2003 byla úmluva doplněna o dodatek k Úmluvě o počítačové kriminalitě, týkající se kriminalizace činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů.[12]

Cílem úmluvy je sjednotit legislativu signatářských zemí v boji proti počítačové kriminalitě tak, aby bylo možné přeshraniční aktivitu efektivně stíhat. Výše uvedené paragrafy z nového trestního zákoníku České republiky jsou výsledkem implementace této dohody.

Toto byl přehled počítačové kriminality z pohledu litery zákona a mezinárodních úmluv. Nyní se podíváme na počítačovou kriminalitu očima praktického provozování této činnosti. V následujících podkapitolách si představíme nejčastější projevy počítačové kriminality z praktického hlediska.

3.2.1. Nevyžádaná pošta (spam) a phishing

Nevyžádaná pošta se stala součástí používání e-mailových schránek natolik, že ji mnoho lidí za typ počítačové kriminality ani nepokládá. Při tom je třeba si uvědomit, že existují zákony na obranu proti takovéto činnosti a tudíž je legislativa ve většině případů porušována. Často se setkáváme s případy, kdy po nákupu v internetovém obchodě přicházejí nabídky i přesto, že jsme zasílání informačních e-mailů při objednávce nezaškrtli. V obchodních podmínkách, jejichž odsouhlasení podmiňuje provedení nákupu, je však zpravidla obsažen souhlas se zpracováním osobních údajů pro marketingové účely, čímž je myšleno i další nakládání s e-mailovou adresou, včetně jejího šíření ostatním

[12] COUNCIL OF EUROPE. *Additional Protocol to the Convention on Cybercrime*, [on-line], dostupné z: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

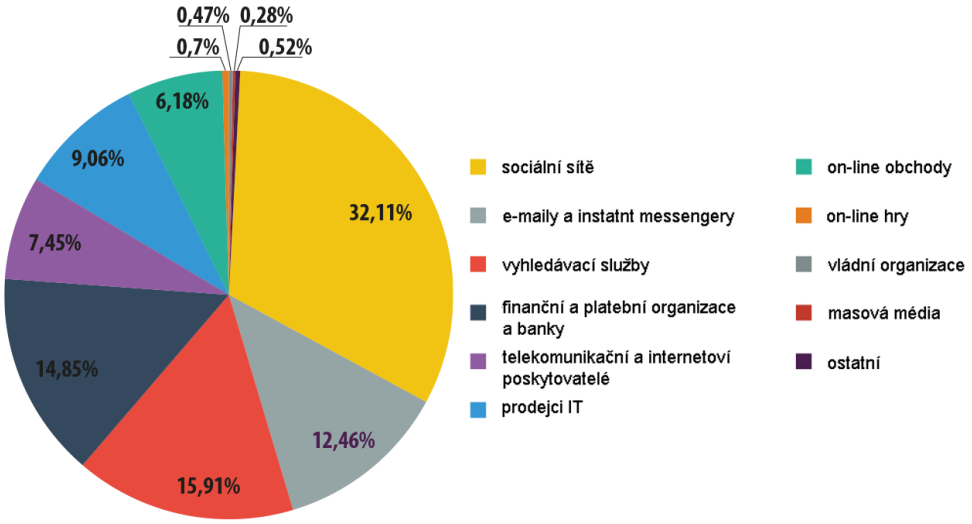
prodejcům. Vždy ale existuje možnost se ze seznamu adresátů reklamních nabídek odhlásit a to buď pomocí odkazu přímo v nabídkovém materiálu, nebo písemnou formou. Jsou-li nabídky zasílány i nadále, je to důvod k řešení prostřednictvím úřední moci. Vlastník e-mailové schránky je sice obtěžován odhlašováním se z databází prodejců dalších e-shopů, které si mezi sebou e-mailové adresy předávají, ale neobdrží-li reklamu i po odhlášení, k porušení žádných předpisů nedochází.

Složitější situací je spam v případě, kdy není znám odesílatel. V takovém případě se není kde ze zasílání spamu odhlásit. Jedná se především o nevyžádanou poštu ze zahraničí.[13] Lze jen ovlivnit šíření vlastní e-mailové adresy.

V reakci na to byly vyvinuty různé systémy, které se snaží nevyžádanou poštu filtrovat a eliminovat tak čas, který musí uživatel schránky třídění a mazání této pošty věnovat. V celosvětovém měřítku se tento strávený čas vyměřuje i jako škoda vyčíslená penězi[14]. Spamové filtry jsou různé kvality, pracují s různou měrou úspěšnosti filtrování a nelze se na ně plně spolehnout. V praxi tak třídění spamu, či alespoň kontrola e-mailů označených jako spam, uživateli vždy nějaký čas zabere.[15]

Nyní se však dostáváme k mnohem zákeřnější formě internetové kriminality a tou jsou phishingové zprávy. Jedná se o podvodné zprávy, které mají za účel vylákat z oběti citlivá data nebo přihlašovací údaje do různých služeb či stránek.[16] Nejčastěji jde šiřitelům phishingových zpráv o přístup k přihlašovacím údajům do internetového bankovnictví nebo údaje o platebních kartách. V případě získání těchto údajů dochází k největším škodám. Na následujícím grafu můžeme vidět procentuální zastoupení adresátů phishingu:

[13] ADÁMEK, M., *Spam – jak nepřivolávat, nepřijímat a nerozesílat nevyžádanou poštu,* s. 16
[14] MUSIL, J., *Elektronická média v informační společnosti*, s. 177
[15] ADÁMEK, M., *Spam – jak nepřivolávat, nepřijímat a nerozesílat nevyžádanou poštu,* s. 80-83
[16] KOLOUCH, J., VOLECECKÝ, P., *Trestněprávní ochrana před kybernetickou kriminalitou*, s. 37



Graf č. 2 - Cíle odesílatelů phishingu.[17]

Spam skrývá i další rizika, která hrozí v případě chybného nakládání uživatelem. Přílohy zpráv mohou obsahovat nejrůznější škodlivé kódy nebo viry, které mohou po instalaci představovat infiltrace, změny systému apod.

Spam je globálně nejrozšířenější forma počítačové kriminality. Z celosvětových statistik vyplývá, že cca 70 % veškeré e-mailové komunikace představuje v dlouhodobém průměru právě nevyžádaná pošta.

3.2.2. Porušování autorského práva

Předem je třeba říci, že na Internetu v tomto směru neplatí žádné zvláštní zákony a jedná se tak o porušení obecně platných norem.[18] Jedná se však o činnost, na které se podílí, či přesněji řečeno jí podporuje, pravděpodobně největší počet uživatelů výpočetní techniky. Po multimediálním obsahu nebo softwaru, jehož sdílení nebo upravování představuje porušování autorského práva (v počítačovém slangu označováno jako „warez“) a které je trestným činem, je totiž velká poptávka. Instituce na obranu autorského práva se

[17] KASPERSKY SECURITY BULLETIN, *Spam evolution 2013*, [on-line], dostupné z: http://media.kaspersky.com/pdf/LK_KSB_2013_spam_EN.pdf
[18] SMEJKAL, V., *Internet a §§§*, s.32

touto problematikou intenzivně zabývají, najímají si odborníky, kteří vyhledávají na Internetu osoby, sdílející chráněná data. Následně podávají trestní oznámení, ve kterých se snaží vyčíslit škody sdílením způsobené. Mezi nejčastější způsoby, kterými k šíření takového obsahu dochází, je ukládání chráněných souborů na webová úložiště. Jejich uživatelé chráněný obsah nahrají a další si jej stahují. Mezi neznámější úložiště patří mediálně známý Megaupload.com, který byl v lednu 2012 kvůli šíření souborů chráněných autorským právem zablokován, jeho majitel zatčen a obviněn ze způsobení škody na půl miliardy amerických dolarů. Úložišť, která se se sdílením chráněného obsahu potýkají, je po celém světě nespočet. Jedním z takových známých českých serverů je například Uloz.to. Společným znakem takovýchto úložišť je zřeknutí se odpovědnosti za vložený obsah v podmínkách použití a deklarace snahy závadný obsah mazat. Zodpovědnost za porušování autorského práva je pak plně delegována na uživatele, kteří server používají. Míra skutečné snahy je však různá a lze spekulovat nad jejím praktickým plněním. Servery, které jsou svým atraktivním, byť nelegálním obsahem známy, tím de facto svou atraktivitu snižují a připravují se tak o zisky. To dokládají neustálé kritické články a vyjádření na adresy těchto serverů. Vyhledávání uživatelů, kteří chráněný obsah vkládají a tím autorské právo porušují, je komplikováno mezičlánkem v podobě provozovatelů těchto serverů a jejich odhalení je závislé na jejich spolupráci. Na tu lze spekulativní teorie o snižování atraktivity aplikovat též.

Dalším velmi populárním způsobem šíření chráněných dat jsou sítě Peer-to-Peer (P2P). Principem této sítě je přímá výměna dat uživateli. Ti používají software (tzv. klienty), ve kterém jsou propojování pomocí serverů (nazývanými Huby), ale skutečný předmět výměny se nachází přímo v počítačích uživatelů a přečinu porušování autorského práva se tak v tomto případě dopouštějí všichni uživatelé, kteří takovou aktivitu provozují. Tento způsob prošel vývojem, který zvýšil efektivitu stahování a vyústil ve dva nejčastěji používané způsoby. V prvním, starším případě, je nutno dát určité množství dat k dispozici ostatním uživatelům ze svého počítače proto, aby bylo možné stahovat obsah od ostatních a efektivita sítě a objem dat se tím zvýšil. Tento případ je z pohledu odhalování této trestné činnosti nejjednodušší. To vědí i společnosti zabývající se ochranou autorského práva a pro odhalování této činnosti jej hojně využívají. Druhým, vývojově mladším způsobem, jsou tzv. torrenty. Jsou to malé soubory nesoucí informaci o požadovaném souboru, stažitelné z torrentových vyhledávačů. Ten uživatele odkáže na server (tracker), který sice

neobsahuje požadovaný soubor, ale má informaci o ostatních uživatelích, kteří soubor nebo jeho části vlastní a zprostředkuje připojení k nim. Následuje stahování souboru po částech od různých zdrojů (tzv. segmentové stahování). Každý takový segment, jehož stažení je dokončeno, je automaticky dán k dispozici ostatním uživatelům.[19] Díky tomu se množství zdrojů zvyšuje a stahování se stává efektivnějším, protože na rozdíl od webových úložišť, ze kterých stahuje mnoho uživatelů najednou, dochází k rozdělení zátěže a nároku na rychlost připojení mezi mnoho uživatelů. Z tohoto principu pak vyplývá, že čím je soubor žádanější, tím víc zdrojů segmentů je k dispozici a stahování je rychlejší. Oba popsané principy sítí P2P jsou na odhalování pachatelů poměrně jednoduché, protože klientské aplikace umožňují zjistit IP adresu uživatele, který dává sdílený obsah k dispozici. Následuje už jen identifikace uživatele podle IP adresy a trestní řízení může být spuštěno. Nutno dodat, že sdílení prostřednictvím sítí P2P je často využíváno i k distribuci softwarů, které nepodléhají autorskému zákonu, ale mají velký datový objem (například volné distribuce operačního systému Linux). Nejčastěji jsou však známy právě v souvislosti šířením chráněného obsahu.

3.2.3. Infiltrace do cizího systému

Dalším častým kriminálním činem bývá proniknutí nebo snaha o proniknutí do privátních sítí, případně uzavřených počítačových systémů, doprovázená krádeží informací nebo jejich vědomé poškozování, změna či mazání. Tomu zpravidla předchází prolomení hesla. Nejjednodušší způsob je samozřejmě zjištění přístupových údajů pomocí prozrazení nebo neopatrnému zacházení vlastníka nebo použití počítače, kde uživatel zanechal neodhlášený účet. Není-li heslo známo, existuje několik metod k jeho prolomení. Mezi nejpoužívanější patří Brute Force Attack (hrubou silou), kdy jsou postupně zkoušeny kombinací znaků tak dlouho, dokud není heslo uhodnuto. Tento způsob je prováděn prostřednictvím programů. Čím je heslo kvalitnější, tedy složitější, tím trvá prolomení hesla déle. Další možností je tzv. slovníkový útok. Princip zkoušení správného hesla je stejný, znaky ale nejsou voleny náhodně nebo pomocí systematických kombinací, ale pomocí známých výrazů, u kterých je předpoklad, že jsou v heslu obsažené. Tyto dva

[19] PETROWSKI, T., *Bezpečí na Internetu pro všechny,* s. 55-58

způsoby je možno kombinovat. Obranou proti těmto útokům je použití dlouhého hesla, které nedává žádný smysl, ideálně ještě v kombinace se speciálními znaky, velkými a malými písmeny a čísly. Heslo je samozřejmě vhodné často měnit. Ve skutečnosti se tomu tak zpravidla neděje. V roce 2013 unikla ze společnosti Adobe databáze 130 milionů uživatelů, z níž se hackerům podařilo zjistit mimo jiné jejich přihlašovací hesla. Vznikla tak nejrozsáhlejší databáze hesel právě z takto kvalitního vzorku. Z té vyplynula následující tabulka těch nejčastějších[20]:

Poř. č.	Počet uživatelů	Heslo
1	1911938	123456
2	446162	123456789
3	345834	password
4	211659	adobe123
5	201580	12345678
6	130832	qwerty
7	124253	1234567
8	113884	111111
9	83411	photoshop
10	82694	123123
11	76910	1234567890
12	76186	000000
13	70791	abc123
14	61453	1234
15	56744	adobe1

Tab. č. 1 - Nejčastější hesla.

Jak můžeme vidět, téměř dva miliony uživatelů mělo heslo „123456“. I z dalších uniklých dat serverů IEEE.org (100 tis. vzorků) či z hacku RockYou.com (32 milionů vzorků) vyšlo jako nepoužívanější totéž heslo.[21]

Velmi nebezpečným způsobem je monitorování činnosti uživatele pomocí malware, což je software, který je vpraven do počítače prostřednictvím viru a odesílá

[20] SCG, *Top 100 Adobe Passwords with Count* [on-line], dostupné z: http://stricture-group.com/files/adobe-top100.txt

[21] DOČEKAL, D., *Adobe unikly údaje 130 miliónů uživatelů,* [on-line], dostupné z: http://www.lupa.cz/clanky/ze-130-milionu-uzivatelu-adobe-melo-heslo-123456-skoro-dva-miliony/

informace o činnosti uživatele útočníkovi prostřednictvím Internetu. Tímto způsobem může útočník zjistit kompletní přihlašovací údaje do sítí i používaných aplikací, včetně bankovních. Stejně jako u ostatních virů je včasné odhalení závislé na antivirových programech, lépe pak komplexních zabezpečovacích softwarech. Dalším způsobem odhalení přihlašovacího hesla je odposlech síťové komunikace. K tomu dochází při používání nezabezpečených webových stránek. Při komunikaci se stránkami, které nepoužívají zabezpečené protokoly (HTTPS), ji lze rozpoznávat třetí stranou. Některé webové prohlížeče na tuto skutečnost i upozorňují. Proto by uživatel, který svěřuje svá citlivá data nebo prostředky, měl sledovat, zda jím používaná stránka zabezpečený přenos používá. To lze zjistit jednoduchým způsobem v prohlížeči, konkrétně v jeho adresovém řádku.

3.2.4. Viry a škodlivé kódy

Jedná se o malé škodlivé programy, jejichž účelem je především množení efektivním šířením a další aktivita v počítačovém systému. Aby toho bylo možné dosáhnout, musí šíření probíhat co nejméně nápadným způsobem. Právě tato schopnost se dá pokládat za příměr kvality viru. Velmi často se tak viry snaží napadnout jiné aplikace a stát se tak jejich součástí.[22] Nejčastěji k tomu dochází prostřednictvím výměnných médií, elektronické pošty a webových stránek. Další aktivita pak spočívá v poškozování uživatelů počítačů. V lehčích případech se jedná pouze o obtěžování uživatele ve formě zpomalení systému či přímo audiovizuálními projevy viru. V těch závažnější pak může jít o čtení a odesílání dat uživatele, zachytávání činnosti uživatele při používání počítače nebo o poškozování softwaru v počítači mající za následek znefunkčnění systému či dokonce ztrátu dat.

V případě kombinace používání kvalitního antivirového programu, rozmyslu při otevírání příloh v elektronické poště a dodržování alespoň minimální obezřetnosti při navštěvování podezřelých webových stránek, lze těmto útokům efektivně čelit. Na Internetu lze navíc nalézt mnoho nástrojů, které přímo závadný obsah vyhledávaných stránek kontrolují a i mnohé vyhledávací portály se z výsledků svého vyhledávání snaží

[22] POŽÁR, J., KALAMÁR, Š., POKORNÝ, V. *Základy teorie informační bezpečnosti*, s. 101

nebezpečné stránky odstraňovat. Existuje však mnoho webových stránek s velmi atraktivním obsahem, které jsou mnoha uživateli cíleně navštěvovány i s vědomím vysokého rizika pokusu o infikaci virem. V těchto případech je plně spoléháno na kvalitu antivirových programů.

Zde je nutno zmínit velice důležitou poznámku a tou je udržování aktuálnosti virových databází antivirových programů. Viry a škodlivé kódy jsou vyvíjeny doslova každou hodinou a tak je třeba na měnící se hrozby reagovat pružně. To lze z opačného pohledu pozorovat i právě na antivirových programech. U těch kvalitnějších a spolehlivějších lze pozorovat zmíněnou aktualizaci databází i několikrát denně.

V každém případě je nutné si uvědomit, že rozšiřování virových databází vychází z reakcí vývojářů antivirů na nově příchozí hrozby. V případě kvalitně připraveného útoku vedeného novým typem viru může mít i drobná prodleva v reakci vývojářů fatální důsledky.

3.2.5. Útoky na webové stránky

Principielně podobným činem, i když s jinou motivací, bývá napadání webových stránek a to zpravidla orgánů státní moci nebo velkých společností, které mají vysokou návštěvnost. Napadání spočívá v odstavení stránek, k čemuž bývají požity tzv. DoS útoky (Denial of Service), které spočívají v zasílání nadměrného množství požadavků na cílový server, a to v takovém objemu, že server není schopen kapacitně všem vyhovět a zahltí se. Účinnější variantou tohoto útoku je pak DDoS, což je distribuovaný útok, kdy jsou uvedené požadavky zasílány z více míst najednou.[23] Nad trestností tohoto způsobu se vedou polemiky, protože při něm nedochází ke znakům trestného činu podle § 230 odst. 2) písm. c) Trestního zákoníku[24].

[23] PETROWSKI, T., *Bezpečí na Internetu pro všechny,* s. 40

[24] § 230 odst. 2) písm. c) TrZ: „Kdo získá přístup k počítačovému systému nebo k nosiči informací a data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže, nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“

Jiný a bezesporu trestný způsob naplňující znaky výše zmíněného paragrafu je napadání stránek změnou jejich obsahu. Podaří-li se útočníkovi dostat k administraci stránek, může jejich obsah libovolně měnit. Toho bývá útočníky využíváno nejčastěji k vlastnímu zviditelnění nebo jako forma protestu.

Nutno dodat, že oba uvedené útoky jsou prováděny i legálně, a to na objednání firmami zabývajícími se tvorbou webových stránek. Firmy tímto způsobem testují kvalitu zabezpečení svých produktů, které posléze prodávají.

3.2.6. Bankovní krádeže

Další oblastí jsou bankovní krádeže. Stejně jako v případě krádeží a loupežných přepadení se zbraní v ruce jde o velice oblíbený cíl mnoha útočníků s vidinou velkého zisku, jako zbraň zde však slouží informační technologie. Z historie jsou známy mnohé případy odčerpávání peněz z bank pomocí ICT jejich zaměstnanci a to mnohdy velice úspěšně s dlouho prodlevou před dopadením. Nezřídka to bývají zaměstnanci IT oddělení, kteří mají přístupy do bankovních informačních systémů. Pro účel této práce jsou ale zajímavější krádeže peněz z bank útočníky zvenčí, kteří získali přihlašovací údaje klientů bank. Přestože se banky snaží proti takovým činům bránit nebo alespoň je komplikovat používáním vícefaktorové autentizace, účinně zamezit se jim stále nedaří. Způsobům překonávaní a jejich odhalování se budeme věnovat dále v empirické části práce.

Výrazem často spjatým s bankovními krádežemi je zmiňovaný phishing. Jedná o nástrahy na uživatele v podobě více či méně věrných kopií stránek, vyzývající k zadávání přihlašovacích údajů. Odkazy na tyto stránky jsou nejčastěji rozesílány e-mailem. Zadá-li uživatel své údaje do této stránky, odevzdá je de facto dobrovolně útočníkovi, který je může snadno zneužít. Obranou před tímto útokem je obezřetnost a důkladná znalost originálních stránek. Například banky často na svých stránkách opakovaně své klienty upozorňují na to, že prostřednictvím e-mailu nikdy k přihlašování do svých stránek nevyzývají. Dalším vodítkem je kontrola již zmíněného zabezpečeného protokolu HTTPS, či důkladná kontrola adresy přístupového portálu. V názvech adres falešných stránek bývají drobné rozdíly od těch skutečných. V případě, kdy uživatel „naletí“, je vhodné své heslo co nejrychleji změnit na pravých stránkách banky. Protokolem HTTPS a jeho využíváním se budeme také více zabývat v empirické části této práce.

Dalším předmětem zájmu útočníků jsou údaje z platebních karet. Banky se stále snaží vymýšlet sofistikovanější způsoby autorizace svých klientů a tím útočníkům znepříjemňují jejich snahy. Naproti tomu u platebních karet plně postačí údaje na ní uvedené a k žádnému ověřování majitele nedochází. V okamžiku získání potřebných údajů z karty již nic nebrání jejich zneužití na rozdíl od převodu peněz z banky, kdy musí útočník získat například nejběžněji používanou autorizační zprávu SMS. Zájem o nákup zboží na cizí účet je samozřejmě nižší než převod peněz z cizího účtu, přesto tímto způsobem bývají způsobeny rozsáhlé škody. Z pohledu počítačové kriminality lze zařadit mezi podobné trestné činy kopírování platebních karet pro účely krádeží peněz kartou z bankomatů. K tomu slouží tzv. skimmery, které okopírují magnetický proužek na platební kartě a v kombinaci s kamerou nebo podstrčenou klávesnicí zaznamenávající PIN kód ke kartě umožňují vyrábění a používání kopií karty. Slabým místem platebních karet je právě magnetický proužek, jehož kopírování není nikterak složitým procesem. Účinná ochrana proti kopírování platebních karet spočívá v postupném omezení používání magnetického proužku a přesun k využívání čipu, kterým je dnes již většina karet vybavena a který je velice dobře proti kopírování chráněn. Většina platebních terminálu již tento čip namísto magnetických proužků využívá. Problém tkví spíše v nejednotnosti karet i ve faktu, že například v USA jsou stále čipy využívány minimálně, a mnohé nově vydané karty jej stále nemají. Příčinou je pravděpodobně stále vysoká obliba off-line terminálů, které v České republice až na výjimky nejsou využívány.

3.2.7. Falšování peněž, dokladů a písemností

Falšování peněz, dokladů a písemností tvoří další oblast trestné činnosti, která se použitím výpočetní techniky výrazně zjednodušila a nabrala na svém objemu díky dostupnosti kvalitního vybavení. Pokročilé grafické programy a kvalitní tiskárny umožňují vytváření velmi věrných kopií a jejich následný tisk. Vidina snadného zisku z falšování peněz a jiných cenin za relativně malého úsilí vyústila v nárůst těchto kriminálních deliktů. V kombinaci s dostupností ochranných prvků se pak výroba zdařilých kopií stává předmětem podnikání i neprofesionálů. Dovolíme si použít slova nejmenovaného obviněného: „Ochranné hologramy jsem si objednal přes e-shop z Číny. Největší problém byl, že nejmenší objednatelné množství bylo 2000 kusů“. Jednalo se o rozsáhlý případ

falšování dokladů, při kterém byly v počítači obviněného nalezeny stovky občanských průkazů a jejich obdob, řidičských průkazů a pasů z několika desítek států celého světa. Většina dokladů je v současné době chráněna množstvím ochranných prvků, ale právě zmíněná možnost objednat si přes Internet prakticky cokoliv, doprovázená vynalézavostí falzifikátorů, značně komplikuje rozpoznávání pravosti dokumentů bez technických prostředků. Navíc falzifikátoři a majitelé falešných dokladů spoléhají na neznalost dokladů z exotických zemí při kontrolách dokladů autoritami. Obranou proti falšování dokladů jsou verifikační databáze, na kterých se sice pracuje (například veřejný rejstřík PRADO, zřízený Radou EU)[25], ale celosvětové propojení je na dlouhou dobu stále v nedohlednu.

3.3. Historie

Díky historii se dále pokusíme nastínit první možné příležitosti pro nežádoucí jevy v podobě útoků a zneužívání technologií.

3.3.1. Informační pravěk

Za prvopočáteční předchůdce informačních technologií lze s trochou nadsázky považovat dorozumívání lidí kouřovými signály nebo ukládání dat formou zářezů do prutů, uzlů či hliněných destiček.[26] K dnešní podobě bylo nutno urazit notnou časovou vzdálenost a vynaložit mnoho energie, ale tento příklad je uveden proto, že i takovéto způsoby dorozumívání a nakládání s informacemi jsou výsledkem pradávné potřeby lidí komunikovat a na dálku si důležité informace sdělovat. V těchto dobách pak o to důležitější, že nedostatek informací mohl mít fatální důsledky na společenství lidí v podobě přímého ohrožení nebo existenčních problémů.

Jak se lidská společnost vyvíjela a civilizovala, nároky na množství předávaných informací se zvyšovaly a tím lidstvo nutily k vynalézání efektivnějších prostředků. Snaha o rychlejší předávání informací vedla lidstvo přes živé posly, cvičení poštovních holubů, potrubní poštu a další jednoduché způsoby předávání informací. V tomto kontextu

[25] RADA EVROPSKÉ UNIE, *PRADO,* [on-line], dostupné z http://prado.consilium.europa.eu/cs/homeindex.html
[26] PROKEŠ, J., *Člověk a počítač anebo svítání digitální kultury,* s. 10

o informačních technologiích stále hovořit nelze, ale jedná se o prostředky lemující cestu k nim. Budeme-li pokračovat v nadsázce, lze mluvit o tom, že první náznaky informační kriminality lze nalézt ve zneužívání těchto prostředků za účelem zlomyslného zisku či získání výhody nad protivníkem, a to například zasíláním falešných zpráv, odchytáváním poštovních holubů za účelem odcizování důležitých zpráv, či výměnou strategických informací za jiné, matoucí. Žádné statistiky nejsou v této oblasti k dispozici, ale takové případy jsou známé.

3.3.2. První počítače

Pro vznik informačních technologií ve smyslu, který dnes známe, je klíčové 20. století. V jeho první polovině byl vyvinut první elektronický předchůdce dnešních počítačů ENIAC za využití elektronek[27]. V druhé polovině 20. století pak spatřuje světlo světa první počítač sestrojený za použití tranzistorů[28]. Později přichází tzv. třetí generace využívající integrovaných polovodičových obvodů a konečně tzv. čtvrtá generace využívající mikroprocesorů, které umožnily formu osobních počítačů a jejich masovější výrobu směřující k informačním technologiím tak, jak je známe dnes.[29]

Kromě pravděpodobně prvního známého případu z Francie z roku 1801, který lze považovat za počítačovou sabotáž, kdy se jednalo o poškození textilního tkacího stroje řízeného děrnými štítky[30], lze z kazuistiky českého prostředí uvést jeden případ počítačové kriminality z kriminalistického sborníku, datujícího se k roku 1985.

Již v úvodní informaci k tomuto případu, který se odehrál v národním podniku Sklárny Kavalier Sázava, je uvedeno, že se tímto setkáváme s novou formou trestné činnosti spočívající ve zneužívání výpočetní techniky. Vynalézavost jisté mzdové účetní, později odsouzené na čtyři a půl roku odnětí svobody, byla obdivuhodná – dokázala využít absence kontrolních mechanismů v používané výpočetní technice. Prvotním impulsem byla situace, kdy mzdová účtárna opomenutím nezanesla zkrácení pracovní doby zmíněné

[27] První generace počítačů výhradně na elektronickém principu. V literatuře můžeme narazit i na pojem „nultá generace počítačů“, který zahrnuje počítače založené na mechanickém nebo mechanicko-elektrickém principu.
[28] Tzv. druhá generace počítačů, která se vyznačovala především velmi vysokou prostorovou a energetickou náročností.
[29] NAUMANN, F., *Dějiny informatiky – Od abaku k internetu,* s. 195-197
[30] SMEJKAL, V., *Internet a §§§,* s.154

účetní do děrných pásků[31] a jí tak byla nadále vyplácena mzda za dobu v původním rozsahu. K tomu postupně přidávala již svépomocí do podkladů pro mzdy i dny své pracovní absence. Zkouška kontrolních systémů vyvrcholila zanesením mzdy propuštěného pracovníka. Když toto nebylo odhaleno, začala zavádět do systému „černé duše“, jejichž výplatní pásky ničila a výplaty ve státní spořitelně změnovými lístky přeposílala na vlastní vkladní knížku. Proti odhalení se pojistila tak, že na začátku kalendářního roku, kdy počítač zpracovává mzdové listy, tyto listy vyřadila a ukryla. Navíc výplaty „černých duší“ nedanila, aby nebyla odhalena finanční správou. Dlužno dodat, že odhalena byla pouze škoda v podobě počtu odpracovaných hodin navíc. Vyplácení za černé duše bylo zjištěno jejím vlastním doznáním.[32]

3.3.3. Vynález mobilního telefonu

Dalším významným vynálezem dvacátého století je mobilní telefon. Představení mobilního telefonu provedeme jen velice letmo a více se budeme zabývat tzv. chytrými telefony, jejichž příchod přinesl značnou příležitost pro nový druh počítačové kriminality, popř. rozšíření praktik zavedených na tradičních počítačích.

Vynález mobilního telefonu ve smyslu „bezdrátový“ je datován již do konce 19. století. K užívání pro veřejnost byly poprvé dostupné v 50. letech 20. Století. Z počátku jako vybavení automobilů, které jim poskytovaly potřebnou elektrickou energii, možnost připojení potřebně velké antény a v neposlední řadě absorbovaly jejich velkou hmotnost[33]. O prototypu prvního funkčního mobilního telefonu ve smyslu plně přenositelných přístrojů lze mluvit v roce 1973, o deset let později v roce 1983 byl představen první sériově vyráběný telefon Motorola DynaTAC 8000X fungující na analogové síti.[34] Telefony, využívající analogovou síť byly schopny pouze telefonovat, ale již tato jediná funkce se stala předmětem útoků, a to například krádeže identit díky nedostatečné autentifikaci. Příchod sítě GSM, zaváděné v letech 1982 – 1991, přináší i možnost dalších služeb podmíněných digitálním provozem a tedy i úsvit prvních příležitostí pro kybernetickou kriminalitu. Pokusy o krádeže identit pokračovaly pomocí nových vynalézavých způsobů,

[31] Předchůdce paměťových médií.
[32] HAUERLAND, M., *Jedna z forem zneužití výpočetní techniky k osobnímu obohacení*, s. 669-671
[33] První mobilní telefony, používané v automobilech, představovaly zátěž kolem 40 kg.
[34] Tzv. síť první generace. Počínaje druhou sítí GSM je vývoj orientován na sítě digitální.

například duplikováním karet SIM, které proti tomu nebyly zabezpečeny. S příchodem tzv. chytrých mobilních telefonů se značně rozšířila oblast počítačové kriminality. Chytrý mobilní telefon lze pokládat spíše za počítač obohacený o funkce mobilního telefonu. Oblast možností napadání telefonu se tak z výše zmíněných útoků na autentifikaci a kopírování SIM karet významně rozšířila, či spíše přesunula. Digitalizace sítě totiž umožnila technologii SIM karet a hlavně proces přihlašování karty do sítě natolik změnit a zdokonalit, že v současné době prakticky není možné funkční klon SIM karty vyrobit. Naproti tomu jsou operační systémy v mobilních telefonech mnohem složitější a otevřenější, a tak se rozšiřuje i možnost jejich napadení či pozměnění vedoucí často ke ztrátě absolutní kontroly nad zařízením. Existuje celá řada softwarů do chytrých telefonů, které umožňují na dálku monitorovat veškerou činnost uživatele, nebo telefon bezmezně na dálku ovládat. A to navíc naprosto skrytě, kdy je často složité přítomnost takovéto infiltrace v telefonu vůbec identifikovat. Jakmile se útočníkovi podaří takový program do mobilního telefonu dostat, otevírají se mu rozsáhlé možnosti dalšího zneužívání.

3.3.4. Historie Internetu

I počátky sítě Internet se datují do druhé poloviny 20. století. Předchůdcem se stala síť pod názvem ARPNET, financovaná grantovou agenturou ministerstva obrany USA, uvedená do provozu v roce 1969. Jednalo se o síť propojující počítače na čtyřech amerických univerzitách. Tato síť se postupně rozšiřovala po území USA a v roce 1973 se propojila s evropským kontinentem a také se odehrálo první využití sítě pro poštovní služby.[35] Do této doby, konkrétně do roku 1971, se datuje i vznik prvního počítačového viru jménem Creeper a v reakci na něj pak programu Reaper, který se tak stal prvním počítačovým antivirem na světě, i když pouze jednoúčelovým. O něco později (1983) se přidává i negativní význam výrazu hacker, a to v souvislosti s neoprávněným přístupem k vojenským informacím, využívajících síť ARPANET.[36] Zde vidíme jasný důkaz toho, že počítačová kriminalita a boj s ní je úzce spjat se vznikem technologií a není tedy ničím novým, tedy ani fenoménem konkrétní pozdější doby. S rostoucím rozšiřováním

[35] NAUMANN, F., *Dějiny informatiky – Od abaku k internetu,* s. 352-359
[36] MUSIL, J., *Elektronická média v informační společnosti,* s. 365

a překotným vývojem Internetu a doprovodných technologií se samozřejmě rozšiřují i možnosti zneužití a přirozeně se rodí i nové nápady, jak kriminální činnost páchat.

Ve spojitosti Internetu a kriminality je vhodné zmínit pojem anonymita. Tvůrcem obsahu Internetu se může stát každý pod jistou mírou anonymity a v souvislosti s tím vzniká absence zodpovědnosti vůči účinku vloženého obsahu.[37] Od tohoto subjektivního pocitu internetové svobody už zbývá jen krok ke kriminálnímu činu.

Z kriminalistického hlediska se jedná o anonymitu zdánlivou, avšak existují i nástroje, které z ní mohou učinit absolutní. Používání těchto nástrojů lze eliminovat pouze legislativní cestou ve spojení s represemi.

3.3.5. Webové sociální sítě

Vznik sociálních sítí má svou historickou vazbu na všechny výše uvedené body popisující historii technologií. Samotnou předchůdkyni Internetu, síť ARPANET a její první využití pro elektronickou komunikaci, či první poštu v roce 1971 lze chápat jako budování sociální sítě. Jinými slovy se jedná o vytváření či posilování sociálních vazeb prostřednictvím informačních technologií. Dalším krokem byl pak BBS (Bulletin Board System) z roku 1978, což byla v podstatě elektronická verze nástěnky. Dalším významným krokem bylo vytvoření prvního on-line chatu (IRC – Online Realy Chat) v roce 1988. První síť současného typu kombinující funkce svých předchůdců vznikla v roce 1997 pod názvem sixDegrees.com, ale pro finanční neúnosnost (předběhla svou dobu) byla v roce 2001 ukončena.[38] Následovaly již známé a většinou stále fungující sítě jako Friendster.com (2002), MySpace.com (2003), Facebook.com (2006) či Google+ (2011) a dále pak celosvětové specializované sítě jako Twitter.com, LinkedIn.com, či české účelové sociální sítě jako Lidé.cz, Spolužáci.cz atd.

Vzhledem k obrovskému množství uživatelů a dat, které z charakteru a obliby sociálních sítí vyplývají, se právě sociální sítě stávají častým terčem kybernetické kriminality. Není dnes žádným tajemstvím, že firmy u svých potenciálních zaměstnanců k vyhledávání informací sociální sítě používají. Některé firmy se k tomu dokonce veřejně

[37] MUSIL, J., *Elektronická média v informační společnosti*, s. 175
[38] OBJEVIT.CZ, *Sociální sítě a jejich vývoj,* [on-line], dostupné z http://objevit.cz/socialni-site-vyvoj-pohled-do-historie-t22280

přiznávají. Tuto skutečnost můžeme chápat ze dvou pohledů. Prvním je konstatování, že informace, které uživatel na svém profilu v sociální sítí nemá pro ostatní uživatele skryté nebo zabezpečené, jsou automaticky pokládány za veřejné. Druhým pohledem je varianta, že potenciální zaměstnavatel má právo pouze na informace, které mu uchazeč vědomě poskytne. Pojem sociální síť a chování jejích uživatelů je někdy zaměňován s veřejným zdrojem informací, k čemuž by v žádném případě nemělo docházet. Budou-li se však uživatelé tímto rozdílem zabývat, mohou svým nastavením soukromí na sítích tuto hranici jasně rozlišit. To platí i pro počítačovou kriminalitu.

4. Empirická část

Jak se v praxi ukazuje, hrozba útoku prostřednictví informačních technologií je v běžném životě uživatelů výrazně podceňována. Nikoliv ve smyslu její nebezpečnosti, ale spíše v reálném dopadu na jednotlivce. Útoky jsou chápany jako cosi abstraktního a většina lidí si nepřipouští, že by se jich mohly bezprostředně dotknout. S tím je pak spojena i nedostatečná pozornost při zabezpečení techniky běžného denního používání.

Jako pracovník znaleckého ústavu v oboru Kriminalistika, odvětví Analýza dat a zkoumání nosičů dat, jsem v každodenním kontaktu s kriminálními činy, při kterých jsou informační technologie buď přímo nástroji pro páchání trestné činnosti, nebo jsou prostředky technologií používány pro vyhledávání dalších důkazů. To spočívá zpravidla v mapování kontaktů, vazeb, k získání informací o motivech takových činů či vyhledávání vodítek v multimediálním obsahu zajištěných přístrojů. Výsledky mají v procesu dokazování titul samostatných přímých či nepřímých důkazů. Tvrzení o technologiích jako součástí běžného života tím dostává jasného rozměru, protože jsou k těmto účelům využívány i v případech, které s počítačovou kriminalitou vůbec nesouvisí. Takovým příkladem může být třeba odhalování sítí výrobců a dealerů drog, kdy se nejedná o kybernetickou kriminalitu. Mobilní telefony jsou podezřelým odebírány za účelem mapování kontaktů a vazeb, nebo jen pro případ používání telefonů jako obrazových záznamových prostředků. Jedním z úkolů analýzy získaných dat je nalezení a vytvoření diagramu vazeb získaných z výpisů hovorů, různých zpráv i mapování oblastí, kde se přístroje pohybovaly. Toho je využíváno v širokém spektru prošetřovaných případů.

Tou hlavní oblastí je však počítačová kriminalita dle uvedených definic. Je na místě položit si otázku, do jaké míry lze počítačovou kriminalitu omezit změnami chování uživatelů. Za tímto účelem byl proveden kvantitativní výzkum, popsaný v kapitole Cíle práce a metodika, zaměřený převážně na zabezpečení dat a komunikace na Internetu. Ze získaných dat se pokusíme identifikovat chování a znalosti, které útočníkům jejich snažení zjednodušují či naopak komplikují.

Téma je o to aktuálnější, že Česká republika se nachází na osmém místě v žebříčku neohroženějších zemí světa v počtu pokusů o instalaci škodlivého software

uživateli.[39] (Seznam prvních deseti zemí je uveden v příloze č. 2). Empirická část se tedy pokusí nalézt spojitost tohoto zjištění a dalších skutečností, vyplývajících z odhalování trestné činnosti, s chováním uživatelů.

4.1. Zabezpečení dat

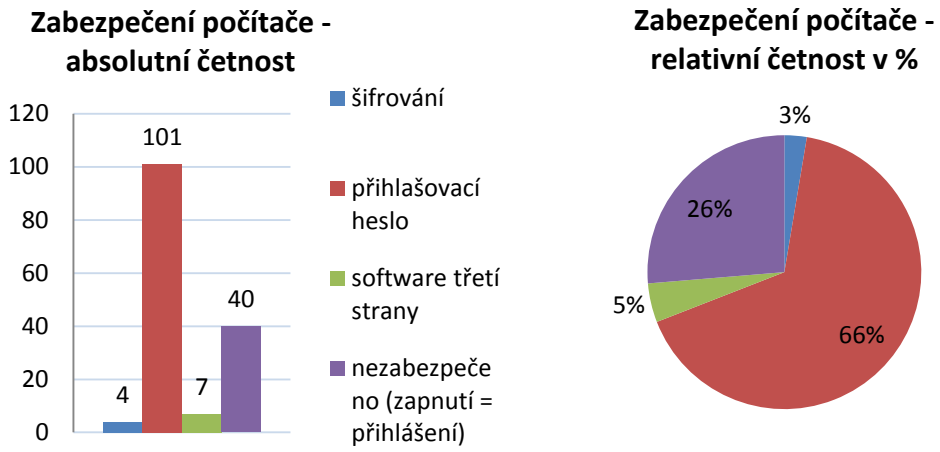
Jedním ze základních kritérií, ovlivňujících účinnost pokusů o nežádoucí kybernetické činy, je zabezpečení zařízení komunikačních a informačních technologií samotnými uživateli. Jedním z cílů práce je charakterizovat českou uživatelskou základnu z pohledu schopnosti a ochoty svá data zabezpečovat.

Dalším kritériem je pak zabezpečení přístupu k nim. Příkladem může být ukládání na webové úložiště spolehlivého poskytovatele za použití zabezpečeného šifrování dat a volba kvalitního hesla, ale také špatné nebo dokonce žádné zabezpečení koncového zařízení. Uživatel, který má hesla uložena v mobilním telefonu a telefon nemá proti neoprávněnému vniknutí nijak zabezpečen, při ztrátě telefonu či volnému odložení bez dohledu pak de facto potenciálnímu zájemci o data umožní volný přístup. Krádeží telefonů nebo počítače pak zloděj kromě zařízení získává často i cenná data, a tím může způsobit větší škodu. Obecně řečeno – nad bezpečností dat je třeba přemýšlet komplexněji.

Jiným příkladem může být odcházení od stolního počítače bez odhlášení. Díky této lehkomyslnosti byl v minulosti spáchán nejeden zločin. Týká se to především firemních sítí. Kvalitní odborná konfigurace sítě jejím uživatelům přiděluje oprávnění, do jaké míry mohou provádět zásahy do dat. I v případě špatné konfigurace lze dohledat, kdo je viníkem neoprávněných zásahů. To ale vychází z předpokladu, že každý vystupuje v síti svým jménem. V případě snahy nebýt odhalen se proto jako jediná možnost nabízí zneužití cizí identity v rámci sítě.

Některé otázky provedeného průzkumu se proto soustředily i na mapování tohoto tématu. První otázka tématu se týkala zabezpečení uživatelských dat počítače. Z dotazníkového šetření bylo zjištěno následující:

[39] KASPERSKY SECURITY BULLETIN 2014, *Overall Statistics for 2014*, [on-line], dostupné z http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2014/12/Kaspersky-Security-Bulletin-2014.-Overall-statistics-for-2014.pdf



Graf č. 3 - Zabezpečení počítače.

Téměř 74 % zastoupení zabezpečení dat v počítačích lze pokládat za uspokojující. Je k tomu však třeba dodat, že z pohledu snahy o zpřístupnění dat se jedná o zabezpečení nedostatečné. Zmocní-li se počítače pachatel za účelem získání dat, není překonání uživatelského hesla nijak složité – postačí pouze připojení pevného disku do jiného počítače. Naproti tomu je pouze v 2,63 % využíváno šifrování dat. Tato metoda zabezpečení je velmi efektivní a k jejímu překonání jsou třeba běžně nedostupné prostředky. Řeč je o extrémním výpočetním výkonu a v případě silných hesel i extrémním času na dešifrování v řádech let. V současné době lze šifrování v kombinaci s kvalitním heslem považovat z praktického hlediska téměř za nepřekonatelné. Zároveň je třeba dodat, že šifrování lze doporučit spíše na novějších a výkonnějších strojích, protože samotné šifrování je poměrně složitý proces probíhající při provozu počítače při každé provedené operaci.

Výzkum dále ukazuje na rozdíly mezi zabezpečením počítačů a mobilních telefonů. Zatímco u počítačů je jejich zabezpečení alespoň heslem využíváno v 73,7 %, u mobilních telefonů je paměť přístroje chráněna pouze ve 48 %. Provedeme si bližší prozkoumání souvislosti zabezpečení a typu mobilního telefonu. Účelem je zmapování změny přístupu k mobilnímu telefonu při přechodu od klasického k tzv. chytrému, který lze s ohledem na výrazně rozšířené možnosti považovat spíše za počítač. Zjištění závislosti zabezpečení přístupu na typu telefonu by mělo prozkoumat hypotézu, že uživatelé používají chytré telefony (71 % respondentů) s jejich funkcemi (internetové bankovnictví, ukládání soukromých dat atd.) a při tom k zabezpečení těchto dat přistupují stejně jako ke

klasickým telefonům, kdy byl zřetel kladen spíše na znemožnění neoprávněného používání účastnického čísla formou ochrany kódem PIN.

K prozkoumání hypotézy využijeme kontingenční tabulku sestavenou na základě dotazníkového průzkumu, konkrétně pak z otázek č. 3 a 4 (viz příloha č. 1). Při výpočtu teoretických četností pomocí vzorce[40] $n_{oj} = \frac{n_{io} n_{jo}}{n}$ byly zjištěny některé hodnoty nižší než 1 a více než 20ti procentní podíl hodnot menších než 5, tudíž bylo provedeno sloučení slabých skupin[41] do následující tabulky včetně vyjádření teoretické četnosti v závorkách:

Souvislost typu telefonu a zabezpečení	kombinace zabezpečení paměti a kódu PIN	heslo, gesto, nebo podobná překážka pro přístup k datům v telefonu	PIN pro přihlášení do sítě po spuštění telefonu	nezabezpečeno
klasický mobilní telefon (tlačítkový)	1 (14,33)	4 (13,20)	29 (19,61)	10 (10,18)
chytrý telefon	37 (23,67)	31 (21,80)	23 (32,39)	17 (16,82)

Tab. č. 2 - Závislost zabezpečení na typu telefonu.

Dále bylo provedeno vyjádření hodnoty testovacího kritéria χ^2 =6,151 dle vzorce[42]:

$$\chi 2 = \sum \sum \frac{(n_{ij} - n_{oj})^2}{n_{oj}}$$

Ta byla dále porovnána s tabulkovou kritickou hodnotou $\chi 2_{0,05(3)}$=7,815. Protože je vypočtená hodnota nižší než hodnota kritická, nelze na hladině významnosti 0,05 nulovou hypotézu zamítnout. Typ telefonu tedy na způsobu jeho zabezpečení uživatelem nezávisí.

V oblasti zabezpečení osobních dat v mobilních telefonech bych rád na tomto místě zmínil zjištění při svém pracovně-studijním pobytu ve Spojených státech amerických. Dvouměsíční pobyt jsem trávil ve školícím zařízení i při volnočasových aktivitách v poměrně specifické skupině lidí. Jednalo se o skupinu cca padesáti amerických vojáků, z různých koutů spojených států, kteří se účastnili kurzu vyšetřování pro vojenské

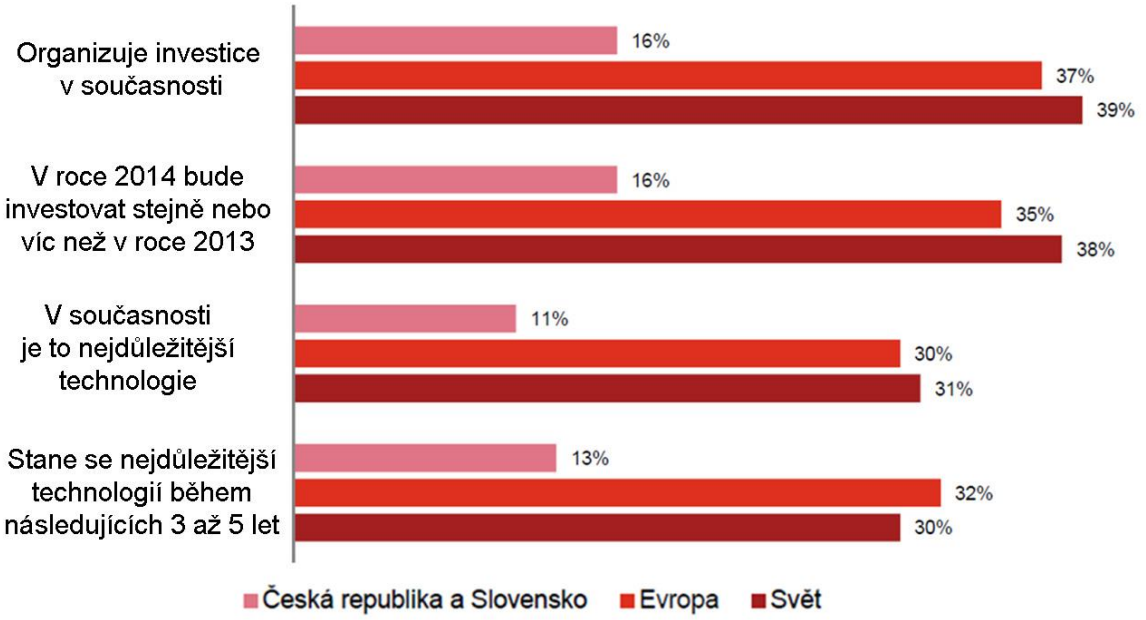
[40] SVATOŠOVÁ, L., KÁBA, B., *Statistické metody II,* s. 14
[41] tamtéž
[42] tamtéž

policisty. Neprováděl jsem žádný kvalifikovaný průzkum, ale v rámci času stráveného se svými americkými kolegy jsem zjistil, že ve 100 % vypozorovaných manipulací s mobilním telefonem v této skupině byl mobilní telefon zabezpečen pomocí gesta, hesla, či jiného prostředku, zabraňujícího přístup k soukromým datům při příležitostném zmocnění se přístroje, či při ztrátě. Naproti tomu v České republice jsou tyto prostředky využívány v méně než 45 %.

Nutno podotknout, že jakákoliv zabezpečení dat představují pro uživatele jisté nepohodlí v používání přístrojů. Ať už se jedná o počítače, ve kterých je jako spolehlivý způsob ochrany dat používáno šifrování, které jeho činnost zpomaluje, tak o mobilní telefon. V případě tzv. chytrých telefonů, kdy jejich používání o mnohé překračuje původní účel telefonování a odesílání textových zpráv, vzniká komplikace v podobě odemykání přístroje, které je zapotřebí mnohokrát denně. Toto nepohodlí se právě pro většinu uživatelů stává důvodem k lehkomyslnosti ohledně zabezpečení jejich přístroje.

4.2. Cena dat

V případě firem a institucí mohou být elektronická data klíčovým vlastnictvím, od kterého se odvíjí základní princip jejich fungování. Úspěšnost mnohých firem je založena na jedinečném know-how, kdy prozrazení tohoto unikátního vlastnictví může firmu poškodit, či přímo existenčně ohrozit. Jejich ochrana pomocí technologií tomu však neodpovídá. Lze namítnout, že lidský faktor je postaven minimálně na roveň možnosti úniků prostřednictvím technologií. O tom nemůže být pochyb. Hlavní rozdíl však lze spatřovat v tom, že únik díky zaměstnanci (i bývalému) bývá zpravidla doprovázen úmyslem. Buďto motivačním, kdy tento podlehne nabídce zájemce o informace, nebo slouží jako prostředek pomsty. Pro tyto případy existují prostředky, jako institut mlčenlivosti, či reálně hrozící postih za takovéto jednání, které lze poměrně účinně aplikovat. Naproti tomu k únikům prostřednictvím elektronických médií dochází často buď z důvodu nedostatečného zabezpečení takových dat, nebo při neopatrnosti nebo neznalosti. V prvním případě bývají příčinou slabé investice do bezpečnostních prostředků, které pramení mimo jiné i z podceňování hrozeb. Dle průzkumu firmy PWC z roku 2013 vyplynulo, že v České republice a na Slovensku je věnováno tématu internetové bezpečnosti 2,4 krát méně než je světový průměr.



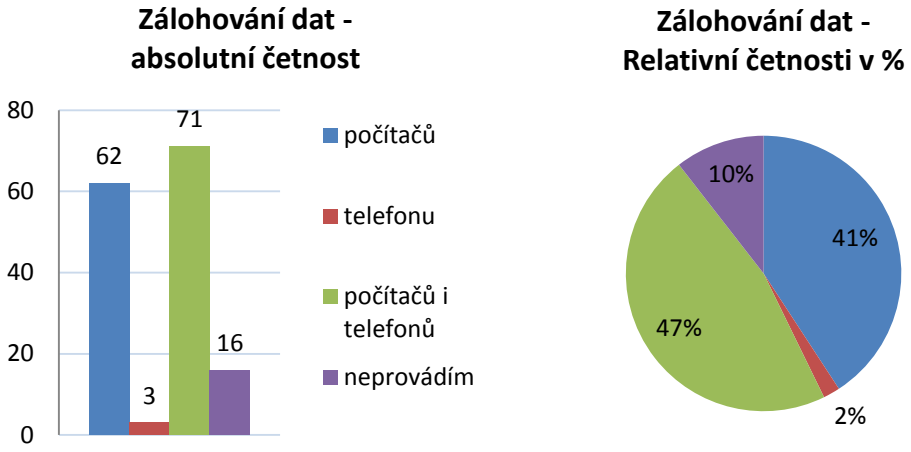
Graf č. 4 - Význam a objem investic do technologií internetové bezpečnosti.[43]

Z vlastní praxe jsem vysledoval ochotu investovat značné prostředky do ztracených dat soukromých osob, přičemž ve většině případů bylo možno takovýmto ztrátám předejít. Vlivem stoupající počítačové gramotnosti se mění poměr důvodů ztráty dat. Případů vlastního neopatrného smazání ubývá a hlavními příčinami se tak stává především selhání hardware. V obou případech by postačila investice do záložních kapacit, které jsou ve srovnání s náklady na obnovu dat jen drobnou investicí porovnatelnou s pojištěním domu, který později vyhoří. V souvislosti se selháním hardware navíc stoupá riziko definitivní ztráty dat. Již několikrát jsem se setkal se zoufalými lidmi s poškozeným pevným diskem v ruce, kteří byli ochotni investovat desetitisíce korun za obnovení kompletní dokumentace rodinných zážitků spojených s vývojem svého potomka.

Zkušenost dále napovídá, že postupem času a s narůstajícími kapacitami paměťových médií jejich spolehlivost klesá. To souvisí se snahou snižovat náklady na jejich výrobu vlivem silné konkurence. Snižování nákladů má pak za následek použití méně kvalitních materiálů i výrobních technologií. Toto povědomí se mezi uživateli šíří a ve spojitosti s četnými zkušenostmi pravděpodobně vyústilo i k výsledku průzkumu na otázku zálohování dat. Z něj vyplynulo, že pouze 10,5 % respondentů neprovádí zálohu dat

[43] PWC, *6. ročník globálního průzkumu Digital IQ Česká republika a Slovensko,* [on-line], dostupné z: http://www.pwc.com/cz/cs/studie-analyzy/pwc-digital-iq-2014-ceska-republika-slovensko.pdf

vůbec. 46,7 % lidí provádí zálohu počítače i telefonů a 40,79 % zálohuje data aspoň v počítači, viz grafy níže.



Graf č. 5 - Zálohování dat.

Dalším rizikem, spojeným především se sociálními sítěmi, je únik osobních či dokonce intimních dat. V policejní praxi odhalování kybernetické kriminality lze najít případy až neuvěřitelné důvěry v zabezpečení dat ve virtuálním prostoru, jejichž únik, v horším případě i veřejný, je zpravidla jen otázkou času. Nepotvrzuje se ani předpoklad, že takovéto riskantní chování lze očekávat spíše u mladší části populace.

4.3. Fenomén sociálních sítí

Téma sociálních sítí v souvislosti s bezpečností dat nelze v této práci opomenout. Především sociální síť Facebook se prakticky od svého masovějšího rozšíření, tedy poté, co opustila svůj původní účel studentské sítě, potýká neustále s problematikou bezpečnosti dat svých uživatelů. Téměř každoročně se z různých zdrojů dozvídáme, k jakým únikům a v jaké míře k úniku dat dochází. Protože disponuje největším množstvím uživatelů, je s ní spojeno i největší množstvím útoků na uživatelská data. Vzhledem k rozsáhlosti služeb, které jsou na Facebooku poskytovány, se i možnosti uživatelského nastavení zabezpečení stávají složitými a tak dochází k nežádoucímu zveřejňování dat ze strany uživatelů.

Fenomén sociálních sítí spočívá i v dalších typech nebezpečí a tedy i s více typy trestné činnosti. První oblastí jsou již zmíněné úniky dat, ke kterým může dojít chybou provozovatele sítě, vzniká však i riziko jejich ukradení útočníky. Tyto krádeže jsou dvojího

typu. Buď krádeže velkého množství dat, nebo jen napadání konkrétního známého uživatele. Často dochází k neoprávněnému přihlašování do cizího profilu a následnému páchání škod v podobě šikanování, vydírání, případně ničení sociálních vazeb poškozeného. Dalším typem činnosti, jejíž cílovou skupinou jsou hlavně děti, je navazování kontaktů založených na důvěřivosti dětí, které mohou mít dalekosáhlé následky v podobě mnohem závažnější trestné činnosti. To je často usnadněno i množstvím zveřejňovaných a přesných osobních informací, o čemž nemají rodiče zpravidla tušení.[44] Tím nejzávažnějším zločinem, se kterým se v policejní praxi bohužel velmi často setkávám, je tvorba, šíření a obchod s dětskou pornografií.

Právě sociální sítě a různé Instant Messengery bývají místem prvního kontaktu pachatele s obětí. Existuje zde mnoho profilů, které jsou zavedeny jen za účelem jejich hledání.[45] Po navázání kontaktu dochází k získávání důvěry pachatele s velkou mírou anonymity, výměně fotografií a psychologické hře, ve které má dospělý pachatel samozřejmě nad dítětem velkou psychickou převahu. Získávání důvěry může dále vyústit v osobní kontakt, kde je fáze vytvořeného vztahu již často situací zneužitelnou k vydírání oběti. V těch horších případech je důvěra dále upevňována a může skončit i fyzickým kontaktem a následnou tvorbou pornografie.

K jejímu šíření jsou pak zpravidla již používány jiné, z pohledu pachatelů bezpečnější, způsoby jako například soukromé webové stránky či elektronická pošta. Existují totiž vyhodnocovací nástroje, které jsou schopny obrazové materiály analyzovat a především dětskou pornografii na sociálních sítích rozeznávat. Provozovatele sociální sítě o tom informují a dále takovéto informace využívají ve spolupráci s orgány státní správy. U dětí kolem pubertálního věku, vzhledem k obtížné odhadnutelnosti věku, spočívá identifikace trestného činu v dohledání totožnosti dotčeného a prokázání trestného činu v souvislosti s jeho věkem skutečným.

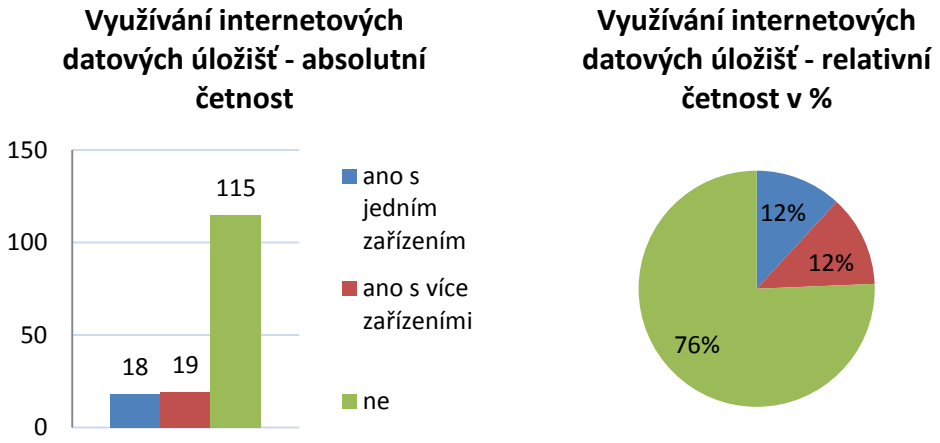
Pro připomenutí dalšího úskalí sociálních sítí uvádím graf č. 2 na straně 23, ve kterém jsou procentuálně vyjádřeny cíle phishingu. Právě zde můžeme vidět sociální sítě a Instant Messengery jako dvě nejčastější oblasti.

---

[44] HULANOVÁ, L., *Internetová kriminalita páchaná na dětech,* s. 94
[45] tamtéž

Facebook má ještě jedno specifikum mezi sociálními sítěmi a tím jsou webové aplikace. I ty se staly oblíbeným prostředkem napadání počítačů útočníky. V tomto případě se jedná o podobné téma jako je spam a phishingové zprávy. Rozdílem je pouze forma doručení k příjemci. Mezi společné znaky webové aplikace na Facebooku patří například to, že se aplikace sama nespustí bez aktivity uživatele a obrana tedy spočívá v prosté ignoraci uživatele. Možnosti takových aplikací poškodit počítač jsou srovnatelné s přílohami útočných e-mailových zpráv. Na rozdíl od e-mailu ale není uživatel chráněn žádnou obdobou spamového filtru. Rozlišování takových aplikací je leckdy značně komplikováno, protože se objevují i takové, které využívají údaje o skutečných osobách, čerpané z uživatelů sociálních sítí. V nastavení bezpečnosti sítě Facebook je možné webové aplikace zakázat, což lze jednoznačně doporučit. Znamená to však nemožnost hrát hry a vyplňovat nejrůznější kvízy. Právě jejich obliba vedla k nápadu tento typ aplikací využívat k infiltraci do počítače.

Nejen sociální sítě, ale i další webové služby jako jsou úložiště dat, mají jednu z největších předností v tom, že jsou data na nich dostupné kdykoliv a z jakéhokoliv zařízení. Kapacitně zpravidla počítačům nekonkurují, ale předpokládá se, že lidé používají více zařízení najednou a potřebují mít svá důležitá data stále k dispozici. Dalším důvodem je samozřejmě jejich sdílení, což platí analogicky k sociálním sítím, pouze se jedná o jiný druh dat a jsou určená k jinému účelu, například k práci.

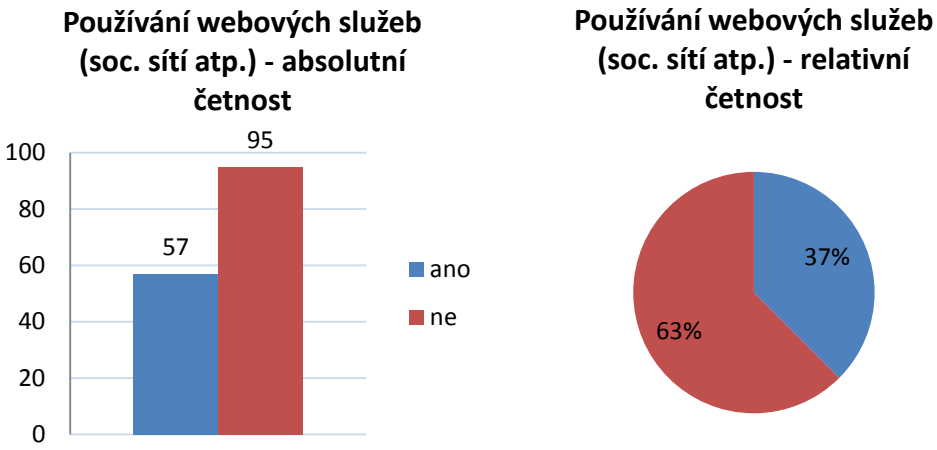


Graf č. 6 – Využívání internetových datových úložišť.

Průzkum ukázal, že i tato úložiště, byť ve velmi omezené míře, postupně nacházejí v české uživatelské základně uplatnění a i hlavní výhoda je dvanácti procenty

respondentů využívána. Mezi důvody vysokého procenta těch, co úložiště nevyužívají, patří i nedostatečná důvěra.

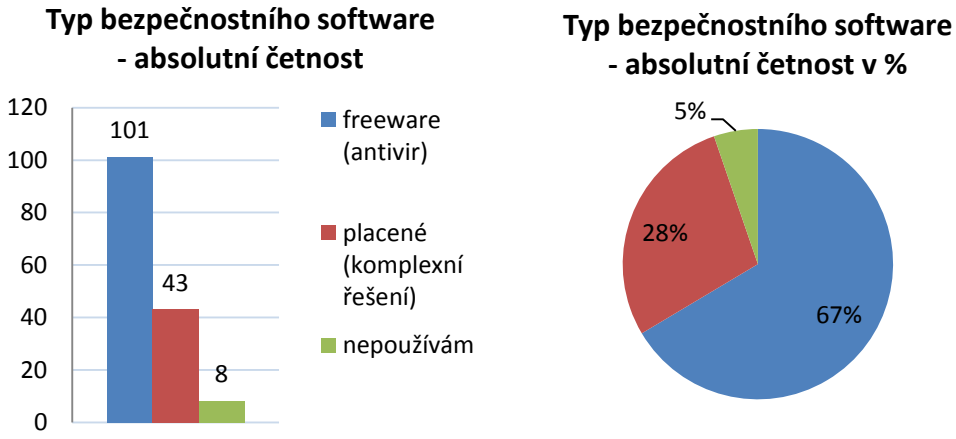
Rozšíříme-li datová úložiště i o ostatní webové služby a sociální sítě, vidíme, že zde je přistupování z více zařízení již mnohem využívanější.



Graf č. 7 – Používání webových služeb.

4.4. Antivirové programy nebo komplexní bezpečnostní řešení

Dalším významným pramenem informací o počítačové kriminalitě jsou statistiky výrobců ochranných softwarových produktů, jako jsou antiviry a firewally. Jak vyplývá z provedeného výzkumu, antivirový program je již automaticky pokládán za nutnou aplikaci pro chod počítače. To lze přisuzovat dvěma skutečnostem. První je, že lze pořídit relativně kvalitní antivirový program zdarma či pouze výměnou za jednoduchou registraci a druhou je to, že nejrozšířenější operační systém současnosti v jeho novějších verzích antivirový software obsahuje jako jeho nedílnou součást. V tomto případě je majitel nového počítače po jeho vybalení proti základním virovým útokům automaticky chráněn bez jakéhokoliv vlastního přičinění. V tuto chvíli však nastává otázka, zda jsou antivirové programy dostačující.



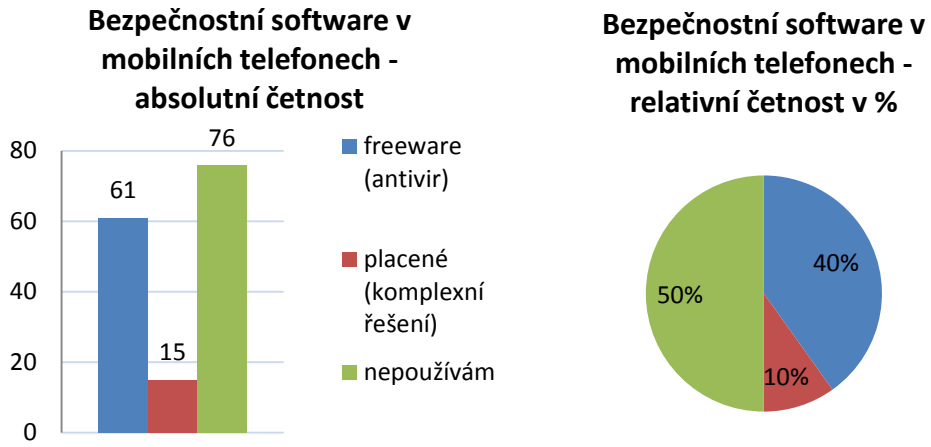
Graf č. 8 – Typy používaných bezpečnostních softwarů.

Můžeme vidět, že mezi respondenty bylo pouze 28 % vlastníků komplexních řešení. Útočníci jsou samozřejmě s výše uvedeným stavem ochrany osobních počítačů srozuměni a tak vymýšlejí stále sofistikovanější způsoby napadání, které už antivirové programy ze své podstaty nezachycují. V takovém případě nastává nutnost komplexního bezpečnostního software, který sice zdarma není, poskytuje však důmyslnější a komplexnější ochranu. Tyto programy v sobě kromě antivirové ochrany obsahují i další nástroje, jako je kontrola aplikací při jejich instalaci na škodlivý kód a další potenciální hrozby vyplývající z jejich instalace, případně jsou schopny analyzovat jejich nestandardní část. Toto řešení lze souhrnně nazvat jako rezidentní štít.[46] Dále jsou tyto programy schopny kompletně monitorovat síťový datový provoz počítače včetně méně využívaných komunikačních protokolů a portů. Díky tomu jsou schopny zabránit útokům z Internetu, tzv. firewall nebo IDS – Intrusion Detection System – systém pro odhalení průniku. Dále existuje celá řada funkcí, jejichž množství se liší podle výrobců. Většina z nich ale poskytuje funkce jako je ochrana systémových souborů, služba vyhledávání odcizeného počítače (mezi respondenty průzkumu využívá pouze 16, 45%), ochrana před otvíráním nebezpečných stránek, ochrana poštovních klientů (i před nevyžádanou poštou), rodičovská kontrola přístupu na webové stránky (možnost zakázat otvírání webových stránek určitého obsahu) nebo ochrana proti phishingu. Vždy záleží na kvalitě softwaru, jak účinné tyto prostředky jsou. Lze však říci, že konkurence nutí propady v efektivitě ochrany zmenšovat a dále je vyvíjet. Navíc lze v současné době hovořit o inteligentních

[46] STŘIHAVKA, M., *Vaše bezpečnost a anonymita na Internetu,* s. 69

softwarech, kdy uživatel často ani jejich aktivitu nepozoruje a přesto jsou skrytě prováděny úkoly, které mohou uživatele ochránit před nepříjemnostmi, ke kterým by se sám mohl zásadním způsobem přičinit. Inteligence těchto softwarů spočívá ve schopnosti učit se z chování uživatele a rozeznávat tak hrozby efektivněji. V době nedávno minulé fungovaly firewallové softwary tak, že byla veškerá komunikace ve výchozím nastavení zakázána (jisté vodítko kvality tehdejších firewallů) a při jakýchkoliv pokusech o síťovou komunikaci byl uživatel dotazován, zdali je požadavek na síťový provoz oprávněný či nikoliv a jestli má být zvolená volba příště zopakována. Kromě toho, že takového dotazování bylo pro uživatele poměrně časově náročné, běžný uživatel nebyl schopen kvalitně o oprávněnosti a bezpečnosti každého takového požadavku rozhodnout. To firewally odsoudilo k užívání zkušenější části uživatelů a dále především systémových administrátorů podnikových sítí. Pro běžného uživatele bylo nastavování obtížné, nesrozumitelné a v případě špatné volby mohl firewall v podstatě znefunkčnit. Požadavků na síťovou komunikaci probíhá v počítači velmi mnoho. Kromě běžného prohlížení webových stránek jsou tyto požadavky kladeny i většinou ostatních programů, které se v počítači nacházejí a to i na různých komunikačních portech a je tedy poměrně složité se ve všech požadavcích orientovat a kvalitně posoudit, zda jsou jejich požadavky na komunikaci oprávněné či ne. Útočný požadavek se pak mezi těmi oprávněnými z pohledu uživatele může „ztratit“.

Vzhledem ke zjištění, že více než 71 % uživatelů vlastní chytré mobilní telefony, je vhodné zabývat se přítomností antivirových programů a firewallů i v nich. Jak již bylo řečeno, jedná se spíše o mikropočítače než o telefony a tudíž se pro ně informace uvedené v této podkapitole vztahují také. V dotazníkovém průzkumu byla položena stejná otázka na antivirové/firewallové zabezpečení i pro mobilní telefony.



Graf č. 9 – Bezpečnostní software v mobilních telefonech.

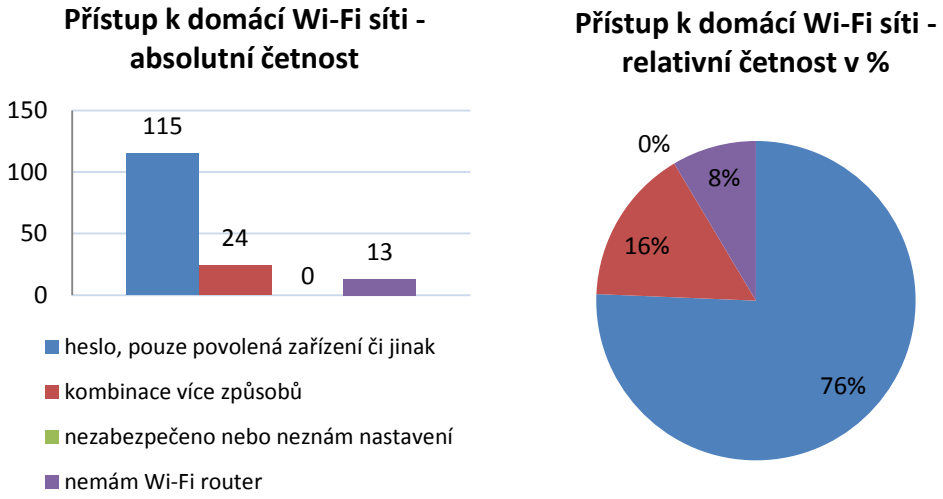
Můžeme vidět, že komplexní zabezpečení v mobilních telefonech je spíše vzácností, a to i přesto, že mnoho lidí své přístroje využívá pro práci s Internetem více než počítače. V případě počítačů lze nízké procento uživatelů přisoudit i faktoru nutnosti finančních výdajů za bezpečnostní služby. Naproti tomu existuje několik kvalitních neplacených bezpečnostních softwarů pro chytré mobilní telefony. Je pravděpodobné, že v budoucnu se bude procento uživatelů zvyšovat a s tím budou možnosti bezplatných možností klesat. Nicméně v současné době tyto možnosti jsou a nízké procento využití neplacených variant lze přisuzovat jen lehkomyslnému přístupu k bezpečnosti dat v telefonu.

4.5. Zabezpečený přenos dat

Jestliže jsme se v předchozí kapitole zabývali bezpečnostním softwarem v koncovém zařízení, nelze opomenout bezpečnost dat na cestě k cílovému zařízení. Ta se může stát slabým článkem přenosu našich dat, před kterým nás sebelepší zabezpečení koncového počítače nemůže ochránit. I v této oblasti existují způsoby bezpečného chování a je třeba se jimi zabývat. Z pohledu běžného uživatele se jedná zejména o dvě hrozby. Tou první je připojování do sítí, které nám zprostředkují připojení do Internetu. V současné době jsou velmi rozšířené bezdrátové sítě Wi-Fi. Ty jsou díky své praktičnosti využívány jak v domácnostech, tak i ve formě možnosti připojit se jednoduše k Internetu na veřejných místech jako jsou hotely, kavárny, obchodní domy, autobusy atd. Úskalí používání této technologie lze rozdělit do dvou oblastí. Tou první je riziko infiltrace do domácí sítě

nezvaným účastníkem. Tomu lze předejít několika způsoby zabezpečení, které lze pokládat za standard, a všechna zařízení k tomu určená tyto možnosti nabízejí. Jedná se o možnost šifrovaného přihlašování, dále možnost přihlášení pouze konkrétních zařízení pomocí tzv. MAC adres, což jsou specifické hexadecimální kódy každého zařízení disponujícího síťovou kartou. Dále existuje nepříliš využívaná možnost skrytého názvu sítě. V takovém případě musí zájemce o připojení do sítě kromě hesla znát i název sítě. Při běžném vyhledávání je taková síť neviditelná. Existují samozřejmě nástroje na odhalení tohoto názvu, nicméně výhodou je, že skryté sítě jsou málo využívané a z pohledu narušitele je složitější řešit tento komplexní problém než „pouze" prolamovat hesla do známých sítí.

Jak ukázal průzkum, uživatelé opět využívají převážně nejjednodušší a nejpřístupnější způsoby zabezpečení, nikoliv ty nejefektivnější. Přesto lze výsledky průzkumu pokládat za více než uspokojivé.



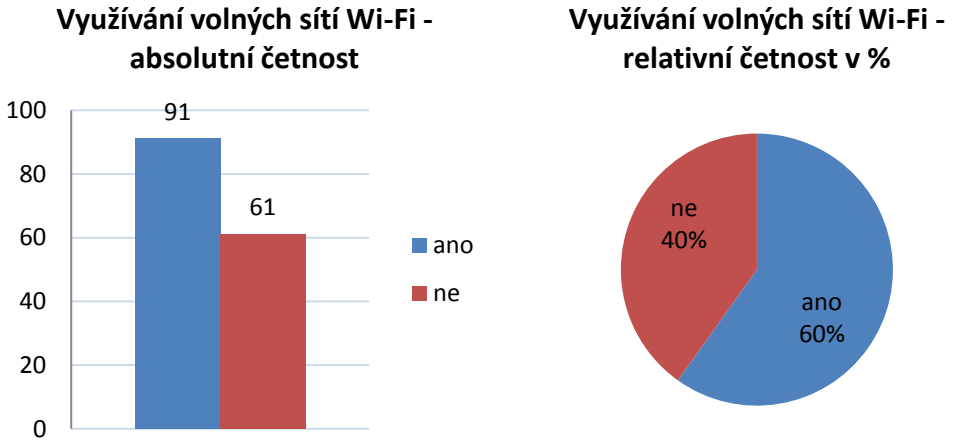
Graf č. 10 – Zabezpečení domácích routerů Wi-Fi.

Ze 152 respondentů se nenašel žádný, který by neměl svůj Wi-Fi router zabezpečen alespoň přístupovým heslem.

Druhým úskalím je připojování uživatele do veřejných sítí. Naše zařízení se stává jejich součástí a podstupujeme tím riziko, že se stává předmětem nám neznámých operací.[47] Je důležité si uvědomit, že ochrana sítě heslem je pouze opatření k přístupu do

[47] PETROWSKI, T., *Bezpečí na Internetu pro všechny,* s. 80

ní. Jinými slovy, nahrazuje kontrolu nad síťovými zásuvkami v případě klasické pevné sítě. V žádném případě tedy není zárukou bezpečnosti jí svěřených dat z našeho zařízení.



Graf č. 11 – Využívání volných sítí Wi-Fi.

Posuneme-li se v procesu přenosu dat o něco dále za hranici místní sítě, připojené k Internetu, i zde můžeme nalézt riziko odposlechu odesílaných dat. Jedná se o to, že uživatelsky není možné zajistit bezpečný přenos dat po celé jejich trase. Internetové spojení z opačných stran planety prochází na své trase mnoha uzly, či spíše desítkami až stovkami uzlů. Na každém z nich může být zařízení, které se bude pokoušet komunikaci odposlouchávat.

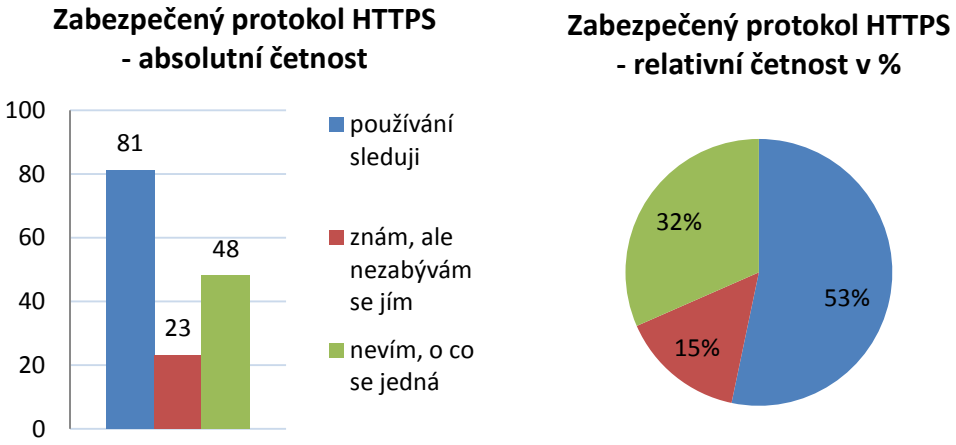
Na obranu proti tomu byl vyvinut zabezpečený protokol HTTPS, který data při odesílání šifruje. V případě nežádoucího zachycení jsou tato data v podstatě nečitelná.[48] Protokol se tedy začal využívat hlavně v případech, kdy jsou do webových formulářů vyplňována osobní nebo jinak citlivá data. Především je využívána provozovateli různých terminálů, platebních společností, bank a dalších institucí pracujícími s financemi.

Přestože je v současné době používání tohoto protokolu již poměrně rozšířené a je používán i v případech, kdy nejsou jeho vlastnosti přímo nutné, stále je potřeba se jeho používáním zabývat. To minimálně z toho důvodu, že se jeho absence na některých webových stránkách může stát jakýmsi indikátorem, že něco není v pořádku.

V běžném životě je třeba si nejčastěji hlídat používání protokolu HTTPS při přístupu k internetovému bankovnictví a při platbě kartou on-line. Znalost protokolu a jeho

[48] PETROWSKI, T., *Bezpečí na Internetu pro všechny,* s. 30

používání v těchto dvou případech bylo i předmětem průzkumu. Kromě jeho znalosti bylo dotazováno i hlídání jeho přítomnosti v obou zmíněných případech.



Graf č. 12 – Znalost a využívání protokolu HTTPS.

Jak je z grafů zřejmé, alarmujících 46,7% uživatelů přítomnost protokolu HTTPS neověřuje nebo jej vůbec nezná. Nyní se ve formě kontingenční tabulky pokusíme vyjádřit závislost znalosti protokolu na používání internetového bankovnictví.

Přihlašování k internetovému bankovnictví v závislosti na znalost protokolu HTTPS	jeho používání na internetových stránkách si při zadávání soukromých dat sleduji	při používání stránek se zadáváním citlivých dat neřeším nebo nevím, o co se jedná
pouze z jednoho (zabezpečeného) zařízení	36 (38,90)	37 (34,10)
z více zařízení (zajímám se o zabezpečení počítače, ze kterého se přihlašuji)	37 (32,97)	23 (28,03)
neřeším zabezpečení nebo nepoužívám	8 (10,13)	11 (8,88)

Tab. č. 3 – Závislost používání internetového bankovnictví na znalosti protokolu HTTPS.

Hodnota testovacího kritéria χ^2 činí 0,503. Jelikož je hodnota nižší, než nalezená tabulková hodnota $\chi_{20,05(2)}$=5,991, potvrzujeme na hladině významnosti 0,05 nulovou hypotézu. Používání internetového bankovnictví na znalosti zabezpečeného protokolu nezávisí, což potvrzuje předpoklad ze zjištěného poměru údajů o počtu uživatelů

s neznalostí protokolu a uživatelů bankovnictví. To je poměrně závažné zjištění, které by nemělo zůstat bez odezvy.

Postup těchto výpočtů a použité vzorce jsou shodné jako v případě kontingenční tabulky na straně 40.

Dalším, neméně důležitým zkoumaným tématem je souvislost znalosti protokolu HTTPS v kombinaci s platbami kartou on-line, které používá 60,53% respondentů. V tomto případě se jedná o téma ještě důležitější a vyžadující více pozornosti, než přístup k internetovému bankovnictví. Webové stránky banky by měly být každému uživateli důvěrně známé, a tudíž se předpokládá větší vnímavost změn a nesrovnalostí. U plateb na Internetu se setkáváme s různými, často i poprvé navštívenými platebními portály a rozlišení těch podvržených tím může být komplikováno. Lze nalézt i stránky, které po uživateli požadují údaje o platební kartě, přestože nejsou s bankami nijak spojeny. To lze často vidět například ve spojitosti s hotelovými rezervačními systémy. Zde je vhodné uvést další příklad z kazuistiky.

Jednalo se o hotel v Itálii, který rezervaci ubytování svých budoucích návštěvníků podmiňoval zadáním údajů z platební karty na svých stránkách. Přestože měl pravděpodobně dobrý úmysl, jeho stránky nebyly dostatečně zabezpečeny a neznámému útočníkovi se povedlo ze stránek tohoto hotelu ukrást údaje o platebních kartách hostů. Jedním z indicií nedůvěryhodnosti těchto stránek byla právě absence protokolu HTTPS. Byl-li by klienty na tuto skutečnost brát zřetel, nemuselo by ke škodám dojít. Kombinace zadávání takto citlivých údajů do nezabezpečených stránek s sebou nese vysoké riziko.

Nyní již k hledání závislosti:

Závislost používání plateb na Internetu v závislosti na znalosti protokolu HTTPS	platím kartou on-line	neplatím kartou on-line
jeho používání na internetových stránkách si při zadávání soukromých dat sleduji	51 (49,03)	30 (31,97)
vím, o co se jedná, ale při používání stránek se zadáváním citlivých dat neřeším	18 (13,92)	5 (9,08)
nevím, o co se jedná	23 (29,05)	25 (18,95)

Tab. č. 4 – Závislost plateb na protokolu HTTPS - absolutní, (relativní) četnost.

Hodnota testovacího kritéria χ^2 činí 6,423. Jelikož je hodnota vyšší, než nalezená tabulková hodnota $\chi_{20,05(2)}$=5,991, zamítáme na hladině významnosti 0,05 nulovou hypotézu. Používání on-line plateb kartou na znalosti zabezpečeného protokolu závisí.

Síla závislosti je pak vyjádřena pomocí Pearsonova koeficientu kontingence C=0,201, vypočteného ze vzorce[49]:

$$C = \sqrt{\frac{\chi^2}{\chi^2 + n}}$$

Jelikož Pearsonův koeficient nenabývá hodnoty 1, je nutné jej normalizovat pomocí tabulkové hodnoty C_{max} a dosadit do vzorce[50] $C_n = \frac{C}{C_{max}}$. Tím získáme normalizovaný koeficient C_n=0,285. Jedná se tedy o slabou závislost.

Můžeme tedy vidět, že v případě používání platební karty on-line je situace se zohledňováním zabezpečeného protokolu o něco lepší než při používání internetového bankovnictví. Přesto jsou oba výsledky velmi slabé a je na místě doporučit na tuto oblast větší zřetel.

[49] SVATOŠOVÁ, L., KÁBA, B., *Statistické metody II,* s. 15
[50] tamtéž

4.6. Policejní statistiky

V České republice se počítačovou kriminalitou zabývají především Kriminalistický ústav Praha (KÚP), odbory kriminalistické techniky a expertiz (OKTE) krajských ředitelství Policie České republiky (PČR) a OKTE Vojenské policie, jehož jsem pracovníkem. Vzhledem k úzké spolupráci s PČR bylo možné pro mapování trendu počítačové kriminality vybrat údaje o počtu vyřízených dožádání z jejich i vlastních přehledů. Ve specifických případech může policie dožádat i soukromé subjekty, ale tato praxe není v běžném životě příliš využívána a statistiky o trendu počítačové kriminality nijak zásadně neovlivňuje.

Pracoviště, ze kterých jsou data o případech čerpána, se z podstatné procentuální části zabývají běžnou trestnou činností ze svého teritoria, ale jsou zároveň dožadována specializovanými útvary policie s celorepublikovou působností, jako je Útvar pro odhalování organizovaného zločinu, Protidrogová centrála, Celní správa apod. Tyto útvary a složky zpravidla rozkrývají závažnější a složitější trestnou činnost, která vyžaduje rychlejší vyřízení, případně dílčí úkony. Nejen z toho důvodu nejsou limitovány oblastními znaleckými pracovišti, ale volí na základě informací o vytíženosti a nabídky termínů vyřízení napříč pracovišti celé republiky a to včetně pracovišť mimoresortních, či soukromých znalců. Tím případem je i Vojenská policie. Primárně je její pracoviště zřízeno pro potřeby Armády České republiky, ale s PČR má uzavřenu meziresortní smlouvu, na jejímž základě policie poskytuje armádě potřebná školení a kurzy pro kriminalistické techniky a znalce. Na druhou stranu umožňuje policii a dalším celorepublikovým institucím zabývajícím se kriminalitou dožadovat o spolupráci právě odborné pracoviště Vojenské policie.

Přestože ve světě existuje mnoho institucí, které se počítačovou kriminalitou zabývají a snaží se jejich statistiky vést, je poměrně problematické tyto informace vyhledávat v kvalitní, zpracovatelné podobě. Počítačová kriminalita je v drtivé většině případů mezinárodní záležitostí, jejíž řešení vyžaduje globální přístup. Přesto je většina těchto zločinů řešena na úrovních státních a statistické údaje jsou tak přístupné pouze v neucelených dílčích měřítkách. Informace o výskytu kybernetické kriminality jsou ve zpracovatelném stavu nejdostupnější z Indie, která však s účelem této práce nekoresponduje a dále z amerického úřadu IC3, který se sice snaží vést informace

o kybernetickém zločinu celosvětově, ale sběr jeho dat neodpovídá rozložení světa a má tak v dlouhodobějším časovém intervalu vypovídací hodnostu spíše pro americký kontinent.

V České republice se komplexněji počítačovou kriminalitou zabývají také některé instituce, jejich krátké působení však bohužel není schopno zpracovatelné informace přinést také.

Složitost, či spíše nemožnost získání relevantních údajů, tedy vyústila ve vlastní provedení sběru dat, jehož výsledky jsou zpracovány dále.

Ze shromážděných údajů o součtu vyřízených dožádání na všech pracovištích (data jsou podrobně uvedena v příloze č. 3) byl vytvořen graf za účelem volby vhodného modelu trendu, ze kterého bude možné co nejkvalitněji odhadnout budoucí vývoj. Zvolená funkce byla verifikována pomocí indexu determinace[51]

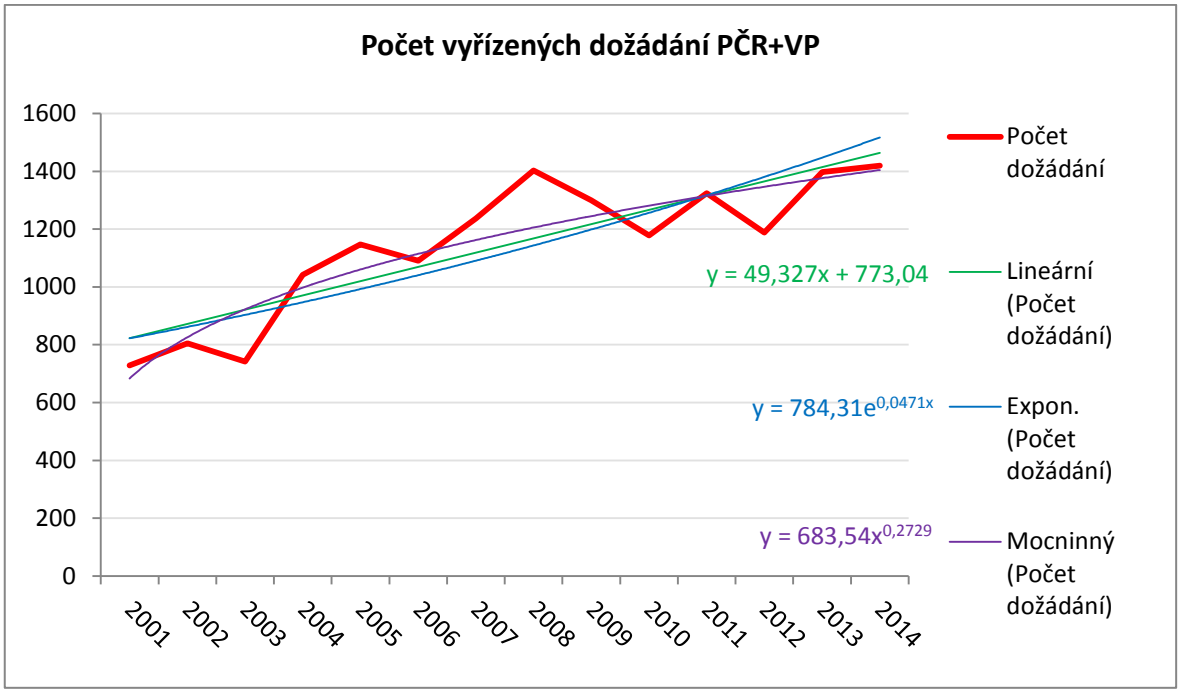
$$I^2 = 1 - \frac{\sum_{n=1}^{n}(y_t - y_t')^2}{\sum_{n=1}^{n}(y_t - \bar{y})^2}$$

ve které vyšlo v případě lineární křivky na 74,95 % vysvětlení celkového kolísání řady a střední absolutní procentuální chyba MAPE (Mean Absolute Percent Error)[52]:

$$MAPE = \frac{100}{n}\sum_{t}\left|\frac{y_t - y_t'}{y_t}\right|$$

která vyšla 8,96, což je pokládáno za dostatečně kvalitní model, nepřekračující hranici 10 %.[53]

[51] SVATOŠOVÁ, L., KÁBA, B., *Statistické metody II,* s. 47
[52] SVATOŠOVÁ, L., KÁBA, B., *Statistické metody II,* s. 46
[53] SVATOŠOVÁ, L., KÁBA, B., *Statistické metody II,* s. 51



Graf č. 13 – Časová řada počtů vyřízených dožádání,
včetně znázornění spojnic trendu.

Obdobné výpočty byly provedeny i pro exponenciální a mocninnou funkci, ale s horšími výsledky a tudíž byla pro výpočet odhadu budoucího vývoje použita právě funkce lineární. Po dosazení následujících let do lineární funkce y_i=773,044+49,327t byl odhad počtu vyřízených dožádání souvisejících s počítačovou kriminalitou na příští tři roky po zaokrouhlení vypočítán následovně:

Rok	Odhad počtu vyřízených případů
2015	1513
2016	1562
2017	1612

Tab. č. 5 – Odhad počtu vyřízených dožádání v letech 2015 – 2017.

V dlouhodobém horizontu můžeme z grafu vidět i přes zřetelné výkyvy vzestupnou tendenci. Dá se tedy očekávat její pokračování. Jelikož se jedná o velmi dynamickou oblast, budoucí ovlivňující faktory se dají jen těžko odhadnout. V každém případě tuto tendenci může bezpečné chování uživatelů Internetu ovlivnit pozitivně ve smyslu jejího poklesu, či alespoň stagnace.

5. Zhodnocení výsledků a doporučení

Z empirické části vyplynulo, že zabezpečení počítačů lze pokládat za relativně dostačující. Nejen přístupová hesla, ale i antivirové programy se staly běžnou součástí používání počítačů a i počet uživatelů s komplexním řešením bezpečnosti činí téměř třetinu. Bude-li se počet používaných komplexních řešení zvyšovat, lze pokládat výsledky za uspokojivé.

Výsledky v oblasti zálohování byly zjištěny na vysoké úrovni a není třeba formulovat doporučení. V úvahu přichází rozšíření používání webových úložišť, která jsou mezi českými uživateli využívána v malém procentu. Jedním z jejich možných využití je právě zálohování. To lze doporučit samozřejmě pouze za dodržování bezpečnostních opatření, jako jsou např. silná hesla.

V tématu přenosu dat byly výsledky rozporuplné. Na jedné straně uživatelé kvalitně zabezpečují své domácí sítě Wi-Fi, na druhé straně v hojné míře využívají volné sítě. To z bezpečnostního hlediska příliš doporučit nelze.

I s ohledem na další výsledky empirické části můžeme bezpečnost zacházení s počítači sumarizovat jako relativně uspokojivou. Přesto je nutné zachovat obezřetnost a formulovat pravidla bezpečného chování, která mohou napomoci tyto výsledky zkvalitňovat.

Naproti tomu se ukazuje, že četná část české populace si navzdory neustále se zvyšujícímu počtu chytrých telefonů stále neuvědomuje nutnost péče o zabezpečení právě těchto svých prostředků každodenní komunikace. Stírající se rozdíl mezi počítačem a mobilním telefon z technologického hlediska tak zdaleka neodpovídá přístupu uživatelů. To, co by v případě osobního počítače považovali za bezpečnostní riskování, nepovažují při užívání mobilního telefonu za hrozbu. Doporučení je proto nutné formulovat především v této oblasti. Na konci roku 2014 používalo chytrý telefon nebo tablet 67 % internetové populace. V témže roce historicky poprvé předstihly chytré telefony (59 %) ty klasické (46

%).[54] V empirickém výzkumu bylo zjištěno, že z celkového počtu uživatelů telefonního přístroje vlastní chytrý mobilní telefon více než 71 % respondentů.

5.1. Hrozby z mobilního telefonu

Jak bylo zjištěno v dotazníkovém šetření, navzdory velkému množství funkcionalit chytrých telefonů nevěnují uživatelé zabezpečení těchto přístrojů dostatečnou pozornost. Z tohoto zjištění lze vyvodit následky, které útočníkova infiltrace do našeho zařízení může mít. Známá je lokalizace přístroje prostřednictvím vysílačů signálu, která je využívána především v souvislosti s pátráním po osobách. Úspěšnost tohoto způsobu je závislá na hustotě osídlení a charakteru terénu oblasti. Hustě osídlené oblasti jsou osazeny větším množstvím vysílačů a lokalizaci tak lze provést přesněji. Naproti tomu výsledky v odlehlých oblastech jsou spíše orientační. GPS moduly v moderních mobilních telefonech jsou však velmi přesné. Při infiltraci a následném vzdáleném přístupu do přístroje se z dat GPS modulu stává mocná zbraň útočníka. Data mohou být zneužívána k nebezpečnému pronásledování, tipování pro vykrádání domů a bytů, krádeže automobilů atd. Na tomto principu funguje i služba vyhledávání počítače/mobilního telefonu, nabízená v rámci softwarů na zabezpečení počítačů. Tato služba začíná být postupně uživateli využívána a to především ve spojitosti s nízkou úspěšností ve vyhledávání ukradených zařízení policií.

Dalším důvodem, proč zabezpečovat data v mobilním telefonu, jsou potvrzovací textové zprávy přijímané při používání internetového bankovnictví. Tento způsob ověřování je účinný při kombinaci používání internetového bankovnictví na počítači a přijímání SMS zpráv klasickým mobilním telefonem. Nástupem chytrých telefonů se jeho efektivita však snižuje. Prvním důvodem je možnost získávat data z telefonu vzdáleně, jak již bylo popsáno. Druhým důvodem je narůstající obliba bankovních aplikací přímo v chytrých telefonech. Verifikační zpráva v tomto případě přichází na stejný přístroj, na kterém jsou prováděny samotné operace. To samozřejmě vědí i útočníci a proto se z útoků na mobilní telefony stává velmi hojně zastoupená oblast počítačové kriminality ve formě phishingu. Více než 48 % veškerých útoků na zařízení s operačním systémem Android,

[54] NET MONITOR, *TZ Smartphony historicky poprvé u uživatelů vedou,* [on-line], dostupné z: http://www.netmonitor.cz/tz-smartphony-historicky-poprve-u-uzivatelu-vedou

využívaný především v mobilních telefonech, bylo zaměřeno právě na získávání SMS zpráv a zjišťování dat z aplikací na mobilní internetové bankovnictví.[55]

Další zneužitelnou funkcionalitu chytrých telefonů představuje možnost pořizovat obrazový a zvukový záznam. V policejní praxi se tak můžeme setkat se vzdálenými odposlechy hovorů či neoprávněným kopírováním multimediálního obsahu pořízeného telefonem. Možnost odposlouchávání mobilních telefonů se tak z oblasti vysoce specializovaných činností dostává k možnosti provádět odposlouchávání telefonu i běžnému uživateli. Jedinou překážkou je nepozorované nainstalování aplikace do telefonu oběti.

Přestože případy z kazuistiky patří spíše do empirické části, je vhodné uvést jeden právě zde. Důvodem je ilustrace kombinace několika závažných chyb, kterých se oběť dopustila a které byly v empirické části rozebírány jednotlivě. Jednalo se o případ z nedávné minulosti, kdy došlo ke krádeži peněz z bankovního účtu. Poškozeným byla osoba z České republiky, která se stala terčem útoku na svá zařízení na dálku z jiného státu Evropské unie. Přestože oběť používala internetové bankovnictví na svém počítači a ověřovací textové zprávy přijímala na svém mobilním telefonu, útočníkovi se podařilo vpravit škodlivé aplikace prostřednictvím e-mailové zprávy do obou zařízení. Spoléhal totiž na to, že většina uživatelů se přihlašuje do své e-mailové schránky z počítače i z telefonu. Pomocí infiltrace do počítače byl útočník schopen odečíst přihlašovací údaje do internetového bankovnictví a tuto infiltraci po sobě následně částečně zahladil. V počítači byl nalezen pouze nestandardní záznam o vzdáleném přístupu, který je jinak v lokálních sítích běžně používán. Do telefonu si oběť pod záminkou vylepšeného zasílání autorizačních zpráv sama nainstalovala z přílohy nastraženého e-mailu aplikaci, která se autorizačních zpráv nejen zmocnila, ale i zajistila, aby se zprávy uživateli na telefonu vůbec nezobrazovaly. Oběť tak nemohla z přijatých zpráv neprodleně reagovat na aktivitu na svém bankovním účtu. Tato aplikace byla při následném zkoumání v telefonu nalezena a jejím rozborem bylo zjišťováno, kam byly zprávy zasílány.

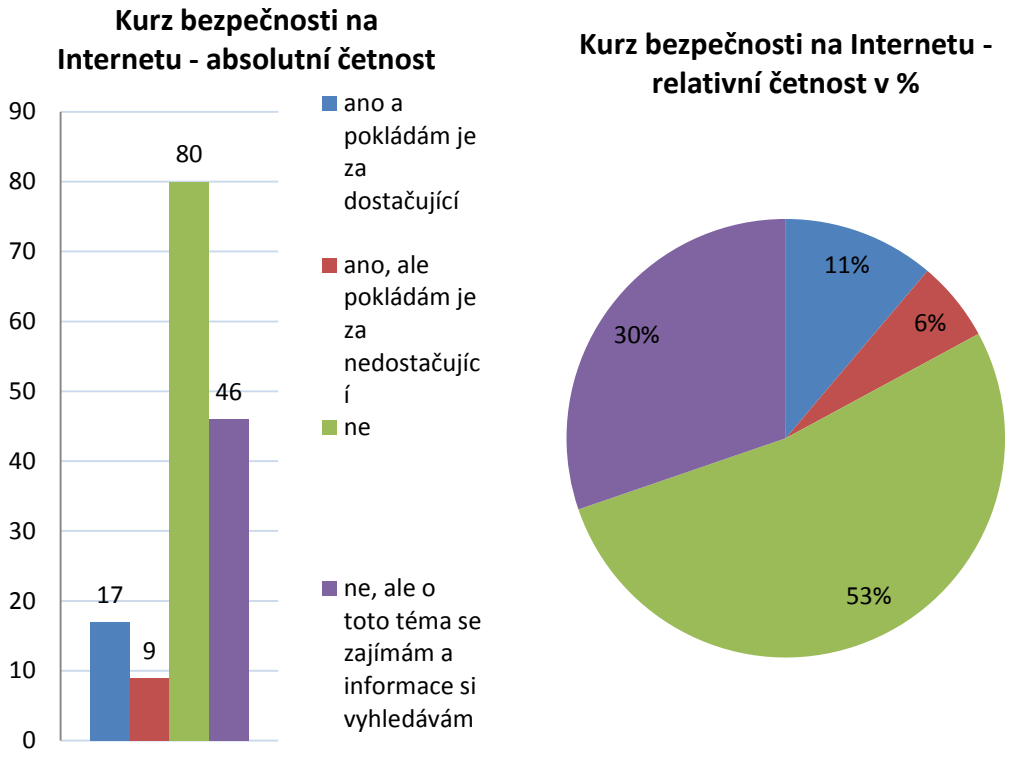
[55] KASPERSKY LAB REPORT. *Financial cyber threats in 2014*, [on-line], dostupné z: http://securelist.com/analysis/kaspersky-security-bulletin/68720/financial-cyber-threats-in-2014-things-changed/

V tomto případě oběť úrovní zabezpečení svých zařízení tento zločin útočníkovi umožnila. V počítači používala pouze antivirový program, který připojení zvenčí neidentifikoval jako hrozbu. V mobilním telefonu nepoužívala antivirový program vůbec. V opačném případě by tento program oběť alespoň informoval o riziku, pokud by instalaci přímo nezabránil. A závažnou chybou byla ruční instalace neznámé aplikace z přílohy e-mailové zprávy. Dále musela oběť ve svém mobilním telefonu vypnout ochranu proti instalaci aplikací z neznámých zdrojů, která je ve výchozím stavu nového přístroje zapnuta.

Phishingové e-mailové zprávy se stávají běžnou záležitostí a je třeba se je naučit rozpoznávat. Jak vyplývá z průzkumu, téměř polovina lidí se již s takovou zprávou setkala. Nelze vyloučit, že takováto zpráva se objevila i ve schránkách ostatních, kteří jej za phishing nepovažovali. Učit se tyto zprávy rozpoznávat je o to důležitější, že se jejich kvalita neustále zvyšuje. Jako jeden z hlavních identifikátorů podvržené zprávy je často prezentována nekvalitní čeština, což je však identifikátor pouze dočasný. Přitom možnosti ověření pravosti zprávy nejsou nedostupné. Hlavním kritériem je ověření adresy, ze které e-mail přišel. Je třeba dbát hlavně na detaily, adresy podvržených zpráv se od těch pravých liší pouze nepatrně. Další možností je zjištění informace o tom, zda banka takové e-maily rozesílá. Asi nejjednodušším způsobem je do banky zavolat s dotazem na takovýto jev. Všechny banky provozují non-stop linky a samy přivítají raději několik dotazů navíc, než aby byly nuceny řešit problémy spojené s touto kriminalitou.

5.2. Osvěta

Z výsledků empirického průzkumu rovněž vyšlo najevo, že v České republice je věnován velmi malý prostor osvětě v oblasti internetové bezpečnosti. Chybí školení pro laickou veřejnost i pořádání kurzů zaměstnavateli, předměty zabývající se touto problematikou nejsou zařazovány do škol.



Graf č. 14 – Otázka na absolvování kurzů internetové bezpečnosti.

Pouze 11 % respondentů si myslí, že prošlo dostačujícím kurzem internetové bezpečnosti. Do jisté míry je toto potvrzeno i výsledkem grafu investic do bezpečnosti informačních technologií v kapitole 4.2 (graf č. 4), ze kterého lze odvodit, že ani investice do chování zaměstnanců nejsou v ČR prioritou, ale spíše záležitostí firem, které se bezpečností zabývají.

Vzhledem k počtu uživatelů Internetu v České republice, který byl v roce 2013 na hranici 70 % populace, by mělo být vzdělávání v oblasti internetové bezpečnosti součástí vzdělávacího systému. Povědomí o bezpečném chování na Internetu by mělo přicházet s prvními kontakty s Internetem samotným a to od rodičů. To může být problematické v situaci, kdy rodiče toto povědomí nemají. Vzhledem k velmi rychlému rozvoji uživatelské základny je tedy nutno provádět vzdělávání na všech úrovních současně.

Nelze jednoznačně určit, která věková skupina lidí je počítačovou kriminalitou obecně nejvíce ohrožena. Některé konkrétnější trestné činy se ve věkových skupinách liší, s jinými se setkáváme napříč věkovými skupinami. V případě dětí útočníci často zneužívají typických dětských vlastností, jako jsou zranitelnost a důvěřivost. Na základě této

skutečnosti dochází k činům, které ohrožují mravní výchovu, či v horším případě vedou ke zneužívání a výrobě dětské pornografie. Ve střední věkové skupině se jedná spíše o činy ve vztahu k majetku a financím, kdy se s rostoucím majetkem této skupiny zvětšují i způsobené škody. Poměrně specifickou skupinou jsou senioři. Značná část této skupiny informační technologie neovládá, či jim nedostatečně důvěřuje a například uživatelů internetového bankovnictví je v ní pouze malé procento. Naproti tomu senioři navštěvují kurzy ovládání počítačů více než jiné věkové skupiny. Mají tedy leckdy více informací o rizicích a jejich chování na Internetu je obezřetnější.

Stejně jako je v poslední době kladen důraz na finanční gramotnost dětí, měl by být kladen minimálně stejný i na bezpečnosti chování na Internetu. Ve školním prostředí výuka počítačů probíhá, ale spíše ve smyslu schopnosti ovládat počítače a programové vybavení. Internet je často chápán jako volnočasová aktivita a schopnost orientovat se v něm tudíž není považována za oblast, které je třeba věnovat odbornou pozornost.

Od roku 2012 se na obrazovkách České televize objevuje osvětový projekt správce domény CZ.NIC pod názvem Jak na Internet, který informuje laickou veřejnost o možnostech celosvětové sítě. Tento pravidelný pořad lze především díky jeho zábavné formě a širokému záběru považovat za velmi zdařilý. Jeho nespornou předností je, že nezřídka zachází i do oblasti bezpečnosti a jejích pravidel a chápe jí jako nutnou součást využívání Internetu. Jeho webová verze pak obsahuje využitelné doprovodné texty a pro zájemce se tak stává kvalitním zdrojem informací ve formě pochopitelné i pro laickou veřejnost.

Dalších zdrojů na toto téma je na Internetu nespočetné množství a v případě zájmu lze nalézt odpověď na jakoukoliv otázku. Většina populace však tyto informace aktivně nevyhledává a je tedy nutné zprostředkovávat je formou školní výuky a jinými formami. Dokud nebudou tyto informace kvalitně zprostředkovávány a zařazeny do systému vzdělávání, lze jednoznačně doporučit, a to i na základě výsledků mého průzkumu, aktivní vyhledávání informací o bezpečnosti na Internetu. Dále je vhodné sledovat nejnovější trendy v oblasti počítačových útoků, které jsou často provázené radami, jak se účinně bránit. Z výzkumu totiž jednoznačně vyplývají zásadní nedostatky v této oblasti.

5.3. Formulace pravidel

V pravidelných intervalech můžeme především z médií slýchávat různá doporučení ohledně zabezpečení svých elektronických zařízení. Zpravidla se však jedná o rady vztahující se k určitému problému nebo události. Zde se pokusíme formulovat pravidla z komplexnějšího pohledu a to především s ohledem na zkušenosti získané při řešení důsledků nahlášené počítačové kriminality. Tato pravidla vychází z konstatování, že v drtivé většině případů útočníci využívají neznalosti či nepozornosti uživatelů. Velmi často došlo k nějakému pochybení uživatele, kterého bylo útočníkem ke spáchání trestného činu využito. Zpravidla se tak nejedná o zcela nové a revoluční způsoby napadání obětí, kterým by tedy nebylo možno zabránit. Dodržování těchto pravidel může o podstatné procento kriminalitu tohoto druhu snížit. Jak již bylo řečeno, je třeba trendy v kybernetické kriminalitě sledovat a tato pravidla podle nich upravovat, případně upřesňovat.

Pravidla:

1) Používat zabezpečené připojení k Internetu a eliminovat tak možnost útočníka odposlouchávat síťový provoz.

   Důležité je využívání ochrany infiltrace do lokální sítě (v domácím případě především kvalitní zabezpečení Wi-Fi routeru). Dále jednoznačně nelze doporučit využívání volných Wi-Fi sítí ve veřejných prostorách. Váš počítač, připojený k volné síti v nákupním centru, se může v krajním případě stát cílem vedle sedícího útočníka.

2) Nenechat manipulovat s počítačem nebo mobilním telefonem nikoho cizího bez dozoru.

   Pro zkušeného záškodníka je instalace špionážního softwaru do počítače nebo mobilního telefonu dílem okamžiku. V tomto případě nám žádný z ostatních bodů této podkapitoly k bezpečnosti nepomůže. Toto doporučení lze zastoupit kvalitním nastavením přístupové překážky k datům v počítači nebo mobilním telefonu.

3) Používat různá a silná hesla.

   Toto pravidlo slouží především jako ochrana před slovníkovými útoky, o kterých bylo pojednáno v předchozích kapitolách. U složitého hesla se navíc snižuje pravděpodobnost, že bude zadávání hesla na klávesnici odezřeno. Pro případ, že k tomu dojde, nebo bude heslo nějakým jiným způsobem odhaleno, je důležité používat více hesel. To se týká hlavně důležitých webových aplikací jako je

internetové bankovnictví nebo jiné servery, kde se operuje s penězi. Pro ty méně podstatné servery, kde nemohou být způsobeny žádné nebo jen minimální škody, postačí jednodušší jednotné heslo.

4) Neinstalovat do počítače ani do telefonu žádný software z pochybných zdrojů.
   Případy z kazuistiky jasně ukázaly, jaké může nedodržování tohoto pravidla způsobit škody. Obecně lze říci, že bezpečnostní softwary nás mohou kvalitně ochraňovat, poslední slovo má ale vždy uživatel. Internetové vyhledávače nám poskytují základní ochranu na určitě úrovni. Největší vyhledávač webových stránek provádí sám základní prověřování stránek, které jsou výsledkem jeho vyhledávání. Problém nastává v další úrovni, kdy klikáme na odkazy přímo v nalezené stránce a ta nás přesměruje na další, která již prověřená není. Taková stránka se pak může pokoušet infiltraci do našeho systému vpravit.

5) Neotvírat pochybné přílohy v elektronické poště.
   Tato oblast je nejnebezpečnější, vyžaduje nejvíce pozornosti a je i nejobtížněji aplikovatelná. Obecně lze říci, že první varování je každý e-mail, který přijde z neznámé adresy. V běžném životě nám jako jednoduchá pomůcka mohou pomoci filtry v e-mailové schránce. Vytvoříme si složky nebo štítky a pomocí automatického filtru nastavíme ukládání například obvyklých výpisů zpráv z banky do přednastavené složky. Ve chvíli, kdy není na zprávu, která vystupuje jménem banky, aplikován tento filtr, je to pro nás jistou indicií, že nemusí být něco v pořádku a nastává tak důvod k bližšímu prověření příchozí zprávy.

6) Nespoléhat se na antivirové a jiné podobné programy.
   Ačkoliv je kvalita mnohých z nich na velmi vysoké úrovni, je třeba tyto programy a jejich používání chápat jen jako pojistku pro případ nebezpečného chování při užívání Internetu. S tímto vědomím je pak potřeba udržovat pozornost nad svým počínáním.

Toto byla obecná pravidla, týkající se pravděpodobně všech uživatelů Internetu. Ostatní doporučení, týkající se užších skupin (například uživatelů sociálních sítí, internetového bankovnictví, on-line plateb, atd.), lze vyvodit z jednotlivých kapitol empirické části.

6. Závěr

Věřím, že práce napomohla čtenářům k uvědomění, že bezpečnost chování na Internetu není doménou hrstky odborníků hovořících v televizi a vývojářů bezpečnostních a antivirových programů, ale že se jedná o oblast, která se týká drtivé většiny naší populace. Nad užíváním Internetu se dnes již nepozastavujeme a chápeme jej jako každodenní součást našeho života. To je podpořeno i jeho prolínáním napříč telekomunikacemi, běžnými domácími spotřebiči i automobily. Naproti tomu vidíme neustále se zvyšující počet kybernetických útoků a s tím i rostoucí počet jejich obětí. Chování obětí se stává zodpovědnější, ale bohužel až na základě špatných zkušeností, které mohou někdy přímo ovlivnit jejich život. Hlavním přínosem této práce by mělo být upozornění na to, že je třeba odpovědné chování při používání technologií vyvolávat dříve, než jsou takovéto zkušenosti uživatelé vystaveni. Zmíněná samozřejmost využívání Internetu by tedy měla být doprovázena stejně samozřejmým smýšlením o potřebě zabezpečení.

Celoživotní vzdělávání v této oblasti je nutné stejně jako jiné činnosti, které považujeme za samozřejmé - psaní, čtení, ochrana osobních dat v neelektronickém styku, atd. Konkrétně doporučuji vzdělávání zaměřit mimo jiné na fakta vyplývající z mého průzkumu, například používání protokolu HTTPS v kombinaci s platebními kartami a bankovnictvím obecně. Nutnost vzdělávání vyplývá i z procenta respondentů, kteří nějakým kurzem bezpečnosti na Internetu prošli. Objevují se v hojném procentu i takoví, kteří pravidla bezpečnosti nedodržují a přesto jsou přesvědčeni, že se bezpečně chovají.

Napříč věkovým spektrem je bohužel stále majoritní skupina uživatelů výpočetní techniky taková, která žádnými kurzy neprošla a lze ji tedy pokládat za samouky. Tato skupina je z pohledu bezpečnosti vystavena největšímu riziku a tedy i tato práce je určena především jí. Počítačovou bezpečnost je nutno chápat jako nutnou součást ICT, což si právě většina této skupiny neuvědomuje. Vyplývá to z potřeby seznamovat se s věcmi nutnými, ze kterých je nějaký užitek. Bezpečnost v tu chvíli stojí bokem a její důležitost si uživatelé uvědomují až ve chvíli, když se nějaký problém přihodí. Závěr, který lze z výzkumu provedeného v této práci učinit je, že současná informovanost populace o počítačové bezpečnosti je stále nedostatečná. Empirická část měla především upozornit na slabá místa průměrného českého uživatele Internetu, která mohou být jedním z hlavních

důvodů stálého nárůstu počtu případů kybernetické kriminality. Jsem přesvědčen, že v případě efektivní osvěty by se nárůst zvyšoval jen v podobě pokusů, nikoliv dokonaných činů. Právě kombinace stále větší tvořivosti útočníků a konstantní nedostatečná pozornost běžných uživatelů v oblasti počítačové bezpečnosti je výsledkem stálého nárůstu.

Případy z kazuistiky měly narušit obecné přesvědčení populace o minimálním riziku postižení počítačovou kriminalitou. Na rozdíl od obecných informací o nárůstu počítačové kriminality přibližují čtenáři reálné projevy konkrétních útoků, jejichž cílem se může stát každý.

Věřím, že práce může posloužit i pro pracoviště zabývající se počítačovou kriminalitou. Tato pracoviště se často při zkoumání předložených stop zabývají způsoby, jakými k infiltracím či jiným druhům zneužití zařízení došlo. Výsledky práce by tedy mohly poukázat na konkrétní aspekty, jimiž uživatelé útočníkům poskytují neúmyslnou „pomoc“ a toto vědomí by se tak v některých případech mohlo stát vodítkem k přístupu samotného prokazování.

Námětem na další samostatnou práci by pak mohl být proces zvyšování uživatelské základny výpočetní a komunikační techniky v rozvojových zemích. Zajímavé výsledky by mohl přinést výzkum ve vztahu vzdělávání v oblasti internetové bezpečnosti při přechodu rozvojových zemí k informační společnosti. Zde je možné vzhledem k nám již známým rizikům tuto oblast informatizace společnosti do tohoto přechodu zahrnout. Je nanejvýš vhodné se tímto tématem zabývat, aby se propast mezi vyspělými státy a rozvojovým světem neprohlubovala i v této oblasti a rozvojové státy se tak nestávaly snadnou kořistí kybernetického zločinu.

7. Seznam použitých zdrojů:

Literatura:

ADÁMEK, Martin. *Spam - jak nepřivolávat, nepřijímat a nerozesílat nevyžádanou poštu.* 1. vyd. Praha: Grada Publishing a. s., 2009. ISBN 978-80-247-2638-0.

CEJPEK, Jiří. *Informace, komunikace a myšlení.* 2. vyd. Praha: Karolinum, 2005. ISBN 80-246-1037-X.

HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech.* 1. vyd. Praha: Triton, 2012. ISBN 978-80-7387-545-9.

JIRÁSEK, Petr, NOVÁK, Luděk, POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti.* 1. vyd. Praha: PAČR a AFCEA, 2012. ISBN 978-80-7251-378-9.

KOLOUCH, Jan, VOLEVECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou.* 1. vyd. Praha: PAČR, 2013. ISBN 978-80-7251-402-1.

MATĚJKA, Michal. *Počítačová kriminalita.* 1. vyd. Praha: Computer Press, 2002. ISBN 80-7226-419-2.

MUSIL, Josef. *Elektronická média v informační společnosti.* 1. vyd. Praha: Votobia, 2003. ISBN 80-7220-157-3.

NAUMANN, Friedrich. *Dějiny informatiky – Od abaku k internetu.* 1. vyd. Praha: Nakladatelství Academia, 2009. ISBN 978-80-200-1730-7. Přeložila Michaela Voltrová.

PETROWSKI, Thorsten. *Bezpečí na Internetu pro všechny*. 1. vyd. Liberec: Dialog, 2014. ISBN 978-80-7424-066-9. Přeložil Tomáš Kurka.

POŽÁR, Josef, KALAMÁR, Štěpán, POKORNÝ, Vladimír. *Základy teorie informační bezpečnosti.* 1. vyd. Praha: PAČR, 2007. ISBN 978-80-7251-250-8.

PROKEŠ, Josef. *Člověk a počítač aneb svítání digitální kultury.* 1. vyd. Tišnov: Sursum, 2000. ISBN 80-85799-82-0.

SMEJKAL, Vladimír. *Internet a §§§.* 1. vyd. Praha: Grada Publishing, 2001. ISBN 80-247-0058-1.

STŘIHAVKA, Marek. *Vaše bezpečnost a anonymita na Internetu.* 1. vyd. Praha: Computer Press, 2001. ISBN 80-7226-586-5.

SVATOŠOVÁ, Libuše, KÁBA, Bohumil. *Statistické metody II.* 1. vyd, 1. dotisk. Praha: ČZU PEF, 2008. ISBN 978-80-213-1736-9.

Další prameny:

HAUERLAND, Miroslav. Jedna z forem zneužití výpočetní techniky k osobnímu obohacení. *Kriminalistický sborník*, 1987, č. 11, s. 669-671

Trestní zákon (Zákon č. 140/1961 Sb.).

Trestní zákoník (Zákon č. 40/2009 Sb.).

Internetové zdroje:

COUNCIL OF EUROPE. *Additional Protocol to the Convention on Cybercrime.* [on-line]. [cit. 2014-09-17]. Dostupné z: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

COUNCIL OF EUROPE. *Convention on Cybercrime.* [on-line]. [cit. 2014-09-17]. Dostupné z: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

DOČEKAL, Daniel. *Adobe unikly údaje 130 miliónů uživatelů*. Lupa.cz [on-line]. 4.11.2013. [cit. 2014-10-02]. Dostupné z: http://www.lupa.cz/clanky/ze-130-milionu-uzivatelu-adobe-melo-heslo-123456-skoro-dva-miliony/

INTERPOL. *Cybercrime*. [on-line]. [cit. 2015-01-04]. Dostupné z: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

JONÁK, Zdeněk. *Informační společnost. KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)*. [on-line]. Praha: Národní knihovna ČR, 2003-[cit. 2014-11-17]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000468&local_base=KTD.

KASPERSKY LAB REPORT. *Financial cyber threats in 2014.* [on-line]. 31 s. (PDF). [cit. 2015-02-28]. Dostupné z: http://securelist.com/analysis/kaspersky-security-bulletin/68720/financial-cyber-threats-in-2014-things-changed/

KASPERSKY SECURITY BULLETIN 2014. *Overall Statistics for 2014.* [on-line]. 31 s. (PDF). [cit. 2015-02-28]. Dostupné z: http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2014/12/Kaspersky-Security-Bulletin-2014.-Overall-statistics-for-2014.pdf

KASPERSKY SECURITY BULLETIN. DARYA GUDKOVA. *Spam evolution 2013.* [on-line]. 22 s. (PDF). [cit. 2015-02-28]. Dostupné z: http://media.kaspersky.com/pdf/LK_KSB_2013_spam_EN.pdf

NET MONITOR. *TZ Smartphony historicky poprvé u uživatelů vedou*. [on-line]. Mediaresearch, a. s. ze dne 28.1.2015. [cit. 2015-02-28]. Dostupné z: http://www.netmonitor.cz/tz-smartphony-historicky-poprve-u-uzivatelu-vedou

OBJEVIT.CZ. *Sociální sítě a jejich vývoj*. [on-line]. 5.3.2013. [cit. 2014-10-02]. Dostupné z: http://objevit.cz/socialni-site-vyvoj-pohled-do-historie-t22280

PWC. *6. ročník globálního průzkumu Digital IQ Česká republika a Slovensko*. [on-line]. 2014. 12 s. (PDF). [cit. 2015-02-28]. Dostupné z: http://www.pwc.com/cz/cs/studie-analyzy/pwc-digital-iq-2014-ceska-republika-slovensko.pdf

PWC. *Celosvětový průzkum hospodářské kriminality 2014*. [on-line]. 2014. 20 s. (PDF). [cit. 2015-02-28]. Dostupné z: http://www.pwc.com/cz/cs/hospodarska-kriminalita/assets/pdf/global-economic-crime-survey-2014-cz.pdf

RADA EVROPSKÉ UNIE. *PRADO.* [on-line]. [cit. 2014-10-02]. Dostupné z: http://prado.consilium.europa.eu/cs/homeindex.html

SCG. *Top 100 Adobe Passwords with Count.* [on-line]. [cit. 2014-10-19]. Dostupné z: http://stricture-group.com/files/adobe-top100.txt

THE OPTE PROJECT. *The Internet.* [on-line]. [cit 2014-09-02]. Dostupné z: http://www.opte.org/maps/

8. Přílohy:

Příloha č. 1 – Dotazník včetně instrukcí.

Příloha č. 2 – 10 nejohroženějších zemí podle počtu stažených škodlivých aplikací.

Příloha č. 3 – Počty dožádání získané z pracovišť Policie České republiky a Vojenské policie.

Příloha č. 1 - Dotazník včetně instrukcí.

Anketa slouží pouze a jen pro získání statistických údajů, jakékoliv informace o respondentech tedy nebudou NIKDE a NIKDY zveřejňovány ani jinak používány!!!

Otázky se vztahují pouze na vlastní techniku, tedy takovou, jejíž nastavení a softwarovou výbavu má uživatel v plné moci.

Prosím o výběr vždy jen jedné z nabízených možností:

1) Jaký je Váš věk?
    a. 15-20
    b. 21-40
    c. 41-60
    d. 61-
2) Vzdělání
    a. základní
    b. výuční list
    c. středoškolské
    d. vysokoškolské
3) Jaký mobilní telefon používáte?
    a. klasický mobilní telefon
    b. s OS Android
    c. s OS Windows
    d. iPhone
    e. Ostatní
4) K zabezpečení telefonu využívám:
    a. heslo, gesto, nebo podobnou překážku pro přístup k datům v telefonu
    b. PIN pro přihlášení do sítě po spuštění telefonu
    c. kombinace výše uvedených
    d. nezabezpečeno
5) K zabezpečení počítače (kromě pracovního, na jehož zabezpečení nemám vliv) používám:
    a. šifrování
    b. přihlašovací heslo
    c. software třetí strany
    d. nezabezpečeno (zapnutí = přihlášení)

6) Zabezpečení domácího Wi-Fi routeru (zařízení pro připojení domácích zařízení prostřednictvím bezdrátové sítě k internetu):
    a. přístupové heslo, přihlášení pouze povoleným zařízením nebo jinak
    b. kombinace více způsobů
    c. nezabezpečeno
    d. neznám nastavení
    e. nemám Wi-Fi router
7) Využívám volných sítí Wi-Fi k přístupu do Internetu (soused, kavárny, obchodní centra atp.):
    a. Ano
    b. Ne
8) Antivir nebo firewall v **mobilním telefonu**:
    a. freeware (antivir)
    b. placené (komplexní řešení)
    c. nepoužívám
9) Antivir nebo firewall v **počítači**:
    a. freeware (antivir)
    b. placené (komplexní řešení)
    c. nepoužívám
10) Služba vyhledávání počítače/mobilního telefonu, obsažené v placených verzích antivirů:
    a. Vyžívám
    b. Nevyužívám
11) Využívám internetová datová úložiště (cloudy) a přistupuji k nim z více zařízení (počítač,
    mobilní telefon, tablet)
    a. Ano
    b. Ne
12) Využívám služeb či stránek kromě Internetového bankovnictví (internetová úložiště, sociální sítě [Facebook, Twitter atp.] pomocí telefonu i PC zároveň
    a. Ano
    b. Ne
13) K internetovému bankovnictví přistupuji:
    a. pouze z jednoho (zabezpečeného) zařízení
    b. z více zařízení (zajímám se o zabezpečení počítače, ze kterého se přihlašuji)
    c. z více zařízení (neřeším zabezpečení)
    d. nepoužívám z důvodu obav o bezpečnost používání
    e. nepoužívám z jiného důvodu
14) Dostal jsem někdy podezřelou e-mailovou zprávu, kterou jsem pokládal za phishing (pokus o získání důvěrných údajů)
    a. Ano
    b. Ne

15) Používám placení platební kartou on-line:
    a. Ano
    b. Ne
16) Zabezpečený protokol HTTPS:
    a. jeho používání na internetových stránkách si při zadávání soukromých dat hlídám
    b. vím, o co se jedná, ale při používání stránek se zadáváním citlivých dat neřeším
    c. nevím, o co se jedná
17) Prošel jsem nějakým kurzem nebo předmětem ve škole zabývajícím se bezpečností na Internetu:
    a. Ano a pokládám je za dostačující
    b. Ano, ale pokládám je za nedostačující
    c. Ne
    d. Ne, ale o toto téma se zajímám a informace si vyhledávám
18) Zálohy dat:
    a. provádím u počítačů
    b. provádím u telefonu
    c. provádím u počítačů i telefonů
    d. neprovádím vůbec

Příloha č. 2 - 10 nejohroženějších zemí podle počtu stažených škodlivých aplikací.[56]

Pořadí	Země	% škodlivých aplikací
1	Vietnam	2,34
2	Polsko	1,88
3	Řecko	1,70
4	Kazachstán	1,62
5	Uzbekistán	1,29
6	Srbsko	1,23
7	Arménie	1,21
8	Česká republika	1,02
9	Maroko	0,97
10	Malaysia	0,93

[56] KASPERSKY SECURITY BULLETIN 2014, *Overall Statistics for 2014*, [on-line], dostupné z http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2014/12/Kaspersky-Security-Bulletin-2014.-Overall-statistics-for-2014.pdf

Příloha č. 3 – Počty dožádání získané z pracovišť Policie České republiky a Vojenské policie.

Rok	t	y_t	ty_t	t^2	y_t'	e_t
2001	1	728	728	1	822,3714286	-94,371
2002	2	805	1610	4	871,6989011	-66,699
2003	3	742	2226	9	921,0263736	-179,026
2004	4	1042	4168	16	970,3538462	71,646
2005	5	1147	5735	25	1019,681319	127,319
2006	6	1091	6546	36	1069,008791	21,991
2007	7	1237	8659	49	1118,336264	118,664
2008	8	1403	11224	64	1167,663736	235,336
2009	9	1300	11700	81	1216,991209	83,009
2010	10	1178	11780	100	1266,318681	-88,319
2011	11	1324	14564	121	1315,646154	8,354
2012	12	1188	14256	144	1364,973626	-176,974
2013	13	1397	18161	169	1414,301099	-17,301
2014	14	1420	19880	196	1463,628571	-43,629