UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
FAKULTA HUMANITNÍCH STUDIÍ
Institut mezioborových studií Brno

Kybernetická kriminalita – zkáza přichází z webu

BAKALÁŘSKÁ PRÁCE

Vedoucí bakalářské práce:
PhDr. Mgr. Zdeňka Vaňková

Vypracoval:
Martin Bartoněk

Brno 2010

Prohlášení

Prohlašuji, že jsem bakalářskou práci na téma „Kybernetická kriminalita – zkáza přichází z webu“ zpracoval samostatně a použil jsem literaturu uvedenou v seznamu použitých pramenů a literatury, který je součástí této bakalářské práce.
Elektronická a tištěná verze bakalářské práce jsou totožné.

V …… dne ……. ……..
Podpis

Poděkování

Děkuji paní PhDr. Mgr. Zdeňce Vaňkové, za odborné vedení konzultací a metodickou pomoc, kterou mi poskytla při zpracování bakalářské práce.

A dále děkuji p. Mgr. Buriánovi R. za korekturu textu, vedoucímu Odboru školství, sportu, mládeže a tělovýchovy ÚMČ Brno-střed p. Nevoralovi J., p. řediteli Základní školy a mateřské školy Kotlářská 4 Brno Mgr. Zřídkaveselému L. a p. profesorce z Biskupského gymnázia Barvičova 85 Brno Mgr. Krumpholcové K., kteří mi umožnili provést výzkum na svých školách.

Martin Bartoněk

OBSAH

Úvod

Díky globalizaci a výsledkům vědeckotechnické revoluce je současný svět stále více těsněji ekonomicky, dopravně, kulturně, ale především komunikačně propojen. Lidstvo na začátku 21. století disponuje širokými možnostmi vědy a techniky, která svou dokonalostí dokáže lidskou existenci ulehčit i způsobit velké problémy. Člověk je bytost společenská a aby dokázal žít, tvořit a existovat i v budoucnu, potřebuje mít pocit jistoty, bezpečí, pořádku a sounáležitosti.

Základy dnešní a hlavně budoucí společnosti jsou založeny především na komunikaci, znalostech a informacích. Velkou úlohu sehrává jejich zpracování pomocí prostředků informačně – komunikačních technologií. Tyto moderní informační technologie (dále jen IT) nalezneme v každé oblasti lidské činnosti, představují tvořivý proces na jedné straně a na straně druhé jsou právě tyto prostředky často předmětem bezpečnostních hrozeb a různé trestné činnosti. V této souvislosti tak můžeme hovořit o sociálně - patologických jevech, počítačové - kybernetické kriminalitě, civilizačních chorobách, o poškozování životního prostředí a dalších.

To vše ovlivnil technologický pokrok, zejména vynález počítače a internetu, který poskytuje obrovský prostor pro nepřeberné množství informací takřka v nulovém čase.

Informace, které proudí v dnešním světě, mají mnohdy charakter citlivých dat a chráněných údajů. Prostřednictvím IT jsou však snadno zranitelné a zneužitelné, proto je potřeba zdokonalovat i oblast právní i legislativní. Pro internet, dle vyjádření Vladimíra Smejkala, *„neplatí žádné zvláštní zákony a je třeba se řídit obecně závaznými normami“*.[1]

V souvislosti s terorismem se pojem internetová bezpečnost v poslední době hodně diskutuje, neboť informace které nabízí, zprostředkovává a sdílí, se člověk snaží „využít – zneužít“ ve svůj vlastní prospěch. A tak důležitost informační bezpečnosti roste geometrickou řadou. Důvod je prostý: stejně rychle totiž rostou útoky proti informačním systémům, lidem, stoupá jejich kvalita i kvantita. Je také statisticky dokázáno, že nezabezpečený počítač připojený k internetu se s pravděpodobností hraničící s jistotou stane terčem útoku cca do deseti minut. Ale i přístroj, který je vybavený aktuálními bezpečnostními programy, odolává útokům a pastím tak dlouho, dokud jeho majitel neudělá nějakou fatální chybu. Většina útoků vedoucích ke ztrátě

[1] SMEJKAL, V. *Internet a §§§*. Praha: Grada, 2. aktualiz. a rozš. vyd., 2001, s. 32

dat, vydírání nebo pomalému fungování počítače, vyžaduje přímou účast naivního uživatele. Před čím se tedy vlastně potřebujeme chránit? Pokud požádáme o taxativní sdělení rizik a hrozeb některé z povolaných osob, dostaneme následující odpověď: hackerské útoky, zneužívání počítačů, dat, utajených informací, instalací zákeřných programů, internetové podvody, sociologické útoky, útoky na děti a další. Dalo by se o tom hovořit ještě hodně dlouho a zcela jistě se ke všem nebezpečím nedostaneme.

Pro svou bakalářskou práci jsem tedy zvolil téma „*Kybernetická kriminalita – zkáza přichází z webu* " proto, že v oboru pracuji již více jak 12 let a ve své každodenní praxi se setkávám a vnímám problémy které s sebou toto médium přináší. Současně je to vysoce aktuální téma, hlavně v souvislosti s nárůstem trestné činnosti v kyberprostoru a jejím vlivem na společnost, především pak na populaci dětí a mladistvích. Dle mého názoru je to jeden z nejnebezpečnějších projevů této doby a neměli bychom mu nečinně přihlížet, vzhledem k vývoji budoucí lidské generace a její bezpečnosti.

Popis problému

V bakalářské práci, která je rozdělena na dvě části, na část teoretickou a praktickou, se snažím postihnout krátce problematiku komunikace a informací, v návaznosti na to historii, vývoj, současnost a okrajově i budoucnost informačních technologií -kyberprostoru jako nejefektivnějšího komunikačního prostředku. Popisuji nevýhody a rizika tohoto fenoménu, zaměřuji se na kybernetickou kriminalitu, definuji její hlavní problémy, jako jsou trendy, hrozby, s nimi spojená rizika, legislativní problémy, problémy policie a justice, společnosti, bezpečnosti i podzemní ekonomiky. Dále zde pojmenovávám nelegální aktivity, které mohou a často přerůstají v trestnou činnost (hacking, cracking, spamming, cybersquating, atd.).[2]

Protože studuji fakultu humanitních studií, obor speciální pedagogika, v jedné z částí se věnuji kybernetické kriminalitě v souvislosti s mladší populací, jakému nebezpečí se sama dobrovolně vystavuje, případně jaké jí hrozí následky a postihy za její jednání.

V praktické části se zabývám empirickým výzkumem přístupu mládeže k internetu, protože mládež představuje budoucnost vývoje civilizace tohoto světa a z jejího chování bychom už nyní mohli mnohé vypozorovat, na co bychom se měli zaměřit a čeho se vyvarovat.

[2] hacking, cracking, spamming, cybersquating - viz. přílohy - slovníček pojmů.

Cíl

Neustále všude skloňovaná bezpečnost, zprávy o virtuální kriminalitě, organizovaném zločinu na internetu, aktuální a hrozící nebezpečí, kdo je jejich obětí a další, mě vedly k napsaní této bakalářské práce. Prakticky všechny děti mají dnes přístup k internetu a část jejich života se tak odehrává ve virtuálním prostředí. Považují to za přirozené a běžné. Chtěl bych tedy provést průzkum na téma „Děti a internet“, jak ho využívají, co na něm dělají, zda je jejich chování nebezpečné, ohrožující jejich psychický i fyzický vývoj, celkově jak si dalece uvědomují hrozící nebezpečí.

Jedním z cílů je připomenout, že klíčové a rozhodující zůstávají dobré vztahy a kvalitní komunikace v rodině, samozřejmě je vždy třeba respektovat věk a individualitu dítěte. Dalším cílem je poukázat nejen na vliv počítačových systémů a informatizaci společnosti, především mládeže, ale i na mechanismy útoků, jak pracují, co je skryto za nebezpečností virtuálního světa, který mnohdy připomíná známou filmovou trilogii Matrix. Bohužel vše, o čem zde budu psát, je reálná součást našeho každodenního života, ať se nám to líbí nebo ne.

Formulace hypotézy

Předpokládám, že v současné době mladší generace dětí nedodržuje základní zásady a pravidla internetové bezpečnosti. Nedostatečně si uvědomují hrozící nebezpečí při on-line komunikaci, sdělují své citlivé osobní údaje, nevyužívají možnost svěřit se s možnými problémy z oblasti kyberprostoru a raději se snaží své aktivity skrývat. Taktéž si plně neuvědomují, že internet není v žádném případě anonymní médium. Často u něj stráví, ať už prohlížením, chatováním, hraním her nebo stahováním, nepřiměřené množství času. Situace v této oblasti z pohledu problematiky dětí je spíše na nižší úrovni vědomostí, a děti tak nemají žádné zábrany, které by je donutily být zodpovědnější.

Metodické zpracování práce

V teoretické části provedu kritickou analýzu dostupných materiálů, odborné literatury z oblasti informačních technologií, kybernetické kriminality a práva. V praktické části zvolím metodu empirického výzkumu, který bude vycházet z informací získaných sběrem dat. Data jsem získal kontaktováním příslušných odborných a odpovědných pracovníků z oblasti školství. Součástí mé práce jsou také konkrétní příklady z oblasti informační kriminality, které se v poslední době objevily. Účelem uvedení těchto příkladů je poukázat na závažnost i nedostatky v právním odvětví a současně přiblížit vysoký stupeň nebezpečnosti pro společnost.

1. KOMUNIKACE - INFORMACE

1.1 VYMEZENÍ POJMU KOMUNIKACE A INFORMACE

Vývoj lidské společnosti je doprovázen vzájemným ovlivňováním jedince a společnosti. Právě tohle ovlivňování posunuje vývoj lidské populace vpřed. K ovlivňování docházelo a dochází ve fyzickém prostředí a jejich aktéry jsou konkrétní jedinci nebo skupiny jedinců. Děje se tak například pomocí různé zábavné činnosti-her, nebo při učení, napodobování blízkých vzorů. Tímto si jedinec vytváří tolik potřebný percepční aparát. Mezilidská komunikace je tak tvořena ze dvou vzájemně propojených a vyrovnaných složek – verbální a mimoverbální komunikace (řeč těla, gestika, mimika, haptika, atd.).

Se zdokonalováním verbální komunikace a vytvářením nových prostředků vyjadřování ustupovala mimoverbální komunikace do pozadí a objevovaly se první příznaky přesunu lidského vnímání do virtuálního prostoru. S trochou přehánění by se dalo říci, že to byly dva vynálezy, které posunuly život člověka do virtuálního prostoru.[3]

***Objev a používání knihtisku**,* který zpřístupnil písemná sdělení širším masám. To však byl jednosměrný tok informací od autora ke čtenáři.

Výpočetní technika a internet - možnost vytváření nesmrtelných virtuálních jedinců, snadný přechod mezi komunitami a potlačená potřeba kompromisů, vedly k vytvoření nového „kybernetického světa“, který se stal pro mnohé jedince snesitelnějším a příjemnějším než svět reálný. Kyberprostor tak představuje další dimenzi v životě člověka, nabývající politické, kulturní, náboženské, emoční a další společenské znaky. Tento prostor akceptuje rysy současné společnosti, ale formuluje si i svá vlastní pravidla, kterým se společnost musí přizpůsobit, přijmout je nebo najít způsoby jak jim čelit, chce-li v kyberprostoru přežít.

Pokud hovoříme o komunikaci, nesmíme zapomenout ani na informace, které jsou nedílnou součástí komunikační existence. Pod tímto pojmem se neskrývají jen události ze společenské nebo vědecké oblasti. V současném období se pojem informace používá v různých souvislostech, například: „informace v daném spise“, nebo „informace ve výsledku nějakého experimentu“, „informace o dané události“ a další. Mnozí odborníci se pokusili o definování pojmu informace, ale do teď se tomu tak nestalo. Jedna z mnoha definic říká, že účelem informací je organizování elementů do systematických

[3] JIROVSKÝ, V. *Kybernetická kriminalita*. Praha: Grada, 1. vydání, 2007, s. 16

celků.[4] Informace je tedy možné považovat za míru organizace, uspořádanosti. Například anglický slovník, vydaný v roce 1987, definuje pojem informace jako: „Information - informing or being informed; something told; news or knowledge given“, jako informování nebo být informovaný, někomu něco říci, dávat zprávy nebo poznatky.[5]

Pojem informace především tvoří základ počítačového světa (kybernetiky), který zkoumá všeobecné zákonitosti procesu řízení, spojení v technických zařízeních, živých organismech a jejich různých kombinací. Můžeme říci, že tato technika zkoumá libovolné organizované systémy, které jsou schopné informace přijímat, udržovat, zpracovávat a následně předávat. Při informaci se předpokládá, že je na blízku příjemce, že je vyjádřena pro příjemce srozumitelným jazykem, že zvyšuje jeho znalost o daném sdělení a má pro příjemce přínosnou hodnotu.

Přestože informace je pouhé sdělení, někdy jen i jednoduché číslo, můžeme se zájmem sledovat, jaké vlastnosti mají systémy, které jsou jejím prostřednictvím organizované. Pozoruhodné jsou i efekty tam, kde je umožněno spontánní vytváření, zpracování a výměna informací v prostředí informační společnosti.[6]

Docházíme tedy k závěru, že ve společnosti, kde není bráněno vzájemné výměně informací, kde je využívána každodenní komunikace, například sdělení si novinek z rodinného života nebo rad ke zkouškám, banální výměna pozdravů, dochází prostřednictvím budování fyzické a logické infrastruktury k rozvoji přirozených základních společenských hodnot, jako je např. rovnost, slušnost, empatie, solidarita, ale především dochází k lidskému zdokonalování a pokroku.

1.2 DRUHY INFORMACÍ – ROZDĚLENÍ

Za ***informace společenské*** běžně označujeme poznatky, které se přenášejí lidskou společností, jsou vytvářené lidskou činností, získáváme je pomocí jazyka nepřímo od jiných lidí nebo je předáváme ostatním. Je to tedy jakýsi obsah vědomí člověka nebo společnosti (společenské vědomí), vyjádřený prostřednictvím jazyka, popřípadě jiného znakového systému, s cílem působit na vědomí ostatních (vyvolat činnost, přesvědčit je, upozornit, atd.).

[4] POLČÁK, R., GŘIVNA, T. *Kyberkriminalita a právo.* Praha: Auditorium; 1.vydání; 2008; s. 12

[5] GREGUŠOVÁ, D., MORAVČÍKOVÁ, A. *Vybrané kapitoly z právnej informatiky.* Bratislava: Vydavatelské oddělení Právnickej fakulty UK, 2000, s. 30

[6] POLČÁK, R., GŘIVNA, T. *Kyberkriminalita a právo*. Praha: Auditorium, 1.vydání , 2008, s. 23

Za ***odborné informace*** považujeme ty, které se dotýkají oblasti vědecko-technických, ekonomických, sociálně ekonomických, nebo ty, které se dotýkají jakékoliv oblasti odborného charakteru. Představují jakousi podmnožinu informací společenských a dělíme je podle různých hledisek.

Naproti tomu ***aktuální informace*** se zase vyznačují tím, že mají určitou vypovídací hodnotu v daném čase. Z toho důvodu je s nimi často zacházeno jako s informacemi, se kterými je možné obchodovat a zacházet jako s majetkem, tedy i krást a ničit. Tuto skutečnost si lidé uvědomují již velmi dlouho a proto se ji snaží patřičně využít. Hodnota informací může být dána rovněž jejich jedinečností, přesností nebo zákonem. Zákon ukládá povinnost chránit informace nejen státním, ale i soukromým organizacím. Jedná se především o informace osobního charakteru a informace ohrožující stát.

Dostatek znalostí a informací hraje např. důležitou úlohu i při vyšetřování počítačového incidentu. Rozvoj komunikačních a informačních technologií je velmi rychlý, a tak publikace s touto tématikou velmi brzy zastarávají. V tomto ohledu sehrávají aktuální informace velmi důležitou roli.

Tímto se dostáváme blíže k problematice informačních a komunikačních technologií (dále jen ICT) – kybernetické kriminalitě a fenoménu zvaný internet. I tady hledají odborníci z oboru kybernetické kriminality informace z posledního vývoje v oblasti bezpečnosti. Ty jim tak mohou posloužit při rychlé orientaci v současných trendech. K nejzajímavějším stránkám patří například:

- konference SANS[7], HTCIA[8] - portál s neustále aktuální tématikou a seznamem všech incidentů na celém světě;
- portály a weby nejrůznějších institucí zabývajících se počítačovou kriminalitou a bezpečností počítačových sítí, můžeme sem například zařadit Computer Security Institute, stránky sítě TechTarget nebo MIS Training Institute.

Nutno říci, že je potřeba zacházet s těmito nalezenými informacemi velice obezřetně, neboť jejich správnost a úplnost není vždy 100%, a to z důvodu neúplnosti nebo ochrany vlastního know-how příslušné instituce.[9]

[7] SANS – Systém Administration Networking and Security Institute - viz. přílohy - slovníček pojmů.

[8] HTCIA – High Technology Crime Investigation Association - viz. přílohy - slovníček pojmů.

[9] JIROVSKÝ, V. *Kybernetická kriminalita.* Praha: Grada, 1. vydání, 2007, s. 261

Pojem informace jako předmět ochrany není v rámci právního pořádku přesně definován. Informace totiž není hmotná, ale pokaždé je zaznamenána pomocí hmotných nosičů nebo signálů. Je tedy potřeba vycházet ze všeobecně známých definicí na jejichž základě je možné vyložit pojem informace jako soubor údajů, který je ve fyzickém dosahu příjemce, je pro něho srozumitelný a po obsahové stránce mu přináší nové znalosti a užitkové hodnoty.

V právním slova smyslu bych informace rozdělil podle toho, jakých nabývají hodnot. Tedy na kvantitativní, kvalitativní a chráněné.

Kvantitativní informace vyjadřují míru informací pro příjemce v konkrétním okamžitém stavu. Množství informací však může obsahovat i poznatky, které se nezakládají na pravdě. Při jejich přenosu může dojít k tzv. informačnímu šumu, způsobeným vnějším prostředím.

Kvalitativní informace vyjadřují míru zvýšení znalostí příjemce, jsou spojeny s abstraktním lidským myšlením a jsou nutné pro rozvoj znalostí a interpretaci konkrétních údajů informace.

Ochrana informací je nesmírně rozsáhlá oblast práva a proto pod chráněné informace můžeme zahrnout právní kategorie, jako je ochrana práv duševního vlastnictví (patenty, know-how, autorské právo apod.), ochrana služebního, bankovního, státního tajemství, ochrana osobních údajů (datové schránky, elektronický podpis) a další.

2. INFORMAČNÍ TECHNOLOGIE

2.1 HISTORIE, VÝVOJ A SOUČASNOST IT

Pro lepší pochopení a uvedení do problematiky kybernetické kriminality bych chtěl také seznámit s historií a vývojem informačních technologií.

Dějiny počítačů začaly možná spíš, než si myslíme. Lidstvo samo začalo počítat nejdříve na prstech, avšak toto mobilní zařízení mělo své limity. Prvním byla paměť, která byla nahrazena škrábanci do dřeva, vrypy do skály apod., jak to dokládají různé archeologické nálezy.

Vůbec prvním strojem, který uměl více než pasivně uložit výsledek, bylo kuličkové počítadlo zvané ABAKUS.[10] Dle historiků jde o vynález, který je tu s námi již dlouhé tisíce let. Jeho vylepšené varianty – ruský „sčot“, ale třeba i čínské a japonské odlišné verze – se stále ještě používají. Pokud bychom chtěli najít něco mnohem náročnějšího, než jsou již zmíněné kuličky na drátě, musíme se přemístit až do dob antiky, kde byly využívány různé stroje a strojky, pro něž dodávali svoje teoretické poznatky místní filozofové a matematikové.[11] Vrcholným kouskem tehdejší doby je tzv. ANTIKYTHÉRSKÝ MECHANISMUS.[12] Známé jsou i jeho parametry: o výpočet se staralo 37 ozubených koleček, vyrobených z bronzu a dřeva. Zatím co účel a konstrukce je známá, dodnes je velkým tajemstvím, jak byly získány znalosti, nutné k sestrojení tak komplikovaného přístroje .

V historii počítačů se najde místo i pro renesančního génia Leonarda da Vinci,[13] když podle jeho náčrtků ozubených kol z konce 15. století byl sestrojen kalkulátor. Byť až v roce 1968.

Stroje podobné těm antickým přicházely na svět až v 17. století, současně s rozvojem matematiky. Mechanické kalkulátory uměly na tehdejší dobu náročné operace, násobení – dělení. Další krok učinil až Charles Babbage,[14] který se věnoval konstrukci počítacího stroje poháněného párou. Stroj byl sice výkonný, ale šlo pouze o spojení mnoha mechanických kalkulaček (velikost menšího domku). Jeho další stroj měl mít více než padesát tisíc součástí, data se měla načítat z děrných štítků, stroj měl mít vlastní paměť a výstup na tiskárnu. Nároky na mechaniku stroje však byly tak velké, že jej nebylo možné sestavit, a tak spatřil světlo světa až při rekonstrukci v roce 1991.

Bouřlivý vývoj zaznamenala počítačová technika před druhou světovou válkou a v jejím průběhu. Vojáci potřebovali počítače ke dvěma účelům. Pro výpočet záměru kanónů a hlavně pro šifrování a dešifrování informací. V roce 1926 začali Němci používat mechanický šifrovací stroj Enigma. Za prapředka dnešních počítačů je však

---

[10] NYGRÝN, P. *ABAKUS* – kuličkové počítadlo, používalo se již přibližně před 5000 lety ve starém Řecku a Římě. Název Abakus je odvozen od řeckého slova abax, které označovalo dřevěnou nebo hliněnou destičku, do níž se vkládaly kamínky - "calculli" - odtud název kalkulačka. Zdroj: http://www.zive.cz/clanky/historie-pocitacu-od-elektronky-po-internet. 05.06.2009

[11] PETRŽELKA, J. Za počátek antické filosofie je považována doba, kdy se od mýtů upouští a přechází se ke kritickému myšlení, které je založeno na zkušenosti a rozumu. Hledá se jiný než božský princip; Milétská škola, Pythagoras, Éleaté, Atomisté (i jejich předchůdci). Zdroj: http://www.phil.muni.cz/fil/antika. 11.07.2009

[12] VELINSKÝ, F., HADRAVOVI, A. a P. *Mechanismus z Antikythéry* - podle aktuálních poznatků nejstarší přístroj pro astronomické výpočty, doba vzniku mechanismu se odhaduje na 150 – 100 let př.n.l. Zdroj:http://www.rozhlas.cz/planetarium/historie/_zprava/629835. 30.08.2009

[13] BOČEK, J. *Leonardo da Vinci* (1452-1519) - všestranná renesanční osobnost, malíř, sochař, architekt, přírodovědec, hudebník a spisovatel. Návrh mechanického kalkulátoru – 1492. Zdroj: http://www.extrahardware.cz/historie-pocitacu-i-pocitacovy-pravek. 15.10.2008

[14] KUČERA, J. *Charles Babbage* – je všeobecně pokládán za tvůrce prvního počítače, jeho poznatky byly využity při výrobě stroje Aritmometr, který se stal později základem pro modernější modely Merchant používané při vývoji americké jaderné bomby. Zdroj: http://www.fi.muni.cz/usr/jkucera/pv109/vystavka/xnezerka_index.html. 11.07.2009

používán ENIAC[15] z roku 1946. Ten spojoval to nejlepší ze svých předchůdců, plnou programovatelnost, digitální výpočty a na tehdejší dobu dosahoval vysoké rychlosti. S hmotností 27 tun byl od dnešních notebooků hodně vzdálen. Další směr poválečného vývoje udávaly ekonomicky nejméně postižené firmy a vojenské laboratoře v USA.[16] V roce 1951 byl vyroben a prodán první sériově produkovaný počítač UNIVAC v počtu 46 kusů. Ve stejném roce se objevila i první počítačová síť, samozřejmě sloužící k vojenským účelům.

K dalšímu velkému kroku v oblasti počítačového světa došlo až v roce 1971, kdy byl představen mikroprocesor, jádro a mozek všech budoucích počítačů, jejichž výroba tímto zaznamenala raketové tempo. Najednou bylo možné sestrojit velmi levně neuvěřitelně spolehlivé stroje. Doba sálových počítačů, které vyžadovaly stálou přítomnost obsluhy, byla pryč. V roce 1981 vstoupila do světa IT firma IBM, která začala s výrobou uživatelských osobních počítačů, které se dostaly takřka do každé domácnosti. V roce 1995 vydává firma Microsoft[17] operační systém Windows. Tímto se stává legendou v oblasti software pro osobní počítače a dochází tak k jejich zpřístupnění i lidem méně znalým.

2.2 HISTORIE, VÝVOJ A SOUČASNOST INTERNETU - KYBERPROSTORU

Mezi tím, ale zcela mimo zájem okolního světa, vznikl v USA přímý předek Internetu – ARPANET,[18] který byl vyvíjen a navržen pro potřeby války. Síť totiž měla být funkční i v případě narušení kteréhokoliv komunikačního kanálu. V roce 1974 se v USA Národní vědecká nadace rozhodla pro osamostatnění, a tak došlo k oddělení části sítě i pro nevojenské účely – dnešní *INTERNET*. Tato síť spojovala superpočítačová centra prostřednictvím telefonních linek a po roce svého založení dokázala propojit na deset tisíc počítačů. Růst počtu uživatelů také přinášel zvýšení počtu informačních zdrojů, které tak mohly být zpřístupněny celé akademické

[15] KUČERA, J. *ENIAC* - elektronkový počítač, který je považován za prapředka dnešních počítačů. Zdroj:http://www.fi.muni.cz/usr/jkucera/pv109/vystavka/xnezerka_index.html, 11.07.2009

[16] NYGRÝN, P. V roce 1947 byl v Bellových laboratořích předveden první funkční prototyp tranzistoru a tím byla zahájena éra miniaturizace. Zdroj: http://www.zive.cz/clanky/historie-pocitacu-od-elektronky-po-internet. 05.06.2009

[17] Společnost Microsoft - založena v roce 1975 (Bill Gates a Paul Allen), tehdejší počet zaměstnanců 11, stávající počet zaměstnanců okolo 95 000 a současný obrat Microsoftu je v průměru bez mála 55 miliard dolarů ročně. Zdroj: http://www.microsoft.com/cze/presspass/msg/20070917_news1.mspx. 11.07 2009

[18] BARTOŠEK, M. *Projekt agentury ARPA* (Advanced Research Project Agency), která koncem 60 let min. st. realizovala vlastní myšlenku, vzájemně mezi sebou propojit jednotlivé existující počítačové systémy. Stalo se tak v roce 1970 v USA první síť ARPAnet spojila univerzity ve státě Kalifornie a Utah. Zanikla v roce 1990. Zdroj: http://www.ics.muni.cz/zpravodaj/articles/22.html. 29.05 2009

společnosti. Postupně dochází k rozšíření tohoto typu sítě a to zejména s grafickým rozhraním WWW (World Wide Web).[19] Tato síť se doslova stává komerční záležitostí. Základním komunikačním prostředkem se prozatím stala elektronická pošta, díky které mohla být uskutečňována rychlejší výměna informací, přenos souborů a v budoucnu videokonference, IP telefonie, řízení důležitých průmyslových odvětví po celém světě a další. Právě proto, že tento kyberprostor nabízí obrovské množství informací, ale umožňuje i pohyb velkých peněžních částek, dochází k tzv. webthreats (ohrožení z webu). Kybernetičtí zloději se již nespokojují s běžnými útoky a krádežemi dat o platebních kartách či osobních účtech. Rozmáhají se krádeže zaměřené na duševní vlastnictví. *Proč ztrácet čas a utrácet peníze za vlastní výzkum a vývoj, když se výsledky dají prostě ukradnout* ?[20] Vznik počítačových sítí - jejich vzájemné propojení v oblasti národní, regionální, evropské a celosvětové - zaznamenal ve vyspělém světě obrovský zájem.

"Internet se přesunul od okouzlení novými možnostmi pro pár jednotlivců k masově užívanému médiu. Služby jsou mnohem propracovanější a profesionálnější. Dříve byl internet spíše kniha na čtení. Dnes je čím dál více naším pomocníkem." podotkl výkonný ředitel portálu Centrum.cz Pavel Mucha.

Přesto internet budoucnosti není zdaleka snadné definovat a ještě obtížnější jej vytvořit. Proto se také v Praze sešli šéfové výzkumných aktivit v informačních a komunikačních technologiích v rámci Evropské komise, politici, představitelé významných výrobců a účastníci evropských výzkumných projektů, aby diskutovali na téma budoucího internetu a učinili efektivní krok k jeho budování. Zaměřili se na strategické směry rozvoje internetu a jejich dopady z hlediska sociálního, ekonomického a na trendy určující budoucí rozvoj informační společnosti.[21]

Již dlouhou dobu se hovoří o internetu nové generace, protože ten stávající přestává stačit rychle se zvyšujícím nárokům na objem přenášených informací, zejména populárního videa (video v reálném čase, videokonference).

[19] KAPOUN, J. Začátek 90 let - Tim Berners-Lee, který pracoval ve švýcarském CERNu (Evropská organizace pro jaderný výzkum se sídlem v Ženevě) na systému pro sdílení vědeckých dat a dokumentů. Vzal za základ to nejlepší z existujících systémů, vše zjednodušil a uvedl do provozu první webový server s prohlížečem. O rok později byl systém veřejně přístupný a začala éra webových stránek. Zdroj: http://businessworld.cz/veda-a-historie/historie-netscape-communications-corporation-1638 30.09.2008

[20] BROŽ, V. *Territory Manager McAfee.* Inc, ICTrevue , vydavatelství Economia, 2009, s. 32

[21] PUŽMANOVÁ, R. *Nové internety. Evropa a my.* Praha: ICTrevue, Economia, 2009, s. 20

Podle posledního výzkumu společnosti Cisco vzroste celkový objem internetových přenosů v příštích čtyřech letech 3,5 krát a na konci roku 2013 tak projde internetem objem dat odpovídající zhruba 10 miliardám DVD.[22]

I počet připojených internetových uživatelů celosvětově rychle přibývá. Na konci roku 2008 překročil magickou metu jedné miliardy. V současné době je již překonána hranice 1,5 miliardy uživatelů. Může za to především Čína, kde je více uživatelů než v USA.

Každý z nás se občas podivuje nad tím, kolik lidí dnes používá internet, a ptá se, zda by je bylo možné spočítat. Podle právě zveřejněné statistiky Evropské komise roste objem internetového provozu každoročně o 60%. Má na tom také lví podíl bezdrátový internet (Wi-Fi),[23] kdy současné čtyři miliardy mobilních uživatelů již z části mohou internet rovněž ze svých mobilních zařízení plně využívat. V roce 2012 má celá miliarda uživatelů používat své mobilní telefony jako jediný způsob přístupu k internetu.

Tím ale příliv nových koncových uzlů internetu nekončí, protože se značně rozvíjí oblast komunikace mezi zařízeními bez přímé účasti lidského činitele. Pro tuto novou technologii se zavedl pojem *Internet of Things (IOT)*,[24] česky internet věcí, a jak předpovídá studie Gartnerů,[25] bude to budoucnost s miliardovými trhy.

2.2.1 Sociální sítě

Sociální sítě, jako celosvětový fenomén dnešní doby, představují rozsáhlý společenský webový systém, který slouží především ke komunikaci mezi uživateli, sdružování členů určitých etnik, sdílení multimediálních dat, navazování nových vztahů a zábavy, ale mimo jiné na ní najdeme i profily firem, institucí, obchodů, hromadných sdělovacích prostředků (masmédií), populárních osobností apod. Tyto sítě nejsou zdaleka jen záležitostí mladých lidí a skoro to vypadá, že kdo je nevyužívá, jako by ani nebyl.

---

[22] ZANDL, P. *Internetový provoz.* Zdroj: www.lupa.cz/zpravicky, 14.07.2009

[23] Wi-Fi - viz. přílohy - slovníček pojmů

[24] ZANDL,.P. IOT- projekt, který má využívat věci po Internetu, např. když se aktualizace ceny v dodavatelském systému bezdrátově přenese na cenovky s LCD displeji nebo elektronickým papírem a rovněž na promo poutače v prodejně, které začnou ihned hlásat novou akci. A nazpět tyto senzory přenášejí informace o tom, kolik lidí se před nimi zastavilo a studovalo cenovou nabídku, aniž by si něco koupilo. Zdroj: http://www.lupa.cz/clanky/internet-veci-internet-of-things. 05.06.2009

[25] Gartner Inc. – konzultační a analytická společnost působící v oblasti ICT. (dříve Gartner Group), Zdroj: http://www.gartner.com/technology/home.jsp. 01.07 2009

Sociálních sítí je spousta a ty nejpopulárnější se těší velké oblibě. Existuje velký počet uživatelů, kteří jsou členy vícero virtuálních komunit, hlavně těch největších a nejznámějších (Facebook, MySpace, Libimseti, Bebo, Skyblog atd.). Všichni víme, že naprostá většina z nich je postavena na takzvaných pozvánkách. Tedy ti, kteří jsou uživateli sítě, rozešlou přátelům (a mnohdy i lidem, které znají jenom podle e-mailové adresy) pozvánku – nabídku přidat se do virtuální party.

Například jedna z nejpopulárnějších a nejnavštěvovanějších sociálních sítí Facebook ohlásila na počátku měsíce května roku 2009 překročení 200 milionů aktivních uživatelů. Dnes už se zde nachází kolem 240 milionů. Poslední tři čtvrtletí roste počet rychlostí mezi 300 až 400 tisíci denně. Aktuálně se však rychlost stále navyšuje a dosahuje už 700 tisíc nových uživatelů denně.

Rychle rostoucí služby sociálních sítí mají obrovský potenciál propojovat a dávat lidi dohromady, jejich zájmy, potřeby, kreativitu, schopnosti, ale stávají se také atraktivnějšími pro kybernetické útočníky. Cestu ke zneužití a podvodům představuje především důvěřivost jednotlivých uživatelů, kteří v rámci sítě svých známých, lidí se stejnými zájmy a těch, kteří se nebojí profilovat na webu, ztrácejí některé základní zábrany.

Na síti si vytvoří svůj vlastní profil - komunitní přezdívku a prozradí na sebe věk, emailovou adresu, místo bydliště i profilovou fotku. Přibližně 60 % členů komunitních webů uvádí i celé jméno, zájmy, koníčky, vlastní fotografie a videa. Zhruba polovina dále zveřejňuje svůj partnerský stav, datum narození, kontakt na komunikační služby ICQ, MSN, Skype či jiný kontakt a údaje o své profesi. Čtvrtina lidí rovněž uvádí své telefonní číslo.

„Není nic lepšího, než sdělit – zpřístupnit svou jedinečnou identitu celému světu! Kam zmizely obavy ze ztráty svého soukromí ?“[26]

Kvůli lidské neopatrnosti se i propouští. Právě zmiňovaný Facebook už připravil o práci i první Čechy. Známý je případ mladíka, který pracoval u velké dopravní společnosti, než na svém virtuálním profilu zveřejnil tržby firmy za jeden pracovní den. Po necelých dvou týdnech si jej nadřízení předvolali s tím, že je propuštěný. Mladíka přinutili podepsat výpověď dohodou.

[26] Vlastní poznámka autora

A není sám, kdo kvůli Facebooku přišel o místo. Proslulost si získal případ třinácti zaměstnanců aerolinek Virgin Airlines (USA), kteří na sociálních sítích pomlouvali pasažéry.

V budoucnosti podobné případy nemusí být ničím výjimečné. Dle vyjádření právníka F.Svobody: *„Právní problémy s internetem budou i u nás více přibývat. Kámen úrazu je v tom, když si mezi „přátele“ přidáte nadřízeného. Má vás pak v podstatě na lopatě, i když to funguje i obráceně. Pro ty, kteří si mezi "přátele" své kolegy a nadřízené přesto přidají, existuje jediná rada: Rozhodně by neměli neuvážlivě psát na svoji „zeď", že se jim nechce do práce, nebo že šli za školu."* [27]

Sociální sítě mají vliv i na ekonomickou oblast. Lidé je totiž „zneužívají v pracovní době. Zaměstnavatelé tím přicházejí zhruba o 1,5% výkonu svých lidí, jako by se z každé stovky zaměstnanců jeden či dva na plný úvazek věnovali klábosení, popichování a komentování fotografií z posledního večírku. Dle průzkumu mezi 237 náhodně vybranými kancelářskými pracovníky se mimo jiné zjistilo, že:

- dvě třetiny těch, kdo mají účet na Facebooku, se k němu přihlašují také v pracovní době a v průměru na něm stráví každý den 15 minut
- 87 % z nich nedokáže vysvětlit, k čemu jim je v práci dobrý
- 6 % z nich se na něj přihlašuje pouze v práci.

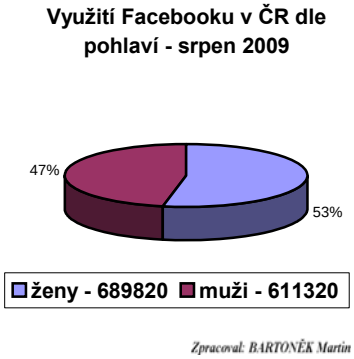
Pro velké korporace představuje Facebook bezpečnostní hrozbu, IT oddělení nemohou kontrolovat obsah zpráv, které si mezi sebou uživatelé posílají, a hrozí tak úniky informací .

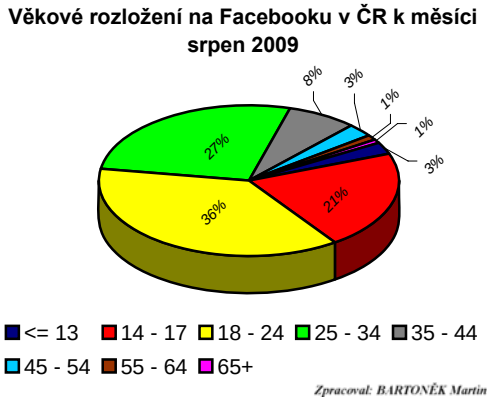
Facebook patří mezi největší a nejprogresivněji se rozvíjející sociální sítě na světě s nejrychleji rostoucím počtem uživatelů. Pozor, v žádném případě ale není anonymní!

V celosvětovém měřítku mají podle odhadů nejvíce uživatelů Spojené státy, kde je na Facebooku téměř 67 milionů účtů. V globálním měřítku to představuje mírně přes 30 % všech uživatelů. Česko pro srovnání má zhruba 0,4 % všech účtů.

[27] WERNER, L. *Kvůli Facebooku se propuští.*
Zdroj: http://www.tyden.cz/rubriky/domaci/kvuli-facebooku-se-propousti-uz-i-v-cesku_129484.html. 20.07.2009

Pro lepší představu jsem graficky provedl znázornění využití dle pohlaví a věkové rozložení sociální sítě Facebook v ČR .[28]





2.3 POSTAVENÍ INTERNETU V INFORMAČNÍ SPOLEČNOSTI

Postavení internetu v dnešní informační společnosti můžeme charakterizovat třemi způsoby:

- ***z technického hlediska*** – představuje tzv. serverové farmy, datové sítě, počítačové stanice
- ***z organizačního hlediska*** – jsou to především provozovatelé, poskytovatelé a uživatelé serverů a komunikačních sítí
- ***z právního hlediska*** – internet nemůžeme označit za právnickou osobu, to znamená, že internet nemůže nabývat práva a povinnosti podle § 18 OZ 40/1964 Sb.

Neopomenutelným znakem právnické osoby je podle § 19c OZ její sídlo, které musí být určeno při zřízení.[29] Internet však svoje sídlo nemá, neexistuje o něm písemná smlouva nebo jeho zakládací listina a nejsou určeny statutární orgány či jiné subjekty, o kterých to stanoví zákon. Dle mého názoru by však šlo označit internet za virtuální osobu, která existuje ve virtuálním prostoru se svou virtuální adresou.

Subjekty právních vztahů jsou tedy samotní uživatelé internetu, vlastníci serverů, sítí a poskytovatelé – zprostředkovatelé internetových služeb, tzv. providers (ISP).[30]

[28] Data byla získána ke konci srpna 2009, ze stránek CheckFacebook.com

[29] Zákon č. 40/1964 Sb., Občanský zákoník, Ministerstvo spravedlnosti, částka 19, ročník 1964

[30] ISP - viz. přílohy - slovníček pojmů

Objektem právních vztahů jsou hmotné i nehmotné objekty, výsledky určitého chování.

Protože jde o poskytování služeb, obsah právního vztahu je založen na smluvním podkladu a můžeme ho definovat jako vtah vzniklý mezi dvěma či více subjekty. Na jedné straně je to poskytovatel a na straně druhé uživatel. V tomto smyslu smluvního vztahu je potřeba věnovat pozornost i obsahu poskytovaných služeb, jejím podmínkám a ceně za tyto služby.

Z právního hlediska zodpovědnost za provozování – chod internetu a závazkové vztahy z toho vyplývající nejsou zařazeny v právním pořádku, přestože existuje odpovědnost za obsah či funkčnost jednotlivých serverů. Z toho důvodu se na internet pohlíží jako na přenosové médium, které umožňuje využívat nabízené služby. Právní režim se řídí dvěma principy:

- ***primární princip teritoriality*** – zde se uplatňuje právo země, kde je služba poskytována (sídlo poskytovatele služeb, případně umístění serveru);
- ***sekundární princip práva*** – upravující druh činnosti, která je tímto způsobem realizována, bez ohledu na médium (autorský zákon, obchodní, občanský zákoník apod.).[31]

Stále více lidí i neodborníků si začíná uvědomovat, že na internetu platí nějaké normativní systémy – i když přesně nevědí, co to je. Normativní systémy jsou totiž nástrojem regulace společenských vtahů a k jejich vzniku, změnám a zániku dochází i v prostředí internetu. Ve skutečnosti se jedná o normy právní, mravní (etické), technické (RFC)[32] a další. Vynutitelnost těchto norem se značně liší.

Normativní soustava RFC je založena na principu dobrovolnosti, dohod, společných politik a pravidel, jejichž závaznost není obecná. Ale přesto je většina dodržuje, protože by jinak nebylo možné propojení celého internetu. Za schvalování a vydávání dokumentů RFC odpovídá více společností (IETF-Internet Engineering Task Force, IESG - Internet Engineering Steering Group, ISOC – Internet Society). Pokud to zobecníme, tak žádné standardy internetu nejsou závazné. Jsou jen specifikací, které slouží pro širokou internetovou obec, kde prochází zkouškou užitečnosti, pro případné použití v navrhovaných normách.

Etické normy internetu jsou spojeny s pravidly společenského chování. Jedná se tedy o etická pravidla při používání počítačových sítí, jejichž vynutitelnost je skoro

[31] PAUKERTOVÁ, V. *Elektronická informační kriminalita.* Zdroj: http://www.ikaros.cz, Vydáno: roč. 10, č. 8-2006, 30.09.2009

[32] RFC - viz. přílohy - slovníček pojmů

nulová. Ale to konec konců platí i pro pravidla společenského styku v reálném životě. Na internetu je nedodržování sice zdánlivě jednodušší (anonymita), na druhou stranu sankce mohou být rychlejší a účinnější (zrušení přístupu na mail-server, omezení možností, zahlcení emaily, atd). Porušování mravního chování může za určitých okolností vést k přestupku nebo trestnému činu.[33]

3. PŘÍSTUP K PROBLEMATICE

3.1 ÚVOD DO PROBLEMATIKY ELEKTRONICKÉ INFORMAČNÍ KRIMINALITY

IT technologie jsou nasazeny téměř do všech oblastí soukromého a společenského života – vzdělání, zdravotnictví, průmysl, ekonomika, veřejná správa, bezpečnostní složky atd. Pro svou činnost využívají právě informace, které jsou více než kdy jindy vysoce ceněnou devizou. Jedná se o různé obchodní informace a převážně citlivé údaje, jejichž zpracováním dochází k tzv. „digitalizaci dat“,[34] aby mohly být později využité i pro další potřeby a systémy. Při tom ale zároveň umožňujeme jejich zneužití. I když jsou snahy zabezpečit počítačovou - komunikační infrastrukturu před napadením, doporučují se stále nové programy nebo zařízení pro ochranu systémů a existují desítky firem, které dodají bezpečnostní řešení, přesto na internetu kolují stovky návodů, jak tato opatření obejít. Počet útoků přes internet se neustále zvyšuje a ten se tak obrazně řečeno může stát skutečným novodobým bojištěm. Informační válka v „tradičním“ pojetí představuje především nepovolenou manipulaci s informacemi.

3.2 TRENDY EL. KRIMINALITY – KYBERNALITY

To, že IT představují obrovský přínos pro lidskou společnost a v případě zneužití se stávají velmi nebezpečnou zbraní, je všeobecně známé. Svědčí o tom i v poslední době se zhoršující bezpečnostní situace v důsledku rozšiřující se globalizace.

Například pokud se zkušení hackeři dostanou k utajeným vojenským informacím, mohou zjistit počty vojenských jednotek, podrobnosti o zbraních a zvláště citlivé informace o vojenských komunikačních systémech. Příkladem může být i případ

[33] SMEJKAL, V. *Normativní systémy a Internet.* VŠE v Praze a VUT v Brně, Zdroj: http: www.znalci.cz, 03.09.2009

[34] Digitalizace dat – převod stávajících záznamů do elektronické formy

veřejného webového serveru Armády České Republiky (http://www.army.cz) z roku 1996, kdy o tom Mladá Fronta Dnes napsala:

„... Computerový nadšenec, který první listopadový víkend vnikl do počítačového serveru armády a z recese tam pozměnil informace, nebude pravděpodobně nikdy odhalen. "Takoví lidé za sebou umějí zametat stopy," míní odborný asistent skupiny počítačových sítí brněnské vojenské akademie Ladislav Hagara. Uživateli, jenž si zvolil příslušnou internetovou adresu, se začátkem měsíce objevil na obrazovce počítače místo informací ministerstva obrany nápis Leo s fotografií dvou nahých žen. Pod snímkem byl nápis: Lidé spěte klidně, nad Vámi bdí Armáda České republiky. Text pak upozorňoval na to, že na armádních stránkách lze najít informace o špionážních akcích, úplatkářských aférách a výrobě semtexu. Vtipálek se podepsal jako voják Švejk.“ [35]

V roce 2000 byli zase na rok těžkých prací odsouzeni dva ruští univerzitní studenti, kteří se v elektronické komunikaci vydávali za raketové důstojníky zplnomocněné vypustit rakety s jadernými hlavicemi. Hackeři stále častěji zasahují do ozbrojených a diplomatických konfliktů, které se týkají jejich národa. Opět ruský případ z roku 2002, kdy byla zaznamenána aktivita jisté skupiny z Tomska, která vedla soukromou elektronickou válku proti rebelům v Čečensku. Je to vlastně způsob vedení kybernetické války. Ačkoliv by se mohlo zdát, že se jedná o zcela nový fenomén, ve skutečnosti probíhá už téměř šedesát let.[36]

Opravdový kybernetický boj zatím sice nevypukl, i když už byly provedeny útoky na infrastrukturu samotných států. Poprvé si to zažilo Estonsko v roce 2007, kdy odstranilo sochu ruského vojáka z talinnského náměstí na vojenský hřbitov. Hackeři ukázali, že jsou schopni během několika minut vyřadit z provozu většinu infrastruktury pobaltského státu. Je také známo, že válka v kyberprostoru je jednou z priorit Pekingu a že časté útoky na síť americké vlády a vlád dalších zemí zřejmě pocházejí z Číny. Podle listu The Wall Street Journal se pirátům už podařilo nabourat do nejdražšího amerického zbrojního programu, projektu stíhaček F-35. Čínským a ruským

[35] Časopis Policista, Hacker. Zdroj: http://web.mvcr.cz/archiv2008/casopisy/policista/2006/01/hacker.html.
Vyšlo v čísle 1/2006 Policista, 15.03 2009

[36] HYRMAN, M. *Kyberválka.* Nové možnosti vedení boje v 21. století.„V průběhu druhé světové války bylo kyberntiky využito při použití elektronických zbraní. První závažnější útok byl zaznamenán v roce 1994 v New Yorku, kdy systémoví administrátoři zjistili, že někdo zaútočil na síť amerických vojenských systémů. Bylo objeveno obrovské množství průniků z desítek různých zemí.
Zdroj: http://www.zive.cz/clanky/kybervalka-nove-moznosti-vedeni-boje-ve-21-stoleti/sc-3-a-146695/default.aspx. 22.04.2009

kyberšpionům se také několikrát povedlo proniknout do amerického elektrického rozvodného systému.

Též se vedou skryté bitvy mezi systémovými správci a hackery nejrůznějších zájmových skupin. V současné době jsou útoky stále intenzivnější, těžko odhalitelné a způsobují obrovské škody. Kyberzločin funguje organizovaně a vydělává „mafiím" podobně jako drogy.

K nežádoucím účelům lze v kyberprostoru využít i běžné počítače připojené do internetu, tzv. bootnet.[37] Těchto rizik v poslední době existuje opravdu mnoho.

Ve vztahu k pojmu kybernetická válka je potřeba říci, že je dnes vnímána jako určitá forma války na internetu, která se soustřeďuje na software a hardware. Je verzí informační války, neboť jejím cílem je rychlé získání, ovládání informací a následná počítačová analýza.

Mezi původce řadíme tradiční a nové teroristické organizace, sektářská, extremistická a radikální náboženská hnutí, nově také kybermafie. Tyto skupiny mezi sebou uzavírají různá účelová spojenectví a tím ohrožují systém chránící základní lidská práva. Snaží se systémy elektronických, informačních a komunikačních sítí ovládnout nebo alespoň poškodit. Patří sem i uživatelé internetu, kteří provádějí nezákonné aktivity pod falešnou identitou, díky níž ztrácejí zábrany, které by měli v reálném světě. Technika a internet umožňuje těmto lidem daleko snadněji než dříve páchat trestnou činnost, jako jsou krádeže, průmyslové špionáže, padělání, šíření pornografie, rasismu, extremismu, vydírání, kyberšikana, cyberstalking atd. Rozsáhlé úniky strategicky důležitých dat, informací, zásahy do informačních systémů podniků, organizací, společností, ať státních či soukromých, které zajišťují základní funkce společnosti, mohou ohrozit nejen strategické, ale i životní zájmy světa.[38]

V této souvislosti se v Praze v dubnu 2009 konalo zasedání na téma bezpečnost, které organizovalo české předsednictví.[39] Zasedání k tématům spravedlnosti a vnitra se konalo za účasti Česka (v té době předsednické země Unie), Evropské komise a USA. Komisi zastoupil komisař pro právo a bezpečnost Jacques Barrot, na jednání přijeli též

[37] Bootnet - viz. přílohy - slovníček pojmů

[38] Dle schválené Bezpečnostní strategie České republiky, 10.12.2003, s. 9 čl. 28

[39] ČTK –Do Česka přijeli i američtí ministři pro vnitřní bezpečnost a pro spravedlnost Janet Napolitanová a Eric Holder. Jednali o fungování amerického bezvízového internetového systému ESTA, boji proti terorismu či ochraně hranic. České ministerstvo vnitra na schůzce zastoupil ministr v demisi Ivan Langer.
Zdroj: http://www.ctk.cz/sluzby/slovni_zpravodajstvi/vseobecne/index_view.php?id=373593. 01.05.2009

ředitelé Frontexu,[40] Eurojustu[41] a Europolu,[42] tedy unijních organizací zabývajících se bezpečností a policejní spoluprací.

Například nedávné události z německého Winnendenu, kdy sedmnáctiletý mladík tam ve své někdejší škole a jejím okolí zabil 15 lidí, donutily všech 27 členských států EU koncepčně se zabývat násilím mládeže, které se často projevuje i na školách.[43] Podle ministrů vnitra Německa, Francie, Itálie, Španělska, Británie a Polska je třeba především zjistit příčiny násilností mezi mládeží, kteří mnozí spatřují právě v roli internetové komunikace a celé této oblasti. Přesto chce EU v boji se zločinem využít právě internet. Hodlá prosadit zákon, který by umožňoval policejním vyšetřovatelům odposlouchávat hovory podezřelých osob uskutečňované pomocí různých internetových programů, jakým je například Skype.[44]

S návrhem takzvaných internetových odposlechů přišla evropská agentura Eurojust. Bezpečnostní odborníci a přední evropští kriminalisté se totiž shodují, že komunikace podezřelých osob, potažmo zločinců, se čím dál více soustředí v internetovém prostředí, namísto klasických telefonních komunikačních kanálů. Celý projekt je zatím v přípravné fázi. Představitelé Eurojustu se hodlají postupně setkat se zástupci všech států sedmadvacítky a diskutovat o tom, jak návrh implementovat do jednotlivých právních systémů zemí a jak ho realizovat po technické stránce.

Právě na technické obtíže by ale možné odposlouchávání hovorů mohlo narazit či ztroskotat. Například zmíněný program Skype, který po celém světě využívá zhruba 350 mil. uživatelů, je podle odborníků takřka neodposlouchávatelný. Do cizích účtů aplikace se v minulosti nepodařilo proniknout ani specializované společnosti, jež si právě pro podobné účely najala bavorská police. Navíc panují obavy, aby společnosti, které služby volání přes internet poskytují, spolupracovaly. Společnost Skype ale už evropské instituce předem informovala o konkrétních detailech vlastní aplikace a hodlá být v rámci projektu nápomocna. Podle mluvčího Eurojustu Joannese Thuye, ale i dalších unijních představitelů, by měly zmíněné odposlechy sloužit pouze v boji proti

---

[40] Frontex - Evropské agentura se sídlem ve Varšavě poskytuje koordinační podporu členským státům EU/Schengenu v rámci ochrany vnějších hranic EU; Zdroj: http://www.frontex.europa.eu. 01.05.2009

[41] Eurojust Evropská jednotka pro justiční spolupráci, orgán EU, který byl zřízen v roce 2002, aby podporoval a zdokonaloval koordinaci při vyšetřování a trestním stíhání mezi příslušnými soudními orgány v členských státech EU, jež se zabývají závažným přeshraničním a organizovaným zločinem, Zdroj: http://www.eurojust.europa.eu. 01.05.2009

[42] Europol - Evropský policejní úřad byl zřízen v roce 1992 s cílem zajistit celoevropské zpravodajství v oblasti trestné činnosti.Úřad sídlí v Haagu a k jeho zaměstnancům patří zástupci vnitrostátních orgánů pro prosazování práva (zástupci policie, celních úřadů, úřadů pro přistěhovalectví, atd.). Ve Správní radě má každý členský stát EU jednoho zástupce.Cílem Europolu je napomáhat členským státům EU v užší a účinnější spolupráci, při předcházení mezinárodního organizovaného zločinu a v boji s ním., Zdroj: http://www.europol.europa.eu. 01.05.2009

[43] BUCHTA, P. ČTK/AP, Český rozhlas Radiožurnál, 26.06.2009

[44] Skype - viz. přílohy - slovníček pojmů

organizovanému zločinu a běžných uživatelů by se neměly týkat.[45] Momentální situace je však taková, že dříve než se zákon a projekt odposlechů podaří prosadit, komunikační program SKYPE skončí sám o sobě. Ohrožují ho právní spory mezi tvůrci programu a novým vlastníkem, společností eBay.[46] Už proto je takový zákon potřebný z jednoho prostého důvodu. Nikdo nemůže zaručit že nevznikne podobný program pro telefonickou a textovou komunikaci přes internet a svět se tím dostane do podobné, ne-li složitější situace.

Nedávné události ze srpna 2009 svědčí o tom, že proběhla největší změna v internetovém undergroundu[47] za poslední tři roky. Romantika objevování možností nového virtuálního světa totiž skončila. Jen o pár kliknutí dále, například od nejpopulárnějšího vyhledávače Google, dnes začíná „Divoký západ". Nabízející se možnosti nového prostoru totiž objevila „mafie". Dokonce se pořádají i celosvětové konference, kde si rozdělují svá teritoria. Mladí počítačový experti se tak mohou rozhodnout, zda svou kariéru spojí s velkou IT firmou, nebo se spojí se silami stojící na opačné straně. Každý měsíc hlásí agentury po celém světě případy krádeží citlivých dat nebo phishingových útoků na klienty bank. Viz nedávný případ zatím největší krádeže identity na internetu, odhalené americkým ministerstvem spravedlnosti v srpnu 2009. Tehdy byly ukradeny údaje 130 milionů kreditních karet.[48]

Na Světovém fóru z Davosu 2009 bylo zaznamenáno, že se v tomto světě nejedná o pouhý vandalismus nebo adrenalinový zážitek, ale o organizovanou kriminalitu. Zástupci velkých internetových firem, jako jsou Microsoft, McAffe, Symantec a další, spočítali roční náklady a ztráty v boji s internetovou kriminalitou na jeden bilion dolarů. Podle antivirové společnosti Sophos se takto „nakažené" stránky objevují na webu každé čtyři vteřiny. Viry pronikly například i do komunitní sítě Facebook, kde své soukromé údaje zveřejňuje přes 200 milionů lidí z celého světa. Osmdesát procent infekcí je přenášeno právě přes oficiální weby. Trojské koně se objevily i na webu irské vlády.

[45] KULHAVÝ, V. *Skype otevírá vývojářské centrum v Praze.*; Čro 1 Radiožurnál – rozhovor; 01.05.2009

[46] HRON, M *Budoucnost skypu je nejasná.* Zdroj: http://mobil.idnes.cz. 10.08.2009

[47] Underground - viz. přílohy - slovníček pojmů

[48] VANČUROVÁ, K. *Největší krádež na internetu.* Zdroj: http://www.mediafax.cz. 18.08.2009

3.3 PROBLÉMY KYBERNALITY

Opět se vracíme k informacím. Ať už jsou informace zaznamenávány jakýmkoliv způsobem, tak kvůli jejich hodnotě je nutné věnovat pozornost i jejich ochraně. Aby se data uložená v elektronických informačních systémech dala využít, musí systémy komunikovat se svým okolím. Nemůžou být zcela izolována, protože pak by byla nepoužitelná. V oblasti zabezpečování obyčejně platí velmi úzká spojitost mezi bezpečností, náklady na bezpečnost a použitelností - uživatelskou přívětivostí. Svou úlohu zde tedy sehrává i ekonomická stránka. Proto je nutné při zabezpečování systému pochopit a uvědomit si několik následujících problémů.

3.3.1 První problém - hrozby a s nimi spojená rizika.

Co rozumíme pod pojmem hrozba a co pod pojmem riziko.

Hrozba: z bezpečnostního hlediska tím rozumíme jakýkoli proces, který má schopnost poškodit zájmy jedince či společnosti, který může vést k nežádoucí změně informace, chování systému nebo změně jeho parametrů. Může být dvojího druhu. Buď je způsobena přírodními, na lidské činnosti nezávislými jevy (vyšší moc), nebo je způsobena úmyslným jednáním jedince – skupiny (personální ohrožení).

Vyšší mocí jsou myšleny všechny jevy, které nelze ovlivnit (přírodní katastrofy, požáry, výpadky energie, apod.). Ochrana proti většině těchto rizik bývá velice složitá a nákladná, proto se mnohdy omezujeme pouze na možnosti odstraňování následků a minimalizaci vzniklých škod. Protože v těchto případech je obvykle současně s informací poškozeno i něco hmatatelného, bývá většinou myšleno na tento druh ohrožení. Podniky uzavírají všemožná pojištění, nakupují záložní zdroje apod.

Personální ohrožení za ně považujeme každou hrozbu plynoucí z působení člověka. Můžeme je klasifikovat jako úmyslné (např. průnik útočníka do sytému, prozrazení dat důvěrného charakteru – únik informací, porušení konzistence dat – jejich změna nebo vymazání, úmyslné bránění legitimnímu subjektu k přístupu k informacím či jiným systémovým zdrojům) i neúmyslné (zde ohrožení systému vzniká například chybou operátora, oprávněného uživatele, samotného systému - softwaru). Pro dosažení rozumné ochrany proti personálnímu ohrožením je potřeba průběžně vynakládat odpovídající úsilí na školení obsluhy a uživatelů, na kontroly dodržování předpisů, na obnovu a vylepšování technických prostředků a zdokonalování bezpečnostních i legislativních norem.

Riziko: z bezpečnostního hlediska tím rozumíme, že s určitou pravděpodobností nastane událost, kterou budeme považovat za nežádoucí. Riziko tak vždy odvozujeme z konkrétní události nebo hrozby. Dále posuzujeme míru rizika, tedy pravděpodobnost škodlivých následků, které vyplývají z hrozby. Provádíme tzv. analýzu rizik, kde zohledňujeme a posuzujeme i připravenost takovýmto hrozbám čelit. Lze je pojmenovat několika způsoby :

Nedostupnost - základní, přesto ne vždy nejkritičtější hrozba. Systém by měl být postaven tak, aby chránil poskytované či zprostředkovávané služby takovým způsobem, kdy musí být potlačeno riziko jejich znehodnocení nebo znepřístupnění bez oprávnění (útoky způsobující nepřístupnost služby – DoS).

Vyzrazení, neoprávněnost - hovoříme-li o bezpečnosti dat, systém by měl být koncipován a schopen chránit data (informace) před přečtením nebo zkopírováním nepovolanou osobou (neoprávněným uživatelem). Ochrana před vyzrazením se netýká jen informací jako takových, ale i jednotlivých drobných údajů, které jsou samy o sobě neškodné, ale mohou být použity k získání jiných již kritičtějších informací.

Vymazání, modifikace a podvržení – neméně důležitá je také ochrana integrity dat a rizika spojená se zpracováním podvržených informací. Mezi citlivé informace přitom nepatří jen účetní záznamy, záložní pásky, časové údaje o souborech a dokumentace, ale i korespondence (e-mail), osobní údaje zaměstnanců, informace o partnerech apod. Málokdo si tato rizika uvědomuje, a proto musí systém poskytovat prostředky, jak zjistit, že daná informace je poskytována oprávněným uživatelem (např. kvalifikovaný certifikát). V případě informačních systémů hrozí největší nebezpečí z podvržení programů.

Charakter a cíl hrozby je dán motivací a zkušeností pachatele. Chceme-li zjistit, kam může být hrozba směřována, musíme brát v potaz, že kybernetická hrozba má narušeny všechny vazby na konkrétní reálné prostředí a národnostní vědomí. Tyto aktivity nemají nějaké specifické zaměření. Lze je nalézt ve všech sférách – bezpečnostních, obchodních, soukromých, náboženských apod.[49]

[49] JIROVSKÝ, V. *Kybernetická kriminalita.* Praha : Grada, 1. vydání, 2007, s. 25

3.3.2 Druhý problém – legislativa.

Na začátku je důležité připomenout, že kyberprostor je možné definovat jako zdánlivě neohraničený, totálně globální, celosvětový prostor, v němž se informace nacházejí na internetu. Lze ho definovat také jako prostředí počítačových a telekomunikačních sítí, různých počítačových her a kybernetických aktivit. Není to však jen virtuální prostor, ale reálná změť věcí, práv a jiných majetkových hodnot, tvořících informační systémy (IS) v nejširším slova smyslu. Tedy zahrnuje nejen vlastní IS, ale i jeho okolí, tj. tvůrce, šiřitele a uživatele informací.[50]

Pro označení zločinného použití těchto technologií v kyberprostoru existuje mnoho termínů. Mezi nejpoužívanější patří: „*computer crime"* - komputerový zločin, „*high-tech crime"* – zločin s použitím špičkových technologií, „*IT crime"* – IT zločin, a „*cybercrime"*- kybernetický zločin. Tyto termíny jsou různě používány, zaměňovány a mezi sebou propleteny. Podle Oxford Reference Online je „cybercrime" definován jako „*trestný čin/zločin spáchaný po internetu*". Webopedia definuje cybercrime jako „*jakýkoliv kriminální čin, týkající se počítačů a sítí*". Obecně bych tedy definoval kyberkriminalitu jako činnost, při které je porušován zákon nebo je alespoň v rozporu s morálními pravidly společnosti. Praktické příklady toho, co se má a může jako cybercrime označovat, podává manuál OSN „*United Nations Manual on Prevention and Control of Computer-Related Crime*". Podle tohoto manuálu se do pojmu cybercrime zahrnuje zejména: podvod, padělání, sabotáž počítačů, neautorizovaný přístup k počítačovým programům a neautorizované kopírování počítačových programů, jako nejčastější příklady.[51]

Na kybernetickou kriminalitu se můžeme podívat z několika různých pohledů. Veškeré doposud známé nelegální aktivity probíhaly ve fyzickém prostředí, kde každý z aktérů se dal lehce identifikovat a postihnout. V kyberprostoru se však setkáváme pouze s virtuálním obrazem skutečných pachatelů, který se od skutečného může značně lišit. To je pro boj s kybernetickým trestným činem značný handicap, neboť standartní metody policejního vyšetřování selhávají. Platné právní normy nejsou schopny tyto nové zločiny jasně a taxativně vyjmenovat, a tak soudnictví tápe ve formulacích trestního zákona. Pokud provedeme srovnání s ostatními státy, zjistíme že některé nemají v této oblasti zákony žádné nebo se existující zákony výrazně liší v jednotlivých

[50] SMEJKAL, V. *Specifické rysy kybernetických kriminálních aktivit.* VŠE Praha a VUT Brno, Zdroj: http://www.znalci.cz/files/PDF/Kyberprostor_2003.pdf. 05.04.2009

[51] BUBLAN, F. *Ministerstvo vnitra ČR.* Zdroj:http://www.mvcr.cz. 02.07.2009

jurisdikcích. Činnost, která je v jedné zemi trestná, druhá země vůbec nepostihuje nebo ji považuje za legální.

Ohraničení jurisdikcí, rychlost provedení trestního činu a zahlazení stop, to všechno jsou oblasti, kde je legislativa teprve na začátku.[52]

Jediným možným řešením v současné době je aplikace právních norem postihující delikty s podobnými charakteristikami a víra v rychlost legislativního procesu. Tu však nelze v současných podmínkách žádným způsobem ovlivnit, neboť je plně v rukou politiků. Schválení každého nového zákona trvá dlouhou dobu, a proto každá chyba a nedokonalost ve schválené normě je špatná. Z toho důvodu bývají normy novelizovány a opět schvalovány. Snad největším nepřítelem kvalitních zákonů v ČR je možnost poslaneckých návrhů úprav do zákona, které jsou často prosazovány s pomocí lobbistů.

Moudré se jeví ustanovení prvorepublikového parlamentu, který mohl předložený zákon pouze jako celek schválit nebo jako celek odmítnout. Tak byla zajištěna smysluplnost zákona a jeho potřebná odborná úroveň.[53]

Můj osobní názor je, že by tomu mohly napomoci konzultace s odbornými pracovníky z praxe, z oblasti kybernality. Budou-li totiž zákonodárci schvalovat skutečně kvalitní zákony, nebude docházet k novelizacím a především se stane právní stav přehlednějším pro všechny občany, tedy i firmy.

Výsledkem tedy je, že legislativa v důsledku překotného vývoje tohoto oboru nedostatečně upravuje toto odvětví kybernetické kriminality, i když dochází k zapracování zcela nových skutkových podstat, jako je tomu v novém Trestním zákoně 40/2009 Sb., nabývající účinnost dnem 1. ledna 2010.

Ani na poli Evropského parlamentu se nedaří prosazovat směrnice a balíčky, které by dokázaly upravit chování v této oblasti. Českému předsednictví se na poslední chvíli podařilo zprostředkovat dokument ohledně telekomunikačního balíčku, který měl sjednotit trh s elektronickými komunikacemi v EU. Vyjednání tohoto balíčku patřilo k největším úspěchům našeho předsednictví na legislativní úrovni. ČR dokázala sblížit rozdílná stanoviska Evropského parlamentu a členských států, což se nedařilo od listopadu 2007, kdy evropská komise předložila návrh. Tento balíček zde zmiňuji především proto, že se týkal i práv občanů na přístup k internetu, řešil otázku regulace internetu, práva spotřebitelů, uživatelů, účastníků apod. Mimo jiné se snažil

[52] JIROVSKÝ, V. *Kybernetická kriminalita*, Praha: Grada, 1. vydání, 2007, s. 16

[53] JIROVSKÝ, V. *Kybernetická kriminalita.* Praha: Grada, 1. vydání, 2007, s. 25

o rozlišování legálního a nelegálního obsahu, filtrování či úplné blokování částí internetu při porušování autorských práv a jiné podobné věci. Podařilo se najít vyvážené řešení, které respektovalo právní systémy členských států v souladu s Úmluvou o ochraně lidských práv a základních svobod. Přesto Evropský parlament celý nový telekomunikační balíček smetl ze stolu. Kamenem úrazu se ukázala být práva uživatelů internetu. Části europoslanců se totiž nelíbily podmínky pro odpojování (domnělých) počítačových pirátů od internetu, které kritici označovali za nevyvážené vůči spotřebitelům a snadno zneužitelné.[54]

Opět tedy velké legislativní zdržení, neboť od roku 2002, kdy byl schválen první telekomunikační balíček, došlo v oblasti elektronických komunikací k velkému pokroku, ať už jde o samotné telefonování, vysílání televize přes internet nebo vznik výměnných sítí.

3.3.3 Třetí problém – policie a justice

Stalo se obecným trendem, že kybernetičtí zločinci reagují na vývoj internetu rychleji než bezpečnostní odborníci. Ukazuje se, že většina nových virů funguje pouze 24 hodin. Pokud během této doby nezaznamenají úspěch, stanou se mrtvými. Jejich tvůrci však ihned začnou pracovat na dokonalejší verzi. Je to nikdy nekončící závod, kde zajištění stop je otázkou minut a ve kterém hackeři bohužel vyhrávají. Nedostatek vysoce kvalifikovaných pracovníků, kteří by byli schopni zvládnout problematiku kybernality nejenom po stránce technologické, ale i po stránce právní, je jeden z hlavních problémů policie a justice. Shromažďování důkazů při vyšetřování kybernetických trestných činů je obtížné zejména také proto, že tyto případy neberou ohled na národní hranice ani na národní zvyklosti. A tak, i když je většina projevů kybernality trestná, není vždy snadné takovou činnost odhalit, dokázat a pachatele odsoudit. Justici nepomáhá ani fakt, že soudci jsou specialisty na právo, ne však na informační technologie. V takovýchto případech jsou nuceni využívat soudní znalce a spoléhat se na jejich posudky. Pomalost procesních postupů často vede ke ztrátě důkazů, které bezprostředně po spáchání trestného činu existovaly.

Jako příklad další výhry internetových pirátů nad zákonem může posloužit případ serveru s rekordně velkým datovým prostorem s nelegálními filmy a hudbou,

[54] EU2009.CZ, *České předsednictví jako seriál výsledků.* 01.05. 2009

provozovaný v budově Akademie věd (r. 2009). Očekával se průlom, který bude pro internetové piráty hrozbou.

Vše začalo tím, když policie – oddělení informační kriminality – odhalila v budově, kterou Ústav termomechaniky Akademie věd pronajímal soukromé počítačové firmě, tzv. TopSite server.[55] Ten obsahoval čtyři terabyty nelegálních dat. Podobných serverů je podle odhadů na světě jen zhruba stovka. Pirátské úložiště nabízelo soubory jen měsíc, ale ohromovalo svým objemem dat. Filmovému a hudebnímu průmyslu měly pachatelé způsobit škodu za 35 milionů korun.

Tento kybernetický čin byl klasifikován jako trestný čin podle § 52 TZ (nově bych ho klasifikoval podle § 270 TZ), kde skutková podstata je definována jako neoprávněný zásah do zákonem chráněných práv k autorskému dílu. Obhájcům se však podařilo prokázat, že policie dostatečně neodůvodnila, proč přistoupila k domovním prohlídkám, a neměla tak právo zabavit počítače. Taktéž napadli znalecký posudek. V odůvodnění rozsudku bylo řečeno, že obžaloba byla podána důvodně. Soud jí však vytknul, že v popisu skutku není specifikováno, o jaká konkrétní díla šlo a které subjekty vlastnily autorská práva. Bylo prokázáno, že se skutek stal, ale neprokázalo se, že jej spáchali právě obžalovaní. Ani kvalitní znalecký posudek nedokázal dát odpověď na to, kdo přesně se trestného činu dopustil. Podle soudu nebylo možné připustit žádný z důkazů, neboť nepotvrdily stoprocentně vinu tří obviněných mužů.

Obžalovaným hrozil až dvouletý trest nebo pokuta, přesto se necítili vinni. Dva z nich odmítli vypovídat, třetí tvrdil, že zbylé dva nezná. V červenci 2009 pak Obvodní soud pro Prahu 8 zprostil obžaloby trojici mladíků za provozování serveru s nelegálními filmy a hudebními nahrávkami.

Podle Markéty Prchalové z České protipirátské unie jde o první případ porušení autorských práv, který se dostal až před soud. V boji proti počítačovému pirátství se přitvrzuje po celé Evropě. Švédský soud před nedávnem odsoudil provozovatele podobného portálu k ročnímu vězení a pokutě v přepočtu 70 milionů korun.

Můžeme si však položit otázku: Měl tento a jemu podobný případ ze Švédska, opravdu odstrašující účinek? Odpovím za vás. Ne neměl, právě naopak. Tím jak jsou tyto případy značně medializovány, popularizuje to nelegální stahování z internetu a stahuje se víc než předtím.[56] Podle vyjádření odborníků je evidentní, že pohled na

[55] TopSite server - viz. přílohy - slovníček pojmů.

[56] ČT24, Nelegální stahování z internetu.
Zdroj: http://www.ct24.cz/media/internet/57785-kauzu-ceskych-internetovych-piratu-zacal-projednavat-soud. 10.07.2009

autorská práva ve filmovém průmyslu je překonaný a zůstává jen otázkou, jak průmysl najde nové zdroje pro své financování. Možná změna se už přiblížila. Jsou náznaky, že velká filmová studia uvažují o uvolnění práv, aby mohly být filmy sdíleny na internetu a předešlo se tak výrobě nelegálních kopií a dalším problémům.

Naše justice je úspěšná především při odsuzování pachatelů, kteří porušují autorský zákon. Česká organizace BSA[57] uvádí na svých webových stránkách hned několik desítek případů obvinění a odsouzení občanů a firem. Bohužel řada těchto rozsudků se týká relativně méně závažných trestných činů. Zde se škoda pohybuje v rozmezí desítek tisíc korun. Soudy jsou však ve většině případů závislé na tom, co jim předloží policie. To je také důvodem jejich malé úspěšnosti.

3.3.4 Čtvrtý problém – společnost

Základní hodnotou ovlivňující stav kybernality je vzdělanost a vybavenost společnosti v oblasti IT. Společnost můžeme hypoteticky rozdělit na dvě skupiny. Ta první používá IT velmi intenzivně, nevěnuje však pozornost zabezpečení a kybernetické ochraně. Ta druhá nepoužívá informační technologie vůbec. Je evidentní, že první skupina se stane terčem pro kybernetické útoky, zatímco druhou skupinu to neovlivní. Ve skutečnosti se však naše celá společnost nachází někde uprostřed mezi těmito hypotetickými stavy. Informovanost o bezpečnosti a možných útocích je zhruba ve všech vyspělých státech na stejné úrovni. Důvodem je existence samotného kyberprostoru a jeho charakter. Informace se v něm totiž šíří velkou rychlostí. Odlišným faktorem je v tomto případě legislativní připravenost společnosti a schopnost implementace legislativy policejními a justičními složkami. Zde však není možné dojít k celosvětově srovnatelnému stavu, neboť, jak již jsem zmiňoval, v každém státě platí jiný právní systém, morálka a je zde především odlišný historický a kulturní vývoj.

V důsledku kybernetické kriminality přicházejí firmy každoročně na tržbách o miliardy dolarů. Podle celosvětové studie vypracované na objednávku organizace BSA přesáhly celkové ztráty softwarového průmyslu na celém světě v roce 2007 jako přímý důsledek softwarové kriminality 40 miliard dolarů. Společnost si neuvědomuje, že negativní důsledky kybernetické kriminality dalece přesahují samotného vydavatele

[57] Business Software Alliance (BSA) – volné sdružení významných světových výrobců softwaru, působí ve více než 60-ti zemích světa. V ČR působí od roku 1998. cílem BSA je vzdělávání uživatelů softwaru v oblasti ochrany autorských práv a upozorňování na různá hospodářská, právní a společenská rizika spojená s nelegálním užíváním počítačových programů.
Zdroj: http://www.bsa.org. 01.06.2009

softwaru. Ekonomické ztráty pociťují nejen výrobci softwaru nebo distribuční společnosti, ale především zákazníci, tedy samotní uživatelé.

Internetové pirátství si získalo ve společnosti velkou podporu především mezi mladými lidmi, kteří nesouhlasí s přísnými tresty. V červnu 2009 dokonce ohlásila kandidaturu do sněmovny Česká pirátská strana (ČPS), která chce navázat na úspěch podobné partaje ve Švédsku.[58] ČPS chce změnit autorská práva a více liberalizovat pohyb na internetu. Založení strany bylo podle jejího přípravného výboru reakcí na dubnový rozsudek švédského soudu v kauze vyhledávacího portálu The Pirate Bay,[59] který odsoudil jeho majitele na rok do vězení.

Laxní postoj a přístup veřejnosti k těmto pirátským počinům má tedy své kořeny i v neúspěšnosti vyšetřování a trestání orgány státní moci. Pokud bychom provedli srovnání běžné ozbrojené bankovní loupeže s kybernetickým zločinem podobného charakteru, dostaneme se ke zjištěním, že kybernetický útok vede, pokud se podaří. Zároveň pachatel neriskuje fyzické zranění.

3.3.5 Pátý problém – bezpečnost

Prakticky každému je dnes jasné, že neexistuje ani veřejnoprávní, ani soukromoprávní oblast lidské činnosti, kde bychom v určitém okamžiku nenašli nějaký počítač, resp. informační systém, který by neměl možnost připojit se k internetu. Většina uživatelů internetu už o bezpečnosti nějaké povědomí má. Ví, že je dobré používat antivirový program a firewall.[60] Stále je ale rozšířeno mylné přesvědčení, že stačí, když se člověk vyhne nelegálnímu softwaru a nebude navštěvovat pochybné webové stránky.

Většina běžných uživatelů totiž důvěřuje počítačům víc, než by měla, a zcela opomíjí otázku bezpečnosti. Hledisko bezpečnosti počítačových komunikací zaostává za prudkým rozvojem technologií a softwaru, což je částečně způsobeno také požadavkem na co největší jednoduchost a použitelnost běžných aplikací i operačního sytému. Nicméně univerzálnost počítače jako nástroje, který zpracovává texty, přehrává video a zvuk, komunikuje v reálném čase s jiným uživatelem na jiném kontinentu s sebou nese spoustu možností, jak tuto třídu technologií zneužívat. S připojením

[58] Pirátská strana ve Švédsku – založena v r. 2006, usiluje o reformu autorského zákona. Ve volbách do Evropského parlamentu získali přes 7% hlasů a 1 zástupce v EP, Zdroj:http://www.blisty.cz/2009/5/29/art47090.html. 29.05.2009

[59] The Pirate Bay – česky pirátská zátoka, server, který indexuje a vyhledává rozdělené soubory v celém kyberprostoru. Zdroj:http://thepiratebay.org. 01.06.2009

[60] Firewall – viz. přílohy - slovníček pojmů.

počítače k internetu hrozí daleko větší ztráta soukromí, než si lidé dokáží připustit. Rozmáhá se špehování uživatelů a jejich aktivit, tzv. „snooping“, což považuji za obrovský zásah do soukromí. Nejen že se tím otevírá kanál, kterým se do počítače mohou dostat programy z kategorie malware, spyware[61] a další, ale lze odposlouchávat jakoukoli komunikaci vzdáleně a je možné získat i vzdálený přístup k počítači, pokud není dostatečně chráněn. Další specifické nebezpečí vyplývá z obtížnosti prokázání identity druhé strany (jen těžko ověříte, s kým vlastně komunikujete). Připojení počítače k internetu začíná získáním celosvětově jednoznačného identifikátoru, takzvané IP adresy. To obvykle zajistí firma označovaná jako poskytovatel internetových služeb (ISP – Internet Service Providers). Kromě holého připojení k internetu pak ISP často poskytuje i další služby, jako například emailovou schránku pro příjem a dočasné uložení emailů, POP server, Proxy server, WEB server.[62] Veškerá komunikace mezi počítačem a kterýmkoliv jiným zařízením připojeným k internetu pak prochází přes síť tohoto poskytovatele, a to ve většině případů nezašifrovaná, tedy v „čitelné“ podobě. ISP má také přehled o tom, kdy a jak jste využívali poskytovaných služeb. Právě zde je to místo, kde připojení k internetu přestává být tak anonymní, jak se všeobecně mylně věří. Běžný uživatel zjistí jen rámcově, kdo se skrývá za tou či onou IP adresou, ovšem poskytovatel internetu shromažďuje data o následujících událostech: komu a kdy se odesílají emaily, počet; kdy, odkud a kdo se připojuje; jaké navštívil stránky; a v případě nákupu na internetu i číslo kreditní karty .

Naprosto stejná situace je i v internetových kavárnách, které bývají navíc vybaveny CCTV kamerami.[63] Tady jsou lidé ještě méně obezřetní, v domnění naprosté anonymity.

Základem ochrany je povědomí o tom, jaké informace má poskytovatel k dispozici a jak je získává. V současné době platí, že poskytovatelé v ČR mají povinnost umožnit vyšetřovatelům přístup ke všem dostupným údajům podobně jako mobilní operátoři.

Doba, po kterou ISP záznamy uchovává, je závislá na technických možnostech poskytovatele, objevují se však tlaky nařídit zákonem povinnou dobu archivace, a to na 6 měsíců až 3 roky. Jako důvod bývá uváděn boj s terorismem. ISP argumentují tím, že sbíraná data jsou pro ně anonymní, a ani se nesnaží je nějak vztáhnout ke konkrétním fyzickým osobám. Z toho plyne, že je jen otázkou času, kdy se tak stane a sbíraná data

[61] Malware,Spyware - viz. přílohy - slovníček pojmů.

[62] POP, Proxy, Web server - viz. přílohy - slovníček pojmů.

[63] CCTV kamery - viz. přílohy - slovníček pojmů.

budou „odanonymizována“. Pokušení je příliš velké a za vším hledejme lidský faktor. Uživatelé zkrátka na bezpečnost moc nedají. Odmítají věřit, že vlády i soukromé společnosti budou sledovat místa, která lidé v online světě navštěvují, i to, co tam dělají, že budou takováto data shromažďovat a následně využívat k vytváření co nejucelenějšího obrázku o jejich aktivitách, zájmech a preferencích. Tzv. „sběrači dat“ budou čelit stále většímu pokušení využít takto získaná data i takovými způsoby, k jakým se dnes ještě neodvažují.

3.3.6 Šestý problém – podzemní ekonomika

Počítačová podzemní ekonomika sází na dvě věci. Díry v programech jsou jenom jedna část problému - kupodivu ta méně nebezpečná. Mnohem horší jsou sami uživatelé. Nejčastějším prostředím, kde se obchoduje s kradenými údaji, jsou diskusní fóra a aukce. Ceny jsou pevně stanovené a citlivá data důvěřivých klientů se dají pořídit už od několika centů. Nejžádanějším a nejvýdělečnějším artiklem jsou podle studie bezpečnostní firmy Symantec[64] jednoznačně čísla kreditních karet. Kdyby se totiž internetovým zločincům podařilo odcizit čísla ke všem účtům, ke kterým mají přístup, mohli by se obohatit až o částku 1,7 miliardy dolarů.

Podle studie Underground Economy je podzemní ekonomika momentálně ve stádiu efektivního globálního trhu, na němž je pravidelný zájem o nákup a prodej kradeného zboží i služeb. Funguje úplně stejně jako běžná ekonomika, jsou tam specializované profese, burzy s napadenými počítači nebo s kradenými daty.[65]

Dosud největší případ krádeže identity na internetu odhalilo americké ministerstvo spravedlnosti (srpen 2009). Údaje ze 130 milionů karet byly ukradeny z počítačových systémů společností Heartland Payment Systems Inc., 7-Eleven Inc., Delhaize Group’s Hannaford Brothers Co. a dalších dvou menších firem. Ze spáchání loupeže považované za největší svého druhu v dějinách USA byl podle ministerstva obviněn osmadvacetiletý Albert Gonzales z Miami a dva počítačoví hackeři, kteří pocházejí z Ruska. Čelí obvinění ze spiknutí a zpronevěry. Gonzales začal krást se dvěma spojenci již v prosinci 2007. Gang používal pro svoji práci servery v Kalifornii, Illinois, Lotyšsku, Nizozemí a Ukrajině. Hlavnímu podezřelému hrozí 20 let vězení za

[64] SYMANTEC – společnost, zabývající se ochranou proti softwarové kriminalitě

[65] BERÁNEK, J. *Konec naivity.* Praha : Economia, 2009, s.14-15

nabourávání sítí, pět let za spolčování a pokuta do výše půl milionu dolarů (téměř deset milionů korun).[66]

Zde je jasně vidět, že internet je světem bez hranic a aktivity kyberzločinců po celém světě nebude tak snadné zastavit. Útoky mohou být zaměřeny na uživatele v jakékoliv zemi nebo celém světě. Česko však zatím pro vykrádání čísel kreditních karet není zemí zaslíbenou.

„Je lepší útočit na velké množství uživatelů než atakovat malou zemi v srdci Evropy, kde největší banka má něco přes dva miliony klientů.“[67]

3.4 NELEGÁLNÍ AKTIVITY

S nástupem nových technologií se začaly objevovat i nové druhy trestné činnosti. Mezi ně patří i typy útoků páchané v prostředí internetu, internetové obtěžování a podvody. Protiprávní jednání může být vedeno s počítačem nebo proti počítači. Většinu takovýchto deliktů lze zařadit do působnosti trestního zákona, existují však i takové typy jednání, jejichž klasifikace je obtížnější. V případech, kdy uvedená protiprávní jednání mohou přerůst v trestný čin, se budu snažit uvést skutkové podstaty podle TZ 40/2009 Sb.[68], nabývajícího účinnosti od 1.1.2010, a dle kterého je možno tyto činy kvalifikovat v našem právním řádu. V závorce uvedu kvalifikaci podle původního TZ 140/1961 Sb.[69], ve znění pozdějších předpisů 412/2002 Sb.[70]

Hacking

Hacking je anglické slovo, které v překladu znamená buď nabourávání, průnik např. do počítače, nebo programování z radosti či přesvědčení. Je považován odborníky za druhou nejvýraznější oblast počítačové kriminality ihned po porušování autorských práv. Jedná se o organizované útoky, které se odehrávají v celých sériích. Ochromeny jsou nejenom informační webové stránky a vládní servery, ale útoky zasahují i banky, zpravodajské servery, mobilní sítě a televizní stanice. Některé státy jsou v tomto směru snadno napadnutelné a zranitelné, protože jsou příliš závislé na internetu a přes síť

[66] VANČUROVÁ, K. Zdroj: http://www.mediafax.cz, 18.08 2009

[67] KORENKO, M. *Vyjádření marketingového manažera společnosti GRISOFT*. Zdroj: http://ekonomika.ihned.cz. 18.08.2009

[68] Zákon č. 40/2009 Sb., Trestní zákoník, Tiskárna Ministerstva vnitra, částka 11, ročník 2009

[69] Zákon č. 140/1961 Sb., Trestní zákon, Ministerstvo spravedlnosti částka 65, ročník 1961

[70] 412. Úplné znění zákona č. 140/1961 Sb. trestní zákon, jak vyplývá z pozdějších změn, Tiskárna Ministerstva vnitra, částka 146, ročník 2002,

realizují i volby. Kybernetické útoky se navíc zneužívají k vyřizování si účtů mezi některými vládami. Hacking prošel různými fázemi vývoje.

První etapa, to byly zásahy a průniky do informačních systémů jako takových, byly vedeny zcela legitimně, se snahou odstranit chyby a upravit systém do co nejefektivnější podoby.

Druhá etapa byla ve znamení průniku hackerů do chráněných systémů, přičemž jejich cílem bylo prokázat vlastní schopnosti a kvality, aniž by získali nějaké informace nebo narušili systém. Jejich hlavním cílem bylo překonávat ochranné bariéry, bez toho že by očekávali veřejné uznání. Stačilo jim, když se o jejich činu hovořilo. Hackerství bylo jejich koníčkem.[71]

Třetí etapa už ale představuje nový typ hackerů, jejichž pohnutky jsou ryze materiální. Hacking tedy můžeme definovat jako proniknutí do počítačového – řídícího systému nestandardní cestou, tzn. prolomením bezpečnostní ochrany.

Po stránce právní bychom mohli na tento čin použít *§ 230 TZ 40/2009 Sb. – Neoprávněný přístup k počítačovému systému a nosiči informací*. (§ 257a TZ 140/1961 Sb. - poškozování a zneužití záznamu na nosiči informací). V §230 TZ 40/2009 Sb.[72] se hovoří o překonání bezpečnostního opatření a získání přístupu k počítačovému systému nebo jeho části. Pokud tedy nedojde ke škodě, nikomu nebude způsobena újma, nebo hacker či jiná třetí osoba nebude mít z průniku prospěch, pak skutková podstata nebude naplněna. Trestní sazba činí v tomto případě až jeden rok, zákaz činnosti nebo propadnutí věci – jiné majetkové hodnoty. Při splnění ostatních podmínek může být sazba zvýšena až na osm let.

Warez

Správná definice zní, že warez je termín počítačového slangu označující autorská díla, se kterými je nakládáno v rozporu s autorským právem.[73] Slovo vzniklo z anglického slova „wares“ - zboží a pravděpodobně i „software“. Slovo warez ale může také označovat i internetovou subkulturu, která se warezem zabývá. Člověk zabývající se warezem je lidově řečený warezák, spisovně zvaný pirát.

---

[71] LÁTAL, I. *Počítačová (informační) kriminalita a úloha policisty při jejím řešení.*, Zdroj: http://web.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html. 07.02.2009

[72] Zákon č. 40/2009 Sb., Trestní zákoník, Tiskárna Ministerstva vnitra, částka 11, ročník 2009
Zákon č. 140/1961 Sb., Trestní zákon, Ministerstvo spravedlnosti částka 65, ročník 1961

[73] 398. Úplné znění zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), jak vyplývá z pozdějších změn, Tiskárna Ministerstva vnitra částka 126, ročník 2006

V praxi se jedná o uveřejňování nelegálního softwaru, audio - video souborů, her, prostě autorsky chráněných děl na internetu. Tyto nelegální kopie se obvykle objeví ve stejný den jako oficiální vydání jednotlivých děl. Není to záležitostí jednotlivce, ale skupiny mající a dodržující určitou organizaci. Jejich činnost lze rozdělit do několika fází:

1. fáze - ihned poté, co je oznámeno, že bude vydána očekávaná verze komerčního produktu, vyvíjí warezová skupina aktivitu na jeho získání
2. fáze - produkt je předán zkušenému crackerovi, který odstraní ochranu proti zneužití
3. fáze - rozšíření takto upraveného produktu mezi ostatní zájemce pomocí výměnných sítí a upload serverů[74]

Warezové skupiny ze svého počínání žádný finanční zisk nemají. Motivace těchto skupin může být různá, obvykle je založena na „pověsti" – jednotlivé skupiny mezi sebou soupeří o co nejrychlejší kvalitní vydání. To je v komunitě vnímáno jako úspěch. Mnoho uživatelů, kteří produkty získávají z *warez* zdrojů, je přesvědčeno, že nikomu neškodí. Argumentem např. je, že kdyby produkty nezískali jako warez, jistě by si je ani nekoupili. Tedy tvůrce programu o nic nepřišel.[75]

U nás je kopírování a šíření autorských děl bez povolení autora trestný čin. Ovšem v případech, kdy právnické nebo fyzické osobě, která je vlastníkem systému, vůči němuž je útok crackingem prováděn, nevznikla prokazatelná škoda, může být od stíhání „upuštěno". V ostatních případech se jedná o *§ 270 TZ 40/2009 Sb. - Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi.* (§ 152 TZ 140/1961 Sb.),[76] který se trestá buď:

- odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty
- odnětím svobody na šest měsíců až pět let (tři léta až osm let), pokud tak pachatel konal ve značném rozsahu,

nebo § 230 TZ 40/2009 Sb. – neoprávněný přístup k počítačovému systému a nosiči informací (§ 257a TZ 140/1961 Sb.).

[74] Upload server – viz. přílohy - slovníček pojmů.

[75] JIROVSKÝ, V. *Kybernetická kriminalita.* Praha: Grada, 1. vydání, 2007, s.105

[76] Zákon č. 40/2009 Sb., Trestní zákoník, Tiskárna Ministerstva vnitra, částka 11, ročník 2009
Zákon č. 140/1961 Sb., Trestní zákon, Ministerstvo spravedlnosti částka 65, ročník 1961

Cracking

Tato forma činnosti je velice úzce spjata s oběma předchozími. Cracking znamená prolamování – obcházení ochranných prvků s cílem jejich neoprávněného použití. Osoba odstraňující tyto ochrany se nazývá cracker. Nejčastěji se jedná o tzv. „password cracking“ – zjišťování hesla pro přístup do systému.

Trestní kvalifikace tohoto typu činnosti je rozdílná. Pokud právnické nebo fyzické osobě, která je vlastníkem systému, vůči němuž byl útok veden, nevznikla prokazatelná škoda, může být od trestního stíhání upuštěno. V opačném případě se jedná o postih dle TZ 40/2009 Sb, stejně jako v případě warez.

Kybernetické výpalné

Další formou zneužití IT je tzv. kybernetické výpalné a s tím související vydírání, kdy si pachatel vyhlédne svoji oběť – provozovatele webových stránek a pod pohrůžkou zneužití, znepřístupnění, zničení začne tohoto provozovatele vydírat. Jedná se o typ trestné činnosti, která je založena na strachu z prezentované hrozby průniku do spravovaného nebo vlastněného systému.

Z právního hlediska lze na tento typ trestné činnosti použít *§ 175 TZ 40/2009 Sb. - Vydírání* (§ 235 TZ 140/1961 Sb.),[77] kde je sazba od šesti měsíců do čtyř let nebo peněžitý trest. Při zvlášť závažných případech však až šestnáct let odnětí svobody, s možností rozšíření *o § 230 TZ 40/2009 Sb. - Neoprávněný přístup k počítačovému systému a nosiči informací* (§ 257 TZ 140/1961 Sb.).

Spamming

S tzv. spammingem se jistě setkal každý, kdo běžně využívá elektronickou poštu na internetu. Konkrétněji se jedná o rozesílání nevyžádaných zpráv elektronickou poštou s reklamním či propagačním obsahem, kdy je stále nabízeno něco, co nikdo nechce. Díky spammingu může docházet jednak k zahlcení mail-serverů nebo k narušení řádného fungování interaktivních sítí.[78] Spam totiž napomáhá i šíření klasických virů, trojských koňů a ostatních záludných kódů. Tyto škodlivé kódy se pak snaží o kontrolu nad infikovanými počítači pomocí tzv. bot programů. Pokud tuto situaci zjednoduším, tak centrální ovládání těchto bot programů vytváří tzv. botnet sítě.

[77] Zákon č. 40/2009 Sb., Trestní zákoník, Tiskárna Ministerstva vnitra, částka 11, ročník 2009
Zákon č. 140/1961 Sb., Trestní zákon, Ministerstvo spravedlnosti částka 65, ročník 1961

[78] OTEVŘEL, P. *Spamming a některé otázky šíření obchodních sdělení*. Zdroj:http://www.pravoit.cz, 12.07.2009

Tyto botnet sítě jsou schopny ovládat asi milion počítačů po celém světě a ty jsou schopny denně odeslat až 100 miliard nevyžádaných emailů.[79] A jak se získávají emailové adresy? Velice jednoduše. Např. marketingové firmy je získávají z konferencí na internetu, z registrací, které poskytnou uživatelé pro nejrůznější služby zdarma, nebo za pomocí automatizovaných programů, které umí vyfiltrovat emailové adresy z diskusních příspěvků. Většina organizací či akademická nebo internetová komunita se snaží bránit spammerům blokováním jejich adres, avšak ne vždy se setkávají s úspěchem.[80] Jedinou prevencí je nezveřejňovat svou adresu na kdejakém fóru a neregistrovat se do podezřelých služeb. A když už spam obdržíme, tak na něj v žádném případě neodpovídat. Pokud spam nabízí možnost odhlášení, tuto možnost raději nevyužít. Většinou totiž odesilatele spamu ujistíme, že je naše schránka aktivní.

Právní pohledy na možnost postihnutí spamu jsou následující:

V EU byla vydána Evropská směrnice č. 2000/31/ES o elektronickém obchodu, která vymezuje základní pravidla týkající se zasílání nevyžádaných obchodních sdělení a následně také Evropská směrnice č. 2002/58/ES o soukromí a elektronických komunikacích, která se zabývá ochranou osobních údajů fyzických i právnických osob v souvislosti s elektronickými komunikacemi. S těmito uvedenými směrnicemi je v souladu náš zákon č. 480/2004 Sb.[81] o některých službách informační společnosti, který za uvedené protiprávní jednání může stanovit sankce (má v náplni své práce Úřad pro ochranu osobních údajů - ÚOOÚ).[82] V tomto zákoně je v §7 a následujících spam redukován na nevyžádaná obchodní sdělení a §11 ukládá správní sankce při nevyžádaném šíření takové informace až do výše deseti milionů korun.

Poslední možností je použití zákona č. *40/1995 Sb. o regulaci reklamy*,[83] konkrétně ustanovení §2 odst. 1. písm. e). Nevyžádaná pošta musí mít v tomto případě reklamní charakter a vést k nákladům na straně adresáta (např. alikvotní část ceny za připojení) nebo jej obtěžovat. Porušení tohoto ustanovení je trestáno peněžitou pokutou až do výše dvou milionů korun.[84]

---

[79] NYKODÝMOVÁ, H. *Botnety: Nová internetová hrozba.* Zdroj: http://www.lupa.cz, květen. 15.03.2009

[80] MATĚJKA, M. *Počítačová kriminalita*. Praha: Computer Press , 1. vydání, 2002, s. 70

[81] Zákon č. 480/2004 Sb., Zákon o některých službách informační společnosti a o změně některých zákonů, Tiskárna Ministerstva vnitra, částka 166, ročník 2004

[82] OTEVŘEL, P. *Spamming a některé otázky šíření obchodních sdělení*. Zdroj: http://www.pravoit.cz, 12.07.2009

[83] Zákon č. 40/1995 Sb., Zákon o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů, Tiskárna Ministerstva vnitra částka 8, ročník 1995

[84] JIROVSKÝ, V. *Kybernetická kriminalita*. Praha: Grada, 1. vydání, 2007, s.105

V této souvislosti je trestný i sběr emailových adres pro účely rozesílání spamu. Zde je naplněna skutková podstata *§ 180 TZ 40/2009 Sb. – Neoprávněné nakládání s osobními údaji* (§ 178 TZ 140/1961 Sb.)[85], a to v případě pokud je poskytne spammerovi třetí osoba bez souhlasu subjektu údajů.

Sniffing

Podobně jako ostatní výše jmenované protiprávní jednání, je i sniffing využíván pro páchání počítačové a informační kriminality. Sniffing – čmuchání, se používá zejména při diagnostice sítě, zjištění používaných služeb, protokolů a odposlechu datové komunikace. Tuto metodu často využívají rozhněvaní zaměstnanci nebo šikovní hackeři, kteří tak neoprávněně monitorují či odposlouchávají elektronickou komunikaci. Jejich hlavním cílem bývá zachycování hesel pro chystaný průnik do jiných systémů. Existuje hned několik způsobů odposlechu, ale ke každému je zapotřebí takové softwarového vybavení, které to umožní.

Úskalí nastává, pokud zaměstnavatel odposlouchává i soukromou komunikaci svých zaměstnanců. Pokud by zaměstnanec v tomto případě nahlásil zaměstnavatele úřadu pro ochranu osobních údajů nebo policii, vystavuje se zaměstnavatel pokutě, případně může být i potrestán odnětím svobody až na jeden rok. Neoprávněné odposlouchávání dat je trestná činnost dle *§ 182 TZ 40/2009 Sb. - Porušení tajemství dopravovaných zpráv* (§ 239 TZ 140/1961 Sb.), případně podle *§ 183 TZ 40/2009 Sb. - Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí* (§ 240 TZ 140/1961 Sb.).

Cybersquatting

Pod tímto názvem se skrývá blokování internetových domén, spekulace s doménami za účelem zisku. Cybersquatting jakožto spekulativní registrace doménového jména tak brání jiné osobě v plnohodnotném způsobu její internetové prezentace. V praxi má několik podob:

- registrace domény shodné či podobné s obchodní firmou či ochrannou známkou jiné osoby;
- jde o hromadnou registraci shodných či zaměnitelných domén s tzv. blokačním úmyslem;

[85] Zákon č. 40/2009 Sb., Trestní zákoník, Tiskárna Ministerstva vnitra, částka 11, ročník 2009
Zákon č. 140/1961 Sb., Trestní zákon, Ministerstvo spravedlnosti částka 65, ročník 1961

- jedná se o registraci zaměnitelné domény s tím, že spekulant spoléhá na překlepy uživatelů internetu, jako příklad lze uvést www.gogle.cz nebo www.seynam.cz;
- jde o cílenou spekulativní registraci doménových jmen shodných a zaměnitelných s názvem ochranné známky;
- jde o předvídání určité skutečnosti, kdy spekulant spoléhá na to, že dojde k určité skutečnosti a pak bude z této situace těžit; příkladem může být registrace domény www.benedictXVI.com, kdy si dotyčný před volbou nového papeže v roce 2005 zaregistroval šest domén s pravděpodobnými jmény nového papeže, vycházeje z posledních jmen papežů za několik století.

Spekulanti se prostě spoléhají na to, že dotčená osoba nebude chtít podstupovat náročné soudní či arbitrážní řízení a že raději si doménu od spekulanta koupí.[86]

Právní kvalifikace v tomto případě spadá do více oblastí, neboť spekulanti se svým jednáním dopouštějí několika porušení právních povinností. Jejich jednání tak často představuje:

a) porušení práv k obchodní firmě (§ 12 obchodního zákoníku);[87]
b) porušení práv k ochranné známce (§ 8 zákona o ochranných známkách);
c) vyvolání nebezpečí záměny (§ 47 obchodního zákoníku);
d) parazitování na pověsti (§ 48 obchodního zákoníku).

V určitých závažnějších případech může dojít k naplnění dvou podstat trestných činů:

§ 182 TZ 40/2009 Sb. - *Porušení tajemství dopravovaných zpráv* [88] (§ 149 TZ 140/1961 Sb. – nekalá soutěž),[89]

§ 268 TZ 40/2009 Sb. - *Porušení práv k ochranné známce a jiným označením* (§ 150 TZ 140/1961 Sb. – Porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu)

V obou případech hrozí trest odnětí svobody až na dva roky nebo zákaz činnosti.

[86] JANSA, L. *Cybersquatting a jeho podoby*. Zdroj:http://www.pravoit.cz/article/cybersquatting-a-jeho-podoby. 15.03.2009

[87] Zákon 513/1991 Sb. ‚Obchodní zákoník, Federální ministerstvo vnitra, částka 98, ročník 1991

[88] Zákon č. 40/2009 Sb., Trestní zákoník, Tiskárna Ministerstva vnitra, částka 11, ročník 2009

[89] Zákon č. 140/1961 Sb., Trestní zákon, Ministerstvo spravedlnosti částka 65, ročník 1961

3.4.1 Zneužití internetových stránek

S rozšiřováním IT dostal nový rozměr i jeden z nejstarších trestných činů – pomluva. Dříve lidé řešili neúspěch pomocí hanlivých nápisů na nejrůznějších místech. Dnes je situace jednodušší. Pomluvu lidé zveřejní na internetu v domnění, že nepáchají nic hrozného. Opak je ale pravdou. Takové počínání se hodnotí podle *§ 184 TZ 40/2009 Sb. – Pomluva* (§ 206 TZ 140/1961 Sb.), kde je uvedeno, že kdo jinému sdělí nepravdivý údaj, který ohrozí vážnost u spoluobčanů, poškodí jej v zaměstnání, naruší jeho rodinné vztahy nebo způsobí mu jinou vážnou újmu, bude potrestán odnětím svobody až na jeden rok. Odnětím svobody až na dva roky nebo zákazem činnosti bude potrestán ten pachatel, spáchá-li čin mimo jiné pomocí veřejně přístupné počítačové sítě nebo jiným obdobně účinným způsobem.

3.4.2 Šíření materiálů se závadným obsahem

Povaha internetu jako prostředku, jehož prostřednictvím lze veřejně šířit informace, je významná v oblasti trestněprávní, konkrétně tam, kde se jedná o trestné činy, u nichž je veřejnost jejich znakem. Například:
§ 364 TZ 40/2009 Sb. – Podněcování k trestnému činu (§ 164 TZ 140/1961 Sb.), *§ 365 TZ 40/2009 Sb. – Schvalování trestného činu* (§ 165 odst. 1 TZ 140/1961 Sb.) a *§ 358 TZ 40/2009 Sb. - Výtržnictví* (§ 202 TZ 140/1961 Sb.).[90]

Přitom je trestný čin spáchán veřejně, je-li spáchán obsahem tiskoviny nebo rozšiřovaného spisu, filmem, rozhlasem, televizí, případně jiným obdobně účinným způsobem. Internet lze nepochybně považovat právě za „jiný obdobně účinný způsob“.[91]

Tyto trestné činy v sobě zahrnují šíření pornografie, materiálů podporujících extremismus nebo materiálů podobného obsahu. Nejedná se o nový druh trestné činnosti, ale o nový způsob šíření. Činy spadají spíše do trestní odpovědnosti poskytovatele obsahu, než do trestní odpovědnosti správce počítačového systému.[92]

Lze je kvalifikovat podle *§ 190 TZ 40/2009 Sb. - Prostituce ohrožující mravní vývoj dětí* (§ 205 TZ 140/1961 Sb. vztahující se k ohrožování mravnosti) nebo podle *§ 355 TZ 40/2009 Sb. - Hanobení národa, rasy, etnické nebo jiné skupiny osob*

[90] Obdobně to platí samozřejmě také, např. pokud jde o přestupek proti veřejnému pořádku podle § 47 odst. 1 písm. c) 200/1990 zákona o přestupcích, jehož se dopouští ten, kdo vzbudí veřejné pohoršení.

[91] SMEJKAL,V. *Je Internet kriminogenní?* Zdroj:http://www.rodiny.cz/07/?IdPage=6, 16.03.2009

[92] JIROVSKÝ,V. *Kybernetická kriminalita*. Praha: 1. vydání, 2007, s.103

(§ 198 TZ 140/1961 Sb. – Hanobení národa, etnické skupiny, rasy a přesvědčení) nebo *§ 403 TZ 40/2009 Sb. - Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka* (§ 260 TZ 140/1961 Sb.). Většina citovaných ustanovení klasifikuje tyto trestné činy odnětím svobody až na tři roky. Ať už půjde o jakýkoliv trestný čin, jednou z podmínek jeho spáchání je existence nějakého serveru, paměťového prostoru se závadným obsahem apod.

3.5 DĚTI A INTERNET

V další části své práce se budu věnovat kybernetické kriminalitě v souvislosti s mladší populací, jakému nebezpečí se sami dobrovolně vystavují a jaké jim hrozí následky nebo postihy. Naše děti vyrůstají a budou vyrůstat v prostředí prodchnutém duchem internetu, s tím už se musíme smířit. Zároveň však někteří z nás rodičů mohou mít pocit, že nejsou s počítačem zdaleka tak sžití jako jejich potomci. Rodičům ovšem přísluší povinnost chránit své dítě před nebezpečím, ať se nachází kdekoliv. Erotické weby, pornografie, stránky plné násilí, nevhodná videa apod. dle mého názoru skutečně ubližují dětem. I zkušený uživatel internetu se občas diví, jak se takové hrozné věci před ním v okně prohlížeče objevily. A co teprve když to uvidí nezletilé dítě. Pokud si vzpomenu na svá klukovská léta, tak jsem svůj volný čas trávil opravdu jiným způsobem a mrzelo mě, když jsem např. nemohl jít ven. Dnešním dětem spíše ublíží zákaz hraní s počítačem.

Od roku 1973 probíhají ve vybraných evropských zemích pravidelná dotazovací šetření – Eurobarometr[93] a díky jednomu takovému průzkumu proběhla skupinová setkání s chlapci a děvčaty ve věku 9-10 a 12-14 let. Projekt běžel ve 27 zemích EU, přičemž výsledky byly všude v podstatě stejné. Prakticky všechny děti mají dnes přístup k internetu a část jejich života se tak odehrává ve virtuálním prostředí. Považují to za přirozené a běžné. Znalosti používání počítače a internetu získávají hlavně napodobováním rodičů, sourozenců, kamarádů apod. metodou „pokus-omyl“. Obvykle si myslí, že jsou v „serfování“ zkušenější než jejich rodiče, a věří svým schopnostem vypořádat se s většinou problémů sami. Právě toto sebevědomí může být nebezpečné a může dítě dostat do rizikové situace.

[93] EUROBAROMETR – mezinárodní šetření organizovaná 2 x za rok ve všech členských zemích EU. Předmětem šetření je pravidelný monitoring sociálních a politických postojů obyvatel. Zdroj:http://ec.europa.eu/index_cs.htm. 01.05.2009

3.5.1 Děti a nevhodný obsah

Pornografie

Internetová pornografie je snadno přístupná, cenově dostupná, anonymní a může vypadat utajeně a bezpečně. Žádná internetová aplikace však není imunní vůči těmto projevům. Dítě nebo dospělý může ve svém domově, škole, kanceláři snadno a zcela tajně získat velké množství jakéhokoliv druhu pornografie včetně extrémního a násilného hard core materialu. V minulosti museli dospělí tento materiál cíleně vyhledávat a nebylo pravděpodobné, že na něj narazí děti. Nyní se tomu tak stane i nechtěně během hledání zcela nevinného obsahu. V anglickém jazyce bylo dokonce pro tento fenomén vynalezeno nové slovo – cybersex. Cybersex lze definovat jako jakoukoli formu sexuálního vyjádření, která je přístupná pomocí počítače nebo internetu. Velkým problémem je i šíření dětské pornografie, která se nevyhýbá ani českým webům. Doposud měla policie problém, jak ji pedofilům prokázat. Samotné držení těchto materiálů totiž do roku 2009 nebylo u nás trestné. To změnil až nový trestní zákoník, podle kterého bude postižen i ten, kdo bude mít nebo přechovávat fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě na svém počítači *§ 191 TZ 40/2009 Sb. – Šíření pornografie; § 192 TZ 40/2009 Sb. – Výroba a jiné nakládání s dětskou pornografií; § 193 TZ 40/2009 Sb. – Zneužití dítěte k výrobě pornografie.*[94]

Extremismus a agresivita

Na českém internetu najdeme mnoho různých názorově vyhrocených webů – kromě „tradiční“ ultrapravice (fašismus, nacismus, neonacismus) a ultralevice (anarchismus, bolševismus) se můžeme setkat i s extrémními náboženskými ideologiemi (vesmírní lidé) anebo třeba s hnutími propagujícími anorexii či bulimii. Extrémisté rozšiřují svá stanoviska nejrůznějšími cestami – mimo klasických webových stránek též píší osobní blogy, zakládají diskuse apod. Cílem prezentace těchto hnutí na internetu není jen pouhá propagace názorů a vzájemná podpora, ale též nabírání nových členů, sběr příspěvků a v neposlední řadě i organizace skupinových akcí a setkání. Dalo by se říci, že s tím, jak světová síť zmenšuje komunikační propast mezi lidmi a dovoluje

[94] Zákon č. 40/2009 Sb., Trestní zákoník, Tiskárna Ministerstva vnitra, částka 11, ročník 2009

anonymní vyjádření jednotlivců, tak se vzájemně lépe najdou i vyznavači menšinových přesvědčení. Tím se nepříliš korektní myšlenky snadněji dostávají k nejmladší generaci.

Extrémisté začali poslední dobou zvláště v USA používat zákeřné taktiky, kdy své postoje obalují do relativně nevinného, vcelku přitažlivého kabátu a publikují je na doménách s neškodnými názvy. Také používají různé viry a snaží se rozesílat spamy se svými myšlenkami. Násilného obsahu najdeme na internetu opravdu hodně a ani se nijak nemusí týkat extrémistických webů, i když s nimi bývá často spojován. Přesto psychologové tvrdí, že agresivita je do velké míry vrozenou záležitostí a vystavení násilí v médiích včetně internetu neovlivňuje dítě zdaleka tolik jako vystavení násilí v rodině. I tak ale jiní odborníci nahlížejí na celý problém odlišně – vystavením agresivnímu obsahu získává dítě pocit, že je násilí normální, a nedokáže tolik soucítit s jeho oběťmi. Nejnebezpečnější jsou údajně věci, které může dítě snadno napodobit a které se mohou v jeho okolí odehrát.[95]

3.5.2 Cyberstalking - kyberšikana

I na internetu existují obdoby nepříjemného a agresivního chování, které známe z běžného života. Díky relativní anonymitě kyberprostoru se zde s nimi setkáváme mnohem častěji, neboť zde chybí sociální odezva a násilníci se tak méně bojí trestů a negativních ohlasů. Napadání druhých probíhá nejčastěji na různých druzích komunitních webů, na diskusních fórech a na chatech. Agresoři jsou ovšem často velmi vynalézaví, doplňují si informace o svých obětech přes vyhledávače, posílají e-maily, útočí přes ICQ a jiné internetové prostředky. Může jít o lidi úplně neznámé nebo naopak o jedince, kteří postižené osobně znají například ze školní třídy. Ačkoli jsou nebezpečí internetové agrese vystaveni všichni bez rozdílu, u dětí se jedná o problém mnohem závažnější.

Cyberstalking má svůj původ v anglickém slově „stalking“ – lovit nebo pronásledovat. To přesně vystihuje povahu útočného chování některých osob na internetu. Stalker si nejprve pečlivě vyhlédne svou oběť – obvykle někoho slabého, bez větších zkušeností s internetem, někoho, kdo reaguje na provokace, atd. Právě děti splňují požadavky „ideální kořisti“. Poté začne pronásledování, slovní napadání spojené se zjišťováním informací o oběti, ponižování před ostatními, zaplavování agresivními

[95] SLUNECNICE.CZ, *Bezpečnost dětí*. Zdroj:http://www.slunecnice.cz/special/bezpecnost-deti. 01.10.2009

e-maily a SMS zprávami, negativní komentování na blozích atd. Nejvíc děsivé bývá vyhrožování konfrontací v reálném světě (například: „Já si tě najdu, chytím tě v parku a zmlátím tě.“).

Hlavním motivem stalkera je dokázat nadřazenost nad obětí a tím i sám sobě potvrdit svou vlastní sílu, moc, velikost. Jde mu o to, vyvolat v oběti co největší možný strach, a pak jí díky tomuto strachu kontrolovat. Ve velkém množství případů je stalker veden touhou se nějak pobavit, což ale vůbec nesnižuje závažnost jeho jednání.

Kyberšikana se hodně podobá cyberstalkingu, přesto je v něčem odlišná - o dost zákeřnější. Oběť většinou agresora(y) zná, pouze netuší, že útoky pocházejí právě od nich. Kyberšikana se dá srovnávat s klasickou šikanou – dochází k ponižování postižených z různých stran apod. Také s ní bývá velmi často provázána. Internet však dodává tomuto patologickému chování úplně nový rozměr. Známý je např. případ z roku 2006, kdy čtrnáctiletá tichá dívka byla dlouhodobě obtěžována svými spolužáky. Vyvrcholilo to tím, že přímo ve třídě gymnázia ji spolužáci chytli a předváděli, že jí znásilňují. Všechno natočili na mobilní telefon s úmyslem umístit video na internet. Dívka tlaku neodolala a spáchala sebevraždu.[96]

3.5.3 Děti - stahování a sdílení nelegálního obsahu

S tím, jak se zvětšuje velikost přenosů dat na internetu, se stále častěji řeší otázka ochrany autorských práv ve virtuálním světě. Zákon 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, nijak výrazně neošetřuje zvláštní povahu internetu. Dle něj je zpřístupnění díla prostřednictvím internetu nutno považovat za sdělování díla veřejnosti (§ 18a Z.č. 121/2000 Sb. násl. autorského zákona) a rozmnožování díla (§ 13a Z.č. 121/2000 Sb. násl. autorského zákona).[97] Jinak řečeno: audiovizuální či textový obsah (hudba, filmy apod.) chráněný autorským zákonem lze z internetu legálně pro osobní potřebu stáhnout, ale další sdílení či jiné rozšiřování je již protizákonné. Oproti tomu chráněný software by se neměl ani stahovat.

Dětské a mladistvé viníky čeká při odhalení jejich nelegální činnosti dost tvrdý trest. Děti pod 15 let nejsou trestně odpovědné, soud jim však může v případě prokázání

[96] Internet a kyberšikana, Zdroj: http://cms.e-bezpeci.cz/content/view/36/39/lang,czech/. 06.07.2009

[97] 398. Úplné znění zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem utorským a o změně některých zákonů (autorský zákon), jak vyplývá z pozdějších změn, tiskárna Ministerstva vnitra částka 126, ročník 2006

viny uložit výchovná opatření a musí sami nebo s pomocí rodičů vydat zisk i zaplatit dvojnásobek ceny běžných licencí nelegálně nakopírovaných materiálů. Pokud je viníkům mezi 15 a 18 lety, hrozí jim až 2,5 roku vězení a pokuta do výše půl milionu korun. Samozřejmostí je zabavení pirátských kopií (pokud jsou ve hmotné podobě), propadnutí zařízení sloužícího k trestné činnosti a zabavení veškerého zisku. Krom toho následuje dohled probačního úředníka a další výchovná opatření.

V roce 1958 vytvořil Lawrence Kohlberg teorii morálního vývoje, která by šla přenést na situaci, jak děti a mladiství vnímají internetové pirátství. Pro děti je typické *předkonvenční stádium* uvažování o morálce – nejprve se řídí dle názorů rodičů a možných trestů a poté je nejvíc zajímá vlastní prospěch. Pečující osoba se stává příkladem-vzorem, dítě její chování do velké míry kopíruje a názory bere za vlastní.

Mladiství se zase nacházejí v *konvenčním stádiu morálního vývoje* – chtějí dosáhnout shody se svým okolím a mají sklon podřizovat se nařízení autorit. Situaci však komplikuje pubertální období, tolik charakteristické odmítáním zažitých rodinných a sociálních pořádků. Protože společnost obecně toleruje stahování - sdílení nelegálního obsahu na internetu - a v kruzích náctiletých se dnes dá dokonce označit za módní, zákony vyznávající rodič má se svým potomkem velmi těžké pořízení. V mnoha případech tomu nepomůžou ani názorné příklady České protipirátské unie.[98]

3.5.4 Děti - online hry a jejich potenciální nebezpečí

„Snili jste někdy o tom být crackerem a dostávat se na počítače vlády či podobných organizací? Chtěli byste někdy zažít pocit, jaký máte, když se dostáváte na server a nevíte, kolik vteřin zbývá, než zjistí vaši IP adresu? Pokud je odpověď na tyto otázky ano, pak věžte, že hra Uplink je právě pro vás.“

Tak takhle začíná upoutávka na hru Uplink. Při této hře se hráč dostane do role agenta v crackerské společnosti s názvem Uplink a bude si vydělávat na své živobytí ne zrovna počestným způsobem. Tím je míněno nabourávání se do vládních serverů, krádeže dat, destrukce databází a podobné úkoly, které obyčejný uživatel internetu neprovádí. A jak vůbec probíhá crackování? Zjednodušeně lze říci, že hráč si koupí na uplinkovém obchodě program za určitý počet herních peněz a používá ho na získávání administrátorských hesel. Ve hře se budoucí cracker setká se společností, která se snaží

[98] ČPU – založena v r. 1992 za účelem ochrany autorského práva a práv souvisejících s právem autorským k audiovizuálním dílům a za účelem potírání všech forem pirátství v oblasti výroby, dovozu a šíření audiovizuálních děl.
Zdroj:http://www.filmynejsouzadarmo.cz/cs/co-na-to-osobnosti/, http://www.cpufilm.cz. 05.09 2009

vyrobit virus na zničení internetu, a tady dostane hráč na výběr, zda bude společnosti při vývoji viru pomáhat, nebo zabrání zničení celého internetu. Podle toho, jak je hráč ve hře úspěšný, získává na popularitě a otevírají se mu další možnosti ve hře.

Poslední dobou stále stoupá trend online hraní. Není se čemu divit – virtuální prostředí je stále více propracovanější a interaktivnější. Online hry s sebou ale nesou mnohá rizika, která mohou poškodit jak psychické, tak fyzické zdraví (nejen) dětí. To je právě vidět na výše zmiňované hře, která se svým zaměřením snaží vychovat potencionální kybernetické zločince. Jako velmi negativní vidím i to, že hráč nedokáže ve skutečnosti rozlišit realitu od fiktivního imaginárního světa. Hra, která se snaží upoutat způsobem, že si hráč zvyšuje hladinu adrenalinu tím, že musí splnit úspěšně úkol, který zničí práci ostatních, a on sám nebude nikdy odhalen, není a nepatří mezi kladně motivující činnost. Přesto hry představují i zábavu, odreagování, relaxaci a kupodivu se při hraní cvičí pozornost, analytická část inteligence a překvapivě v určité míře zlepšuje i zrak. Moderní monitory zářením tolik neškodí a potřeba rychlého přeorientování pohledu v některých akčnějších sekvencích trénuje oči. Často se taky mezi odborníky mluví o tom, že málo společenští jedinci díky virtuálnímu světu překonají svůj ostych a hraní je paradoxně přibližuje normálnímu světu mezilidských vztahů. Tohle všechno je však podmíněno tím, že u toho nebudou hráči trávit několik hodin denně. Skutečnost je však přesně opačná. Často dochází k poškozování zraku, poruchám sluchu a někdy se hovoří i o riziku „virtuální“ nevolnosti a epilepsii.[99]

3.5.5 Děti – identita a anonymita na webu

Kyberprostor je obecně považován za prostředí, kde se každý může vydávat za někoho jiného. Ze své praxe vím, že tomu tak není, jelikož existují technické prostředky, pomocí nichž lze identitu jednotlivých uživatelů odhalit. Někdy je to však dosti obtížné a brání tomu i různé legislativní předpisy. Děti ale nejsou IT odborníci a většina pachatelů podobných činů také ne, takže je pro ně anonymita internetu v podstatě absolutní. Pod pojmem anonymita na internetu si lidé představují to, že se mohou libovolným způsobem vyjádřit, projevit a lhát bez pocitu viny za své chování. Chybí zde dohled společnosti (veřejné pohoršení) a vytváří se tak prostor pro uskutečňování jinak nepřijatelných tužeb, z nichž některé mohou být zvrácené a ohrožující ostatní. Děti tvoří zvláště zranitelnou skupinu. Na internetu totiž funguje

[99] SLUNECNICE.CZ, *Bezpečnost dětí.* Zdroj:http://www.slunecnice.cz/special/bezpecnost. 01.10.2009

spousta webů určených dětem, které však nenavštěvují pouze ony. Mezi uživateli se najdou i osoby vydávající se např. za filmové a hudební hvězdy, za důvěryhodné vrstevníky dětí nebo za pečující a milé starší osoby. Jejich cílem je dosáhnout setkání v reálném světě, dostat z nich adresu bydliště, telefon apod. Jednají většinou velmi opatrně, nechtějí vzbudit podezření, a jsou schopní čekat na svou příležitost týdny, měsíce nebo i roky. Zdůrazňují potřebu zachovat vznikající vztah jako „malé společné tajemství“. Snaží se o vyvolání emoční závislosti oběti na útočníkovi. S postupem času někteří z nich začínají zdůrazňovat erotická témata, posílat nevhodné fotografie, videa atd. Vše může skončit až patologickou manipulací oběti. Ve světě je toto chování známé pod anglickým termínem **„cyber grooming“** – jednání manipulátora, které má v dítěti vyvolat falešnou důvěru a připravit ho na schůzku, jejímž cílem je oběť pohlavně zneužít .[100]

Bohužel, jak prokazují studie mnoha společností (např. Saferinternet.cz), mladí lidé se osobnímu setkání nabídnutému přes internet nebrání. Ba naopak, nabídky přijímají. Starší děti (16 let a více) chodí na takové schůzky povětšinou sami. O všem pak poví raději svým kamarádům, sourozencům, ale hlavně ne rodičům. Považují to totiž za osobní záležitost nebo si myslí, že rodiče se stejně o takové věci nezajímají, popřípadě se bojí, aby jim to nezakázali. Zde se jasně projevuje dětská (často přehnaná) důvěra ve vlastní schopnost zvládnout situaci a zároveň je vidět klamavý vliv tohoto média, kdy lidé přikládají zde vyřčeným názorům a věcem větší význam než ve skutečnosti představují.

3.5.6 Děti a „závislost“ na internetu

Počítačové hry, komunikace po internetu i mobilní telefony se mohou stát návykové podobně jako drogy. V roce 1995 zveřejnil newyorský psychiatr Ivan Goldberg zprávu, že objevil nový typ psychické závislosti. Lidé při ní opouštějí své rodiny, přátele a tráví hodiny s počítačem serfováním po internetu nebo hraním on-line her. Goldberg označil tuto poruchu termínem IAD – Internet Addiction Disorder, závislost na internetu. O stejném problému psala o rok dříve i psycholožka Kimberley Youngová. Záležitostí se od té doby zabývala řada odborníků, zdaleka ne všichni jsou však přesvědčeni, že IAD skutečně existuje.

[100] KOPECKÝ, K. *Cyber grooming-projekt E-Bezpečí. Zdroj:http://www.e-bezpeci.cz.* 01.10.2009

Jak se IAD projevuje? Mezi příznaky patří únava, zanedbávání základních potřeb, jídla a pití, spánku či hygieny. „Závislý“ se od běžného uživatele odlišuje tím, že se cítí být kyberprostorem pohlcen, má problémy o virtuálním světě přestat přemýšlet, nedrží se naplánovaných časů pobytu na internetu a v případě jeho nedostupnosti vykazuje abstinenční příznaky v podobě napětí, vzteku či depresivních stavů. Postupně se odklání od nejbližších vztahů s rodinou a s přáteli, přestává se tak dobře orientovat v sociálním světě a častěji ho přepadne stres. Má problémy se spánkem a vůbec s denním režimem, hraje do noci, budí se vyčerpaný. Začíná lhát o svém virtuálním životě a snaží se „zakrývat“ svou „závislost“. Druhotným následkem závislosti na internetu mohou být dále bolesti zad, poruchy zraku a další komplikace způsobené nedostatkem pohybu.Tyto konflikty se u dětí projevují vždy výrazněji. Zpravidla používají internet a počítač pro zábavu (hry, komunikace s ostatními vrstevníky), ač jim je rodiče pořizovali hlavně pro jiné účely (škola, atd.). On-line hry zase nabízejí možnost sociálního kontaktu i těm, kteří jsou jinak z jakéhokoliv důvodu hendikepovaní. [101]

Odborníci se často přiklání k názoru,že „závislost“ na internetu je zvláště u dětí a mladistvých ve své podstatě projevem hlubších problémů v rodině anebo vůbec v sociálních vztazích (např. širší rodina, škola). Přesto jedna ze studií prováděných na toto téma odhalila jisté osobnostní charakteristiky společné lidem s náchylností k této „závislosti“. „Závislí“ obvykle mají větší sklon spoléhat sami na sebe, jsou citlivější, nechtějí se moc odhalovat a nejsou příliš konformní.[102]

A co děti nejčastěji na webu hledají? Podle výzkumu společnosti Symantec, který probíhal od února do června 2009, byl stanoven dětský žebříček 10 nejvyhledávanějších výrazů: YouTube, Google, Facebook, Sex, MySpace, Porno, Yahoo, Michael Jackson, Fred (populární fiktivní osoba na Youtube), eBay. Že se však na čtvrté a šesté místo dostal sex, respektive porno, by nás mělo vést k zamyšlení.[103]

[101] BLINKA, L. *Generace závislých? Dospívající a online hry.* FSS MU Zdroj: http://ivdmr.fss.muni.cz/info/storage/. 15.06.2009

[102] SLUNECNICE.CZ, *Bezpečnost dětí.* Zdroj http://www.slunecnice.cz/special/bezpecnost, 01.10.2009

[103] *Děti na Iinternetu nejčastěji hledají youtube, google, facebook i porno*. Zdroj:http://technet.idnes.cz, 12.08.2009

4. EMPIRICKÝ PRŮZKUM

4.1 CÍLE VÝZKUMU

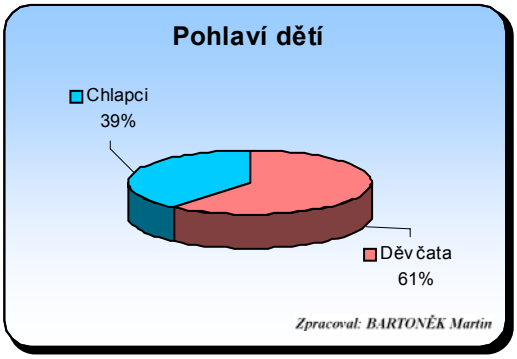
Pro svůj empirický výzkum jsem zvolil metodu dotazníku. Cílem výzkumu bylo získat přehled o tom, kde a jak často děti přistupují k internetu, kolik hodin v průměru tráví na tomto médiu, i jaké aktivity a frekvence využití jsou s jejich činností ponejvíce spojené. V této souvislosti jsem také zjišťoval, s kým nejčastěji komunikují, jaké rizikové činnosti při práci provádějí, zda mají stanovená pravidla pro práci na internetu doma i ve škole, jakým způsobem se liší a zda se jimi řídí. Nakonec jsem ještě použil doplňující otázku z oblasti bezpečnostního nastavení počítačového systému, konkrétně zda mají na počítači nainstalován program pro blokování závadného obsahu z internetu. Zvolil a použil jsem formu uzavřených otázek, pro jejich jednoduchost, stručnost i jednoznačnost při vyplňování a přehlednějším zpracování.

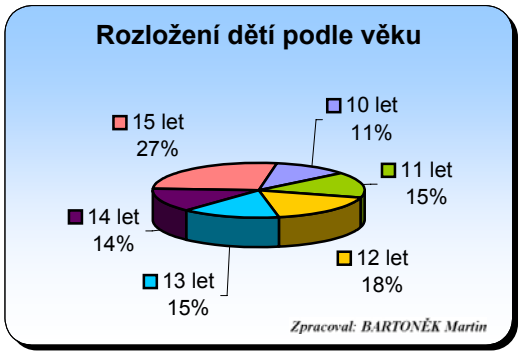
4.2 PRŮBĚH VÝZKUMU

Nejdříve jsem sestavil dotazník s konkrétními otázkami zaměřenými ke shromáždění dat, které jsem chtěl zjistit a které souvisely s cílem výzkumu. Následně jsem provedl předvýzkum, abych si otestoval, zda je dotazník jasný, srozumitelný a vyhovující pro všechny oslovené věkové kategorie. Na základě jeho výsledků jsem doplnil a upravil nejasné položky. V dalším kroku jsem dotazník po dohodě s ředitelem Základní a Mateřské školy Kotlářská 4, Brno, p. Mgr. Zřídkaveselým L. a p. učitelkou Mgr. Krumpholcovou K. z Biskupského gymnázia Barvičova 85, Brno, rozeslal elektronickou formou. Příslušní vyučující ho pak na hodinách informatiky zadali svým žákům. Musím však podotknout, že jeho vyplnění bylo dobrovolné. Vše probíhalo v měsících říjen až listopad 2009. Dotazník vyplňovaly děti ve věku 10 až 15 let. Záměrně jsem chtěl, aby byl vyplněn ve škole, bez asistence rodičů, v zájmu zajištění nezávislosti a objektivity získaných dat. Celkem jsem takto obdržel 211 vyplněných dotazníků.

4.1 VYHODNOCENÍ DAT

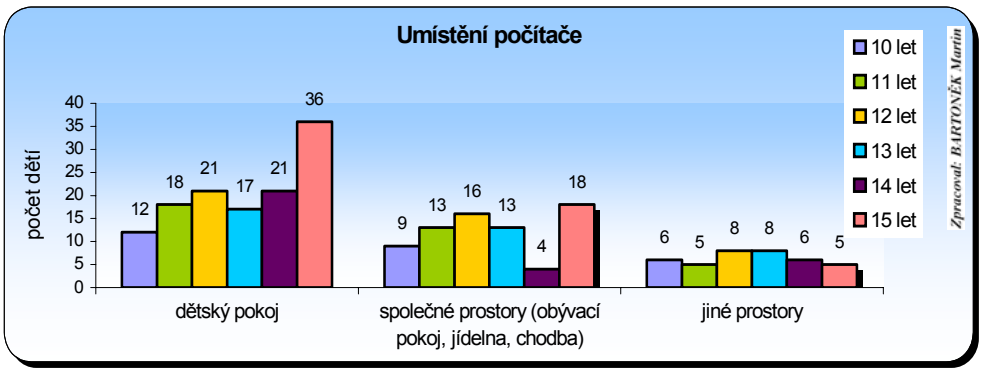
Demografická skladba dětí





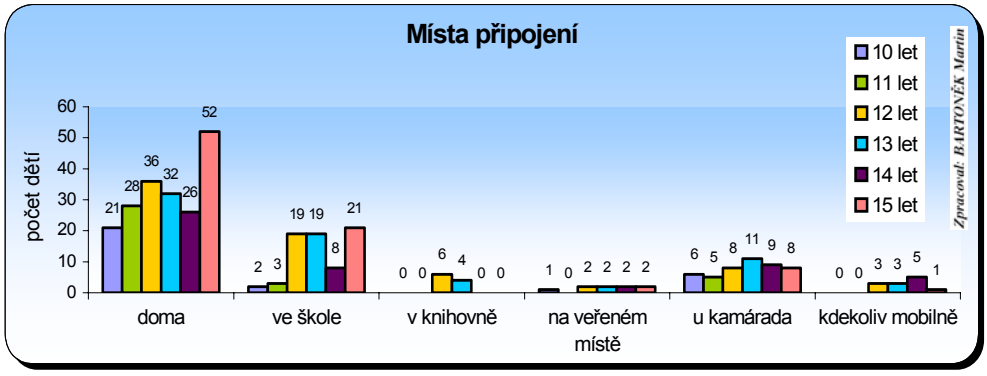
Dotazník odevzdalo celkem 211 dětí, z toho bylo 128 děvčat a 83 chlapců. Poměrné zastoupení dětí bylo následující: 10 let = 11%, 11 let =15%, 12 let =18%, 13 let = 15%, 14 let = 14%, 15 let = 27%.

Umístění počítače, na kterém děti nejvíce pracují



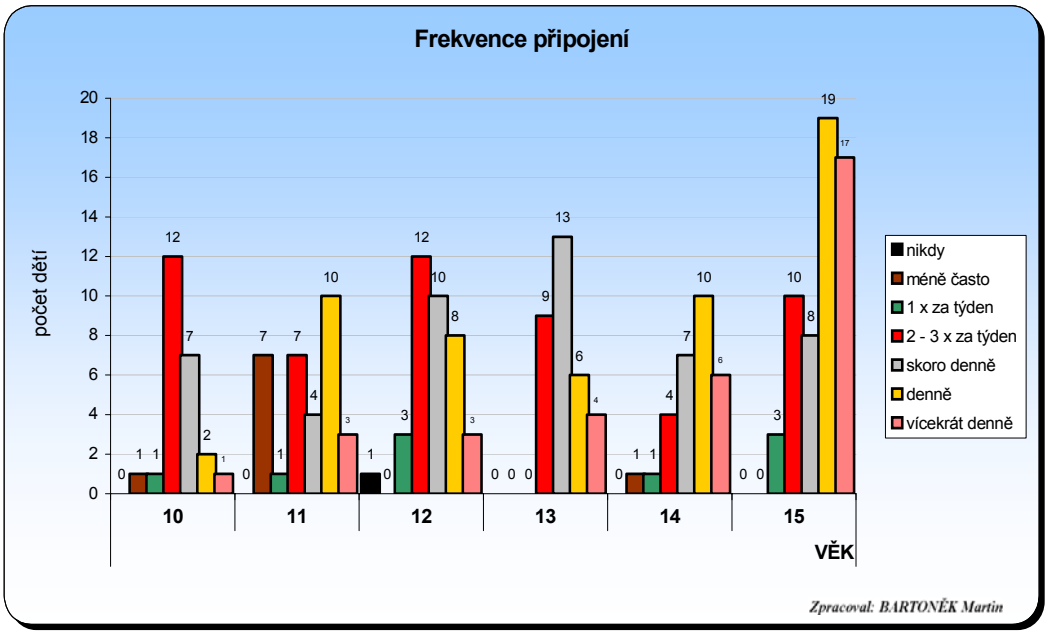
Co se týká umístění počítače, je stav následující: dětský pokoj = 53%, společné prostory (obývací pokoj, jídelna, chodba) = 31%, jiné prostory = 16%. Z toho plyne, že více než polovina dětí má počítač u sebe v pokoji.

Místa připojení k internetu



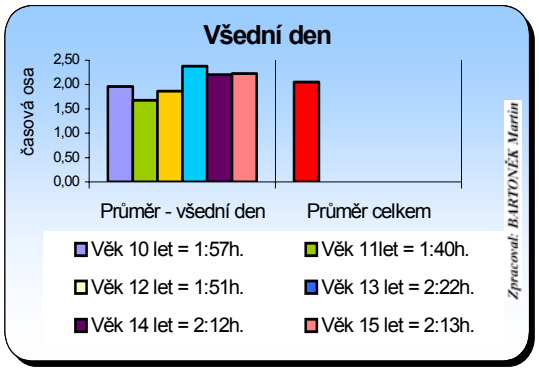
Nejčastějším místem připojení k internetu je z domova = 56%, následuje škola = 21%, u kamaráda = 14%, ostatní místa (knihovna, veřejná místa, kdekoli mobilně) nejsou tak významná a mají shodně po 3%.

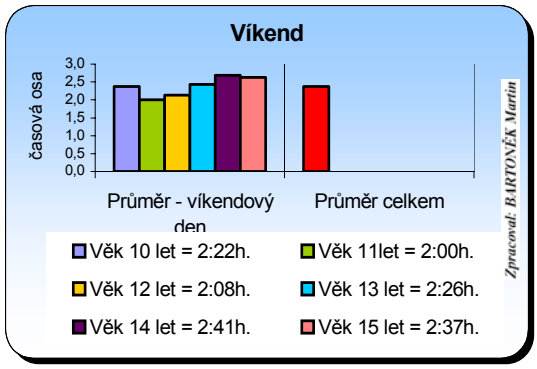
Frekvence připojení k internetu



Frekvence připojení dětí k internetu: vícekrát denně 49%, denně 16%, skoro denně 14%, 2–3 x za týden 15%, 1 x týdně 3% a méně často 3%.

Počet hodin strávených na internetu ve všední den a o víkendu

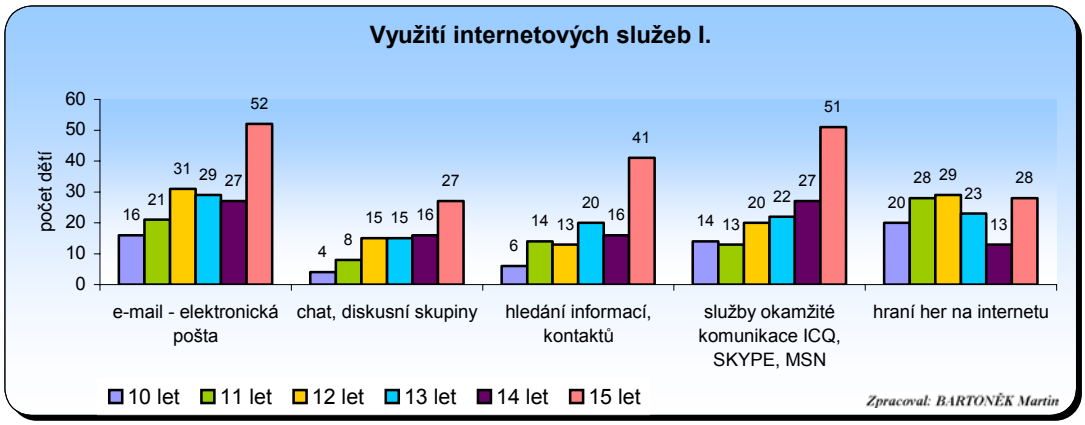


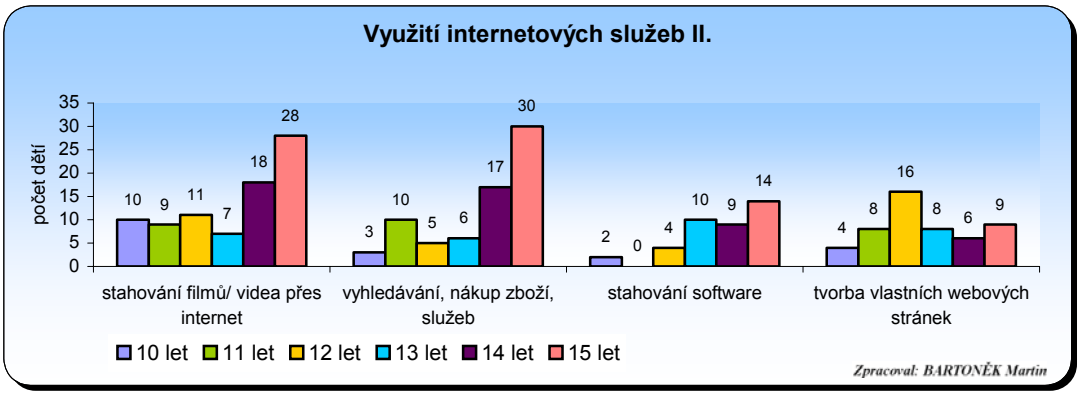


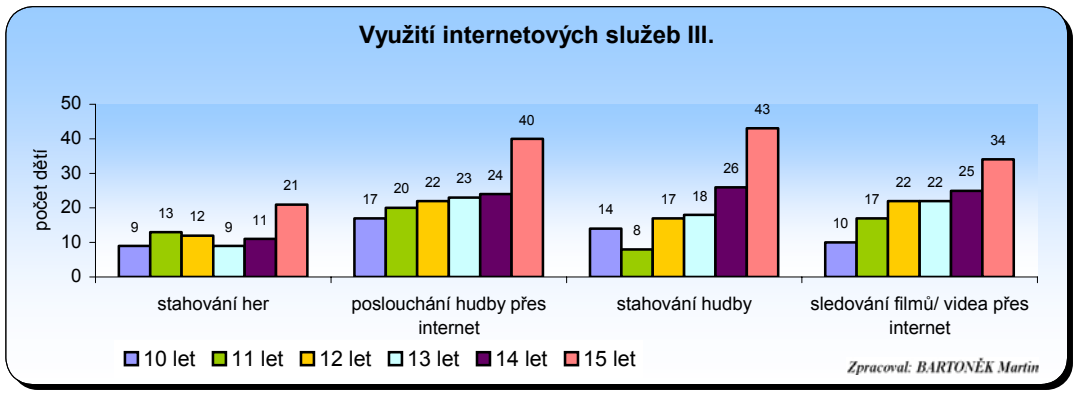
Průměrná doba strávená dětmi na internetu ve všední den je 2h 03m.

Průměrná doba strávená dětmi na internetu o víkendu je 2h 22m.

Různé druhy internetových služeb a jejich využití

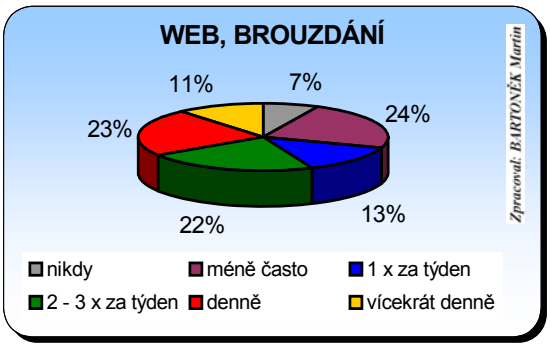


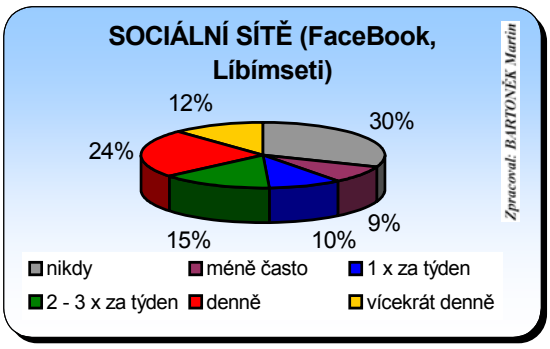


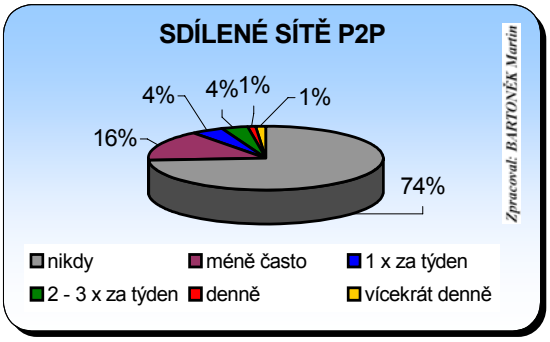


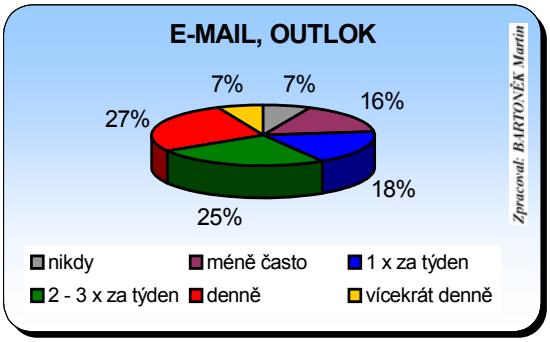
Ze tří grafů, které znázorňují různé internetové služby, je patrné rozdělení na služby více a méně oblíbené. Pokud je tedy seřadíme podle míry využití, dostaneme se k následujícímu pořadí: služby okamžité komunikace (ICQ, SKYPE, MSN, CHAT, diskusní skupiny) = 17%, e-mail = 13%, poslech hudby = 11%, hraní her na internetu = 10%, stahování hudby, sledování filmů/videa = 9%, hledání informací/kontaktů = 8%. vyhledávání, nákup zboží, služeb = 5%, tvorba vlastních webových stránek = 4%, stahování software = 3%.

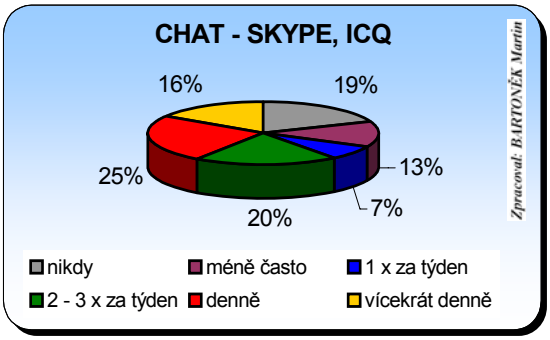
Frekvence využití vybraných internetových služeb





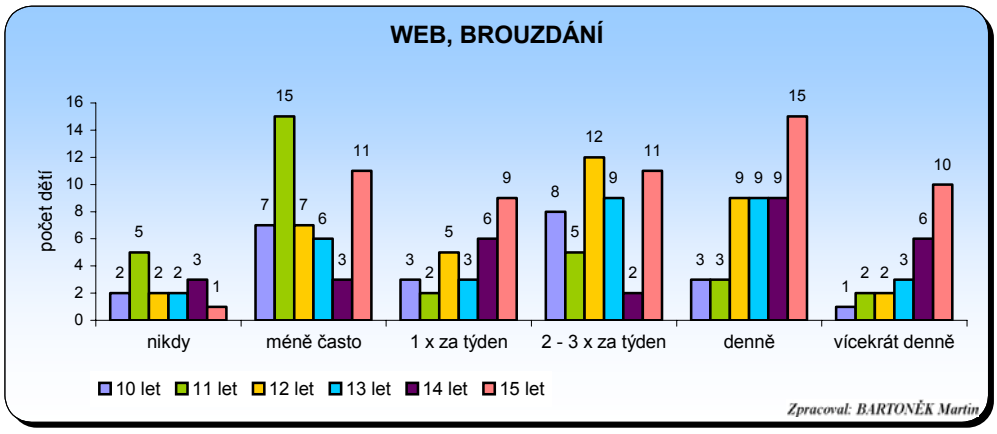


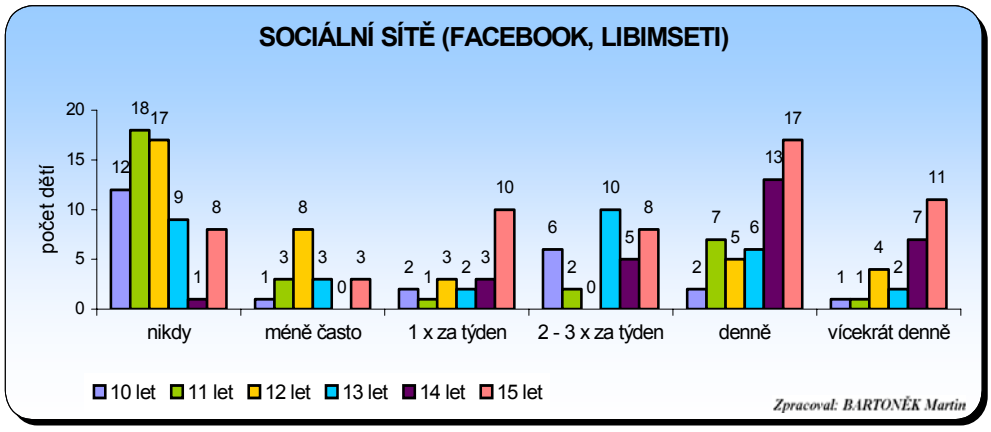


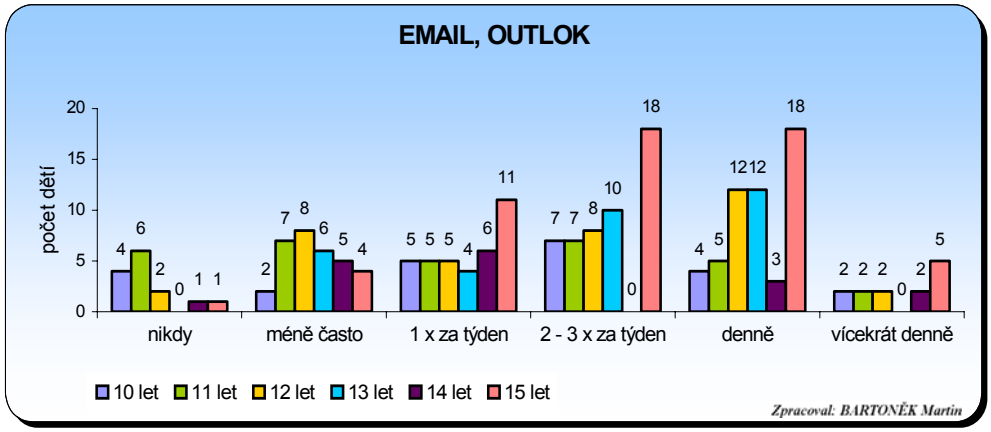


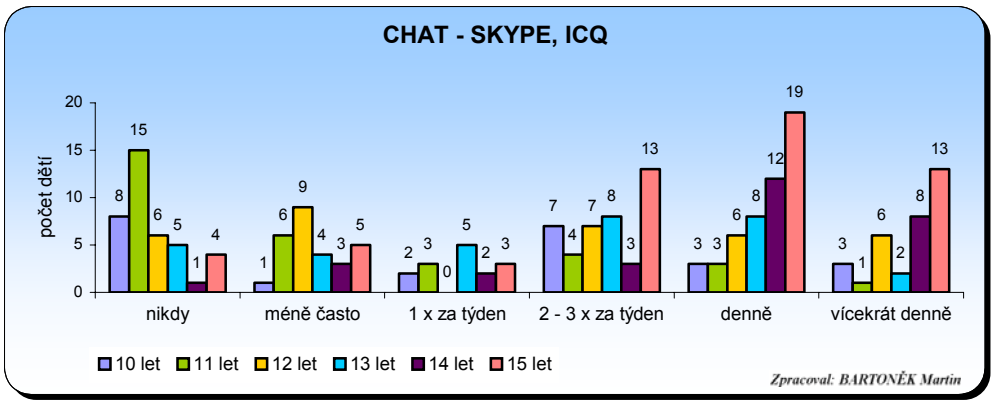
Na výsečových grafech je vidět frekvence využití jednotlivých internetových služeb, společně pro všechny věkové kategorie. Nejméně děti využívají službu P2P (peer tu peer – výměnné sítě, které slouží mezi samotnými uživateli k výměně dat).

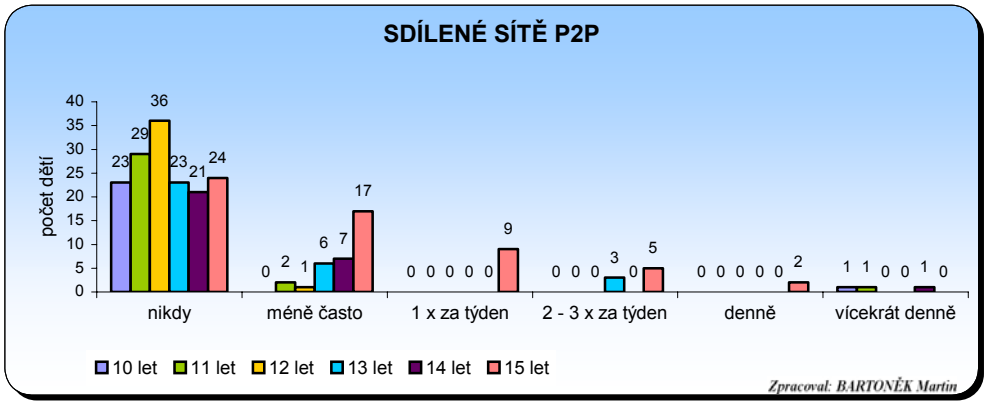
Přehled Využití jednotlivých internetových služeb dle věkových kategorií



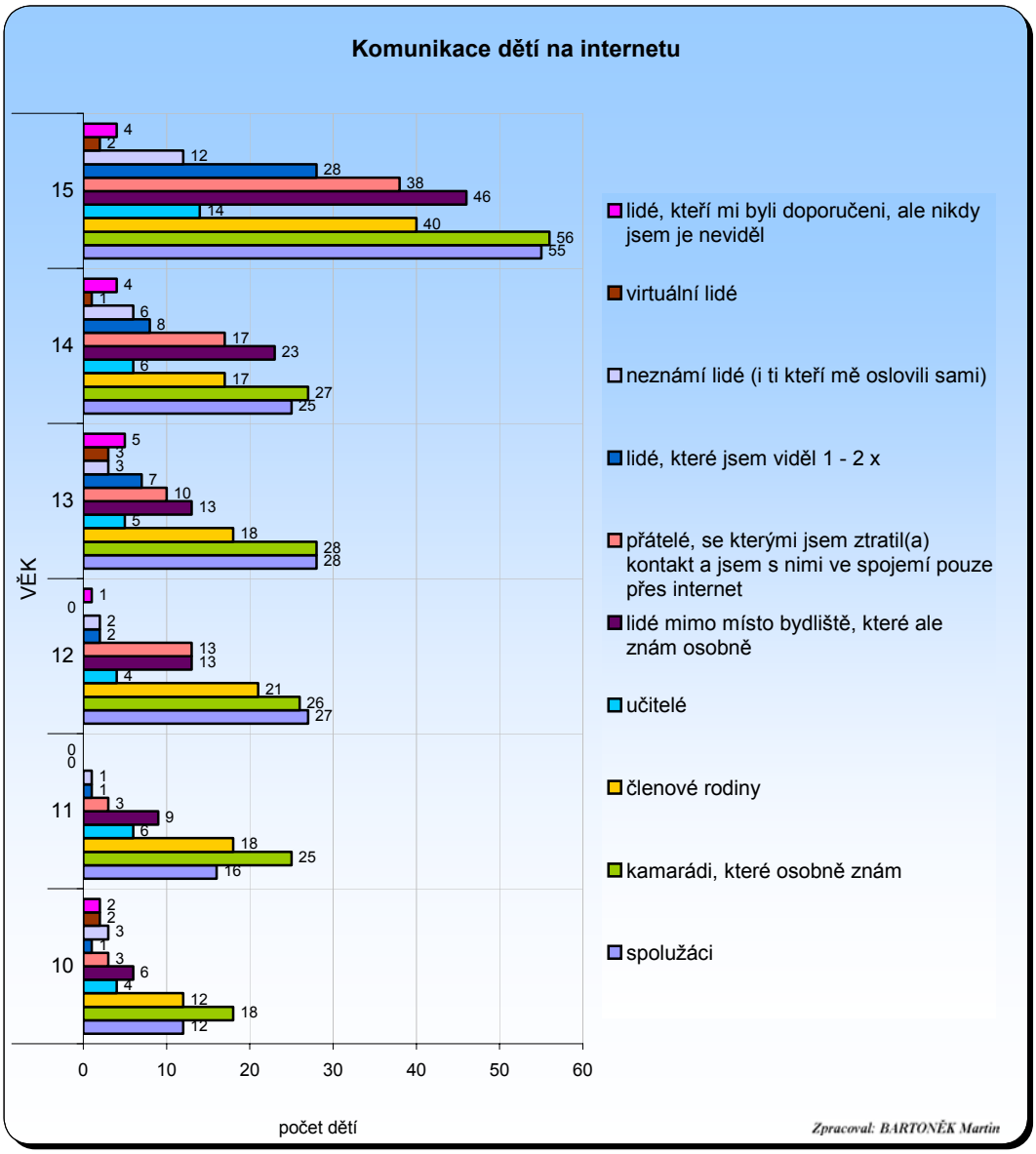

SOCIÁLNÍ SÍTĚ (FACEBOOK, LIBIMSETI)
počet dětí
nikdy
méně často
1 x za týden
2 - 3 x za týden
denně
vícekrát denně
10 let
11 let
12 let
13 let
14 let
15 let
Zpracoval: BARTONĚK Martin


EMAIL, OUTLOK
počet dětí
nikdy
méně často
1 x za týden
2 - 3 x za týden
denně
vícekrát denně
10 let
11 let
12 let
13 let
14 let
15 let
Zpracoval: BARTONĚK Martin


CHAT - SKYPE, ICQ
počet dětí
nikdy
méně často
1 x za týden
2 - 3 x za týden
denně
vícekrát denně
10 let
11 let
12 let
13 let
14 let
15 let
Zpracoval: BARTONĚK Martin

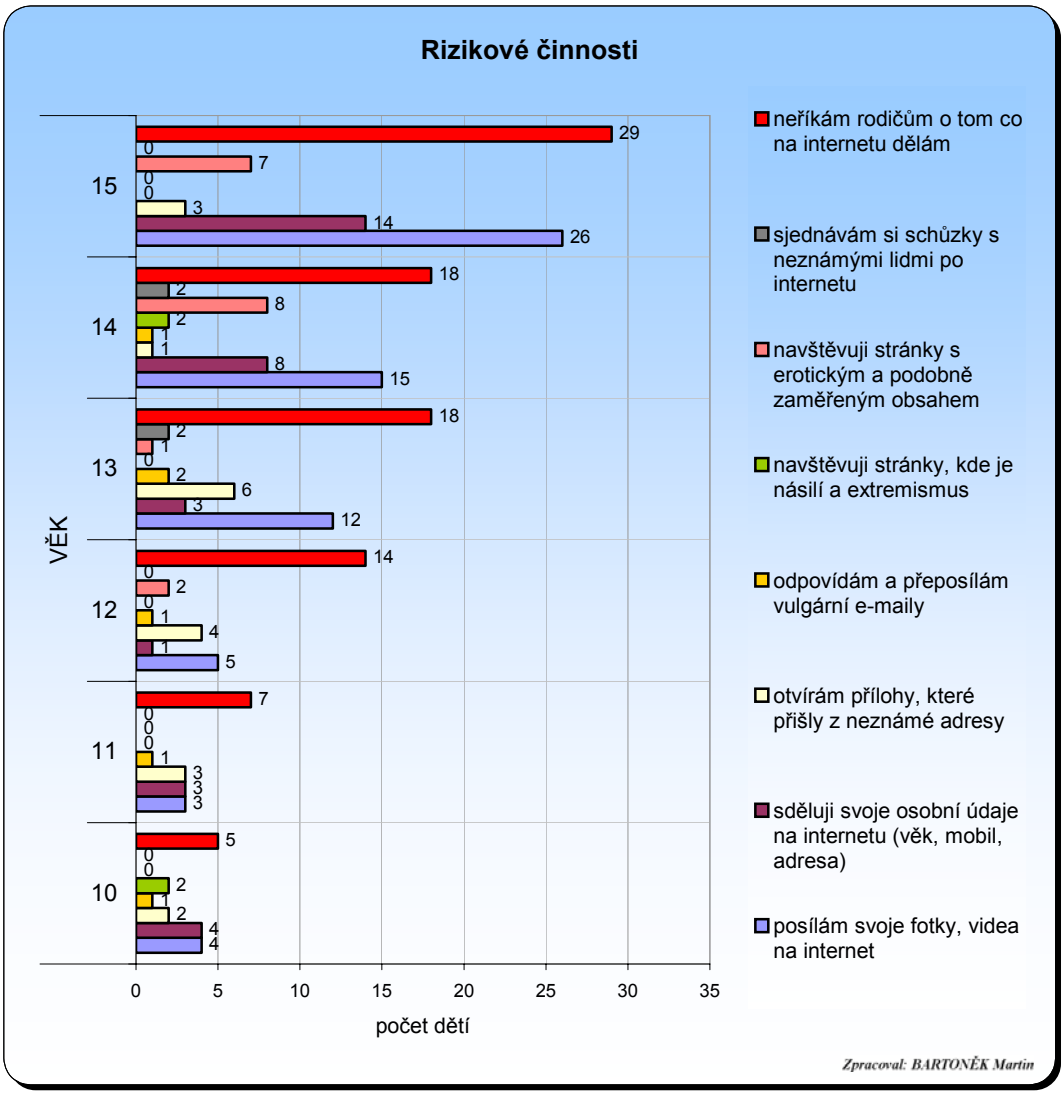

SDÍLENÉ SÍTĚ P2P
počet dětí
nikdy
méně často
1 x za týden
2 - 3 x za týden
denně
vícekrát denně
10 let
11 let
12 let
13 let
14 let
15 let
Zpracoval: BARTONĚK Martin

Komunikace dětí na internetu



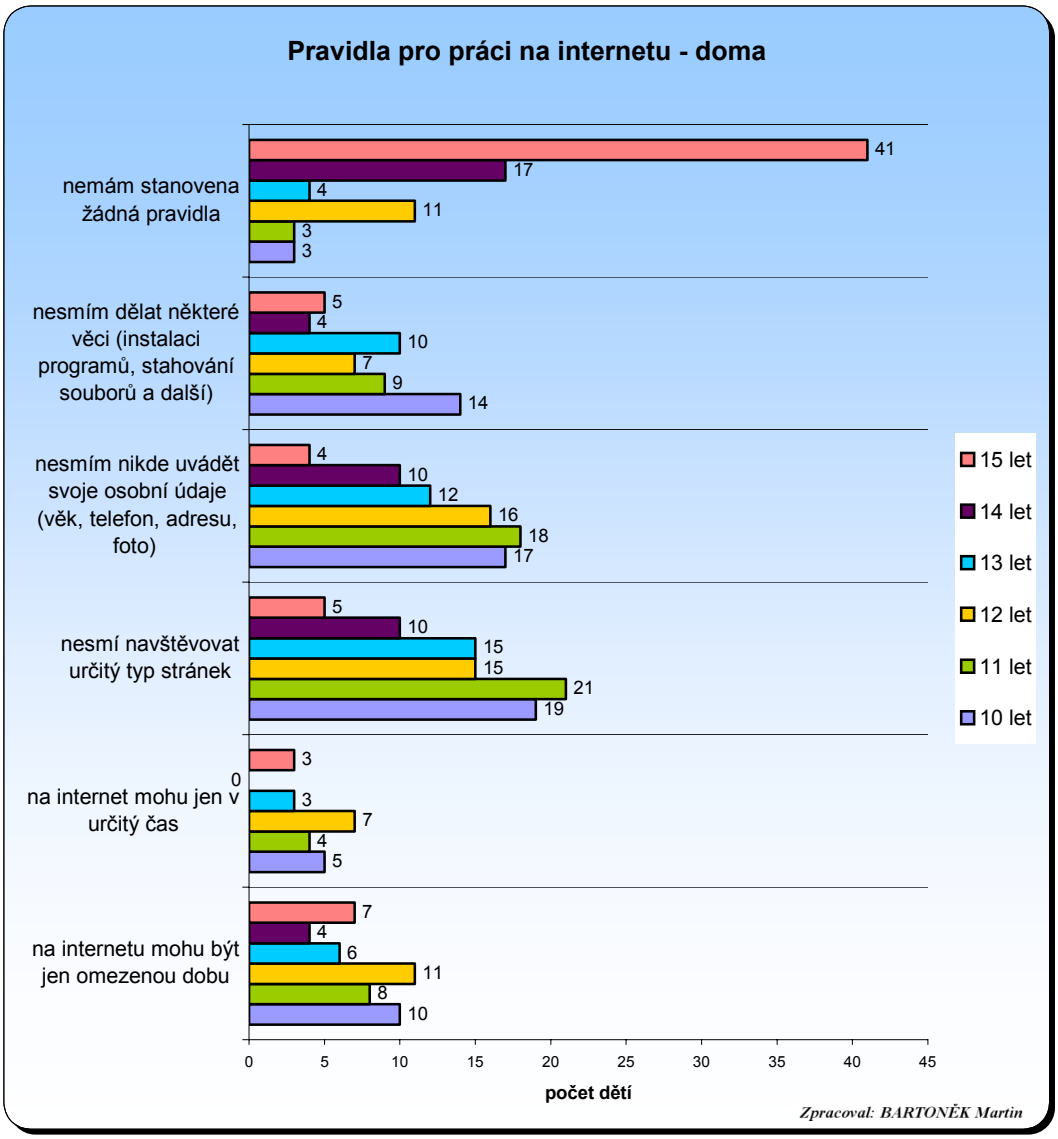
Komunikace dětí přes internet roste úměrně s věkem. Podíl jednotlivých věkových kategorií je následující: 10 let =8%, 11 let = 10%, 12 let = 14%, 13 let = 15%, 14 let = 17%, 15 let = 36%. Dále je možné z grafu vyčíst, s kým děti nejčastěji komunikují: kamarádi, které osobně znám (22%), spolužáci (20%), členové rodiny (16%), lidé mimo místo bydliště, které znám osobně (14%), přátelé, se kterými jsem ztratil(a) kontakt a jsem s nimi ve spojení pouze přes internet (11%), lidé, které jsem viděl(a) 1 – 2 krát (6%), učitelé 5%, neznámí lidé (i ti kteří mě oslovili sami (3%), lidé, kteří mi byli doporučeni, ale nikdy jsem je neviděl(a) (2%), virtuální lidé (1%). Za pozornost jistě stojí, že z celkového počtu 211 dětí jich celkem 43 (5%) komunikuje s neznámými lidmi.

Rizikové činnosti, které děti provádějí na internetu



Pro všechny věkové kategorie shodně platí, že nejvíce se děti odmítají svěřovat rodičům s tím, co na internetu dělají (37%). Hodně také posílají svoje fotky, videa na internet (26%) a sdělují svoje osobní údaje - věk, mobil, adresa (14%). Co se týká návštěvy stránek s erotickým a podobně zaměřeným obsahem, trend se začíná objevovat až od 12. roku věku (8%). Naproti tomu problém otvírání příloh z neznámé adresy (8%) má stoupající charakter v kategorii od 10 let do 13 let (79%), v kategorii 14 a 15 let se tato činnost snižuje (21%). Jako naprosto zanedbatelné se jeví aktivity odpovídání a přeposílání vulgárních e-mailů (3%). Shodně po 2 % mají činnosti: sjednávání si schůzky s neznámými lidmi po internetu a návštěva stránek s násilím a extremismem. Zde bych se pozastavil nad tím, že se jedná již o děti ve věku 10 a 14 let.

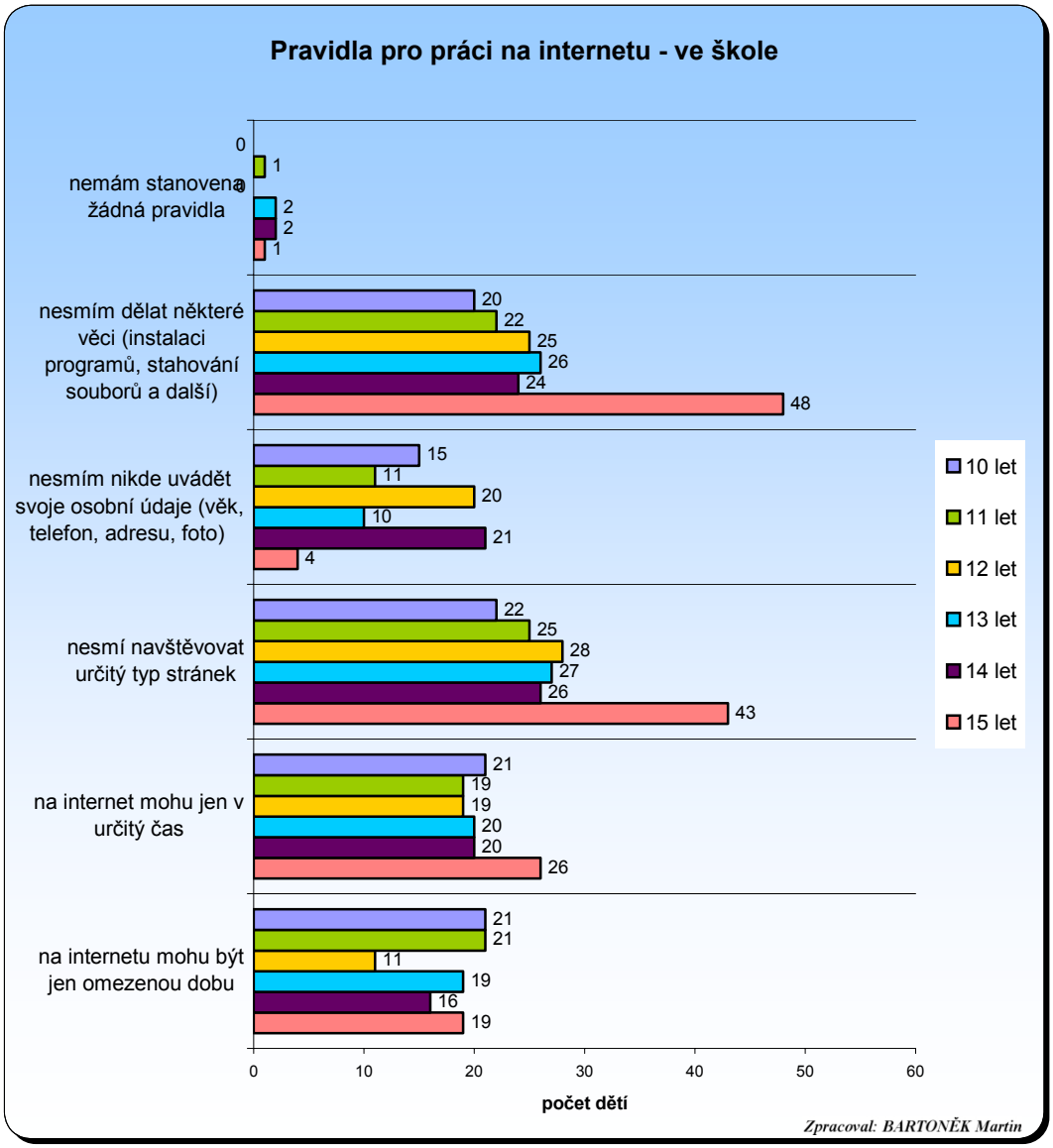
Pravidla dětí pro práci na internetu doma



Celkem 63% dětí má doma stanovená pravidla a 37% nemá stanovena žádná. Podíl jednotlivých věkových kategorií je: 10 let = 23%, 11 let = 22%, 12 let = 20%, 13 let = 16%, 14 let = 10%, 15 let = 9%. Z těchto hodnot vidíme, že se zvyšujícím se věkem mají děti již méně stanovená pravidla pro práci na internetu.

Pokud porovnáme podíl hodnot jednotlivých pravidel, zjistíme že nejvíce by měly děti dodržovat pravidlo, při kterém nesmí navštěvovat určitý typ stránek (30%), nikde neuvádět svoje osobní údaje – věk, telefon, adresu, foto (28%), následuje zákaz instalace programů, stahování souborů a další (18%), na internetu mohou být jen omezenou dobu (16%), a na internet mohou jen v určitý čas (8%).

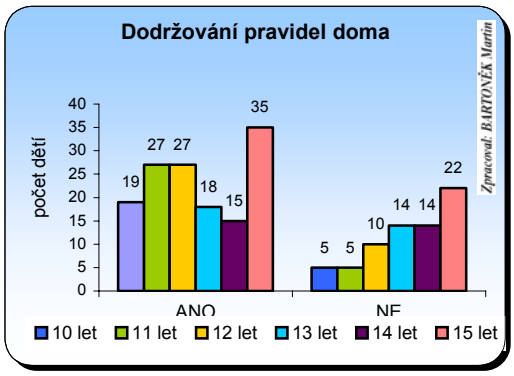
Pravidla dětí pro práci na internetu ve škole

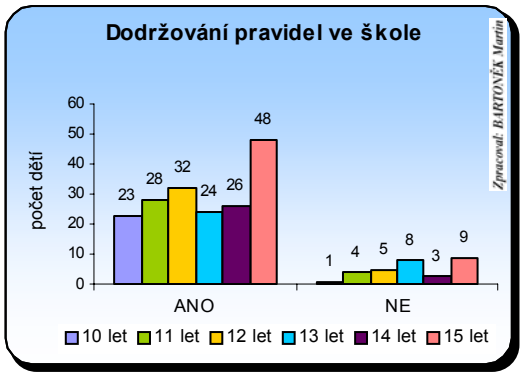


Ve škole má stanovená pravidla pro práci na internetu 97% dětí a 3% dětí odpovědělo, že nemá pravidla žádná. Podíl v jednotlivých kategoriích se pohybuje v rozmezí: 10 ,11 let = 15%, 12, 13, 14 let = 16%, a 15 let = 22% (ve věkové kategorii 15 let je více dětí cca o 10% více). Z uvedeného grafu vyplývá, že ve školách mají nastavená pravidla pro všechny věkové kategorie stejně.

Pokud porovnáme podíl hodnot jednotlivých pravidel, zjistíme, že na rozdíl od pravidel stanovených doma, mají jinou prioritu: nesmí navštěvovat určitý typ stránek (27%), zákaz instalace programů, stahování souborů a další (26%), na internet mohou jen v určitý čas (19%), mohou zde být jen omezenou dobu (16%), nesmí uvádět svoje osobní údaje – věk, telefon, adresu, foto (12%).

Dodržování pravidel doma a ve škole

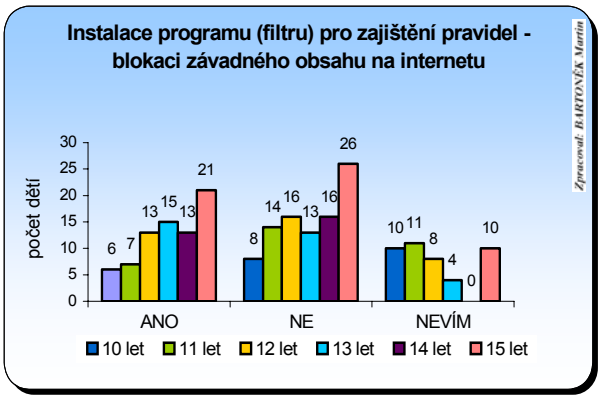




Stanovená pravidla doma dodržuje 67% dětí. Ze sloupcového grafu rovněž vyplývá, že s rostoucím věkem má nedodržování pravidel stanovených rodiči vzrůstající charakter.

Ve škole je poměr dodržování pravidel pro práci na internetu 86% ku 14%.

Počítačový program pro zajištění pravidel využívání internetu



Program pro blokaci některých stránek na internetu má doma nainstalováno 36% dětí, 44% nemá a 20% neví. Obelstít program dovede cca 19% dětí.

4.2 Shrnutí

V praktické části bakalářské práce jsem při zpracování dotazníku dospěl k následujícím výsledkům:

V rámci výzkumu mi bylo umožněno oslovit 2 školy, ZŠ a MŠ Kotlářská 4 Brno a Biskupské gymnázium Barvičova 85 Brno. Z obou těchto školských zařízení odevzdalo dotazník celkem 211 dětí, z toho bylo 61% děvčat a 39% chlapců. Nejvíce vyplněných dotazníků se sešlo z věkové skupiny 15 let (27%).

Více než polovina dětí (53%) má počítač umístěn ve svém pokoji a 31% ve společných prostorách. K internetu se připojují převážně z domova 56% a z menší části ze školy (21%). Téměř 80% z nich se na internet připojuje denně a v průměru na něm stráví více jak 2 hodiny (o víkendu o ½ hod. déle). Mezi nejoblíbenější a nejvíce užívané služby patří zábavná multimediální činnost (poslech hudby, hraní her, sledování filmů) 30% a komunikační služby (e-mail, chat, Skype, ICQ) 24%.

Co se týká frekvence využití vybraných (nejznámějších) služeb na internetu, lze říci, že 38% dětí využívá tyto služby denně, 21% je využije nejméně 2-3 x za týden, 25% 1x týdně a méně, 16% dětí některou ze služeb nevyužije nikdy. Mezi nejméně využitou službu patří výměnné sítě P2P.

Komunikace dětí přes internet obecně i se skupinou neznámých lidí roste úměrně s věkem. Nejčastěji komunikují s kamarády a spolužáky (44%), nemalé číslo 12% tvoří i komunikace, kterou lze označit jako nebezpečnou – s neznámými lidmi, s lidmi které viděly 1-2x, s lidmi na doporučení, s virtuálními lidmi.

Mezi rizikové činnosti, které děti provádějí na internetu patří posílání fotografií a videí (26%), sdělování osobních údajů (14%), návštěva erotických stránek, otevírání příloh z neznámé adresy (8%). Celkem 4 děti (2%) si sjednaly také schůzku s neznámými lidmi.

Jako další otázku jsem zařadil pravidla pro práci dětí na internetu doma a ve škole. Ohledně pravidel doma je vidět, že je rodiče nejvíce stanovují mladším dětem. Kladou důraz na zákaz návštěv určitých typů stránek, uvádění osobních údajů, instalaci programů a snaží se hlídat i dobu strávenou na internetu. Naproti tomu ve škole, jsou pravidla stanovena pro všechny věkové kategorie stejně a o proti těm, která platí doma, se liší pouze ve stanovené prioritě. Je zajímavé, že děti uvedly zákaz uvádění osobních údajů při přístupu na internet ve škole až na posledním místě. Pravidla však dodržují více ve škole 86%, doma je to pouze 67%.

Na otázku softwarového zajištění v souvislosti s pravidly pro využití internetu, skoro polovina dětí (44%) uvedla, že žádný program nemají a 20% neví. Pouze 36% dětí uvedlo, že tento typ ochrany před nebezpečím hrozícím z internetu mají, ale 19% z nich ho dokáže obejít.

ZÁVĚR

Internet bych v současné době přirovnal k „chobotnici s obrovskými chapadly“, pomocí kterých se přenášejí informace po celém světě. Obecně vzato je kyberprostorem, kde je možnost projevovat či uplatňovat vlastní názory a myšlenky. Základní výhodou je jeho otevřenost, rychlost, dostupnost informací a jejich sdílení. V tomto ohledu lze konstatovat, že je jakýmsi ideálním místem pro realizaci svobody projevu bez jakéhokoliv omezování. V důsledku jeho rychlého rozvoje však dochází i k protiprávnímu jednání. Bezpečnostní firmy nestíhají reagovat na neustálé a nové útoky vylepšených virů nebo jiných škodlivých kódů. Počet nezabezpečených stránek roste z měsíce na měsíc a denně se objevují statisíce nových. Dlouhodobé statistiky naznačují, že tento trend bude nadále pokračovat. Na síti tak dnes přestávají platit staré poučky pro bezpečné surfování. Už dávno nestačí vyhýbat se stránkám s podivným obsahem.

S ohledem na samotnou definici svobody projevu jako jednoho ze základních mezinárodně garantovaných práv má i internet své meze. Tou mezí je morální odpovědnost a míra, jakou je svobodně uplatňovaným projevem zasahováno do lidských práv a právního postavení jednotlivých osob, nebo míra, jakou je narušován základní rámec hodnot, na nichž je založena právní a demokratická společnost.

Přestože že zde tedy platí právní řád, jeho aplikace není jednoduchá, někdy dokonce ani možná. Globální charakter internetu je v přímém rozporu s teritoriálními principy práva. Rychlost dějů probíhajících v kyberprostoru znesnadňuje zjišťování informací a znemožňuje dokazování. Největším problémem internetu je zdánlivá anonymita a absence odpovědnosti. Mladí mají často pocit, že kyberprostor je jen hra a pravidla běžného světa tam neplatí. Některé druhy protiprávních činů lze např. v tomto prostoru spáchat snadno a rychle, bez podstatnějších nákladů.

V oblasti práva dochází stále více k vydávání právních norem – zákon o elektronickém podpisu, zákon o informačních systémech veřejné správy, zákon o některých službách informační společnosti a další. I oblast trestního práva reagovala na pronikání IT do běžného života novým trestním zákonem, který obsahuje řadu skutkových podstat počítačové kriminality.

Naproti tomu některé internetové oblasti se stále neřeší, přestože jsou ve stavu, kdy by právní úprava byla žádoucí. Jinde zase právní předpis umožní postihnout závadné jednání, které ale vzhledem ke globálnímu charakteru internetu neznamená, že se ho

zbavíme. Důvodem je právě absence mezinárodní - celosvětové právní úpravy týkající se IT obecně. Jinak řečeno, měla by existovat jednotná právní norma, jíž by byly vázány všechny země. Jinak se může stát, že se kyberterorismus projeví na místech, kde nebude jeho činnost protizákonná. Už v tomto ohledu bychom měli o něm začít jednat, v zájmu budoucího vývoje celého lidstva.

Úkol do budoucna je tedy jasný, boj s kybernetickým zločinem více sjednotit a zvýšit podporu ze strany zákonodárců, neboť jednotlivé státy nemohou bojovat proti globálnímu nepříteli samy. Možná by stálo za úvahu vytvořit bezpečnostní jednotku, něco jako Interpol pro zločiny v kyberprostoru, něco podobného tomu, jako mají na Maltě - Computer forensics (Komputerová soudní věda). Svět se tam venku totiž nebezpečně rychle přibližuje tomu, který známe zatím jen ze sci-fi filmů.

Pokud se vrátím k praktické části této práce, ta jasně ukazuje, že skoro všechny děti mají dnes přístup k internetu a část jejich života se tak odehrává ve virtuálním prostředí. Považují to za přirozené a běžné. Znalosti používání PC a internetu získávají hlavně napodobováním a metodou „pokus-omyl“. Během brouzdání po síti děti narazí na mnoho webových stránek s podezřelým obsahem, při přijímaní e-mailu zase na různé druhy spamů a další. I když tuší, jak rozlišovat mezi závadným a nezávadným obsahem, existují softwarová řešení, která by se měla vhodně kombinovat s řešením psychologickým, aby byly děti na případná rizika a nebezpečí připraveny.

V prvé řadě je tedy potřeba zdůraznit zásadu internetové bezpečnosti číslo jedna: nikdy neuvádět jakékoli osobní informace, za žádných okolností detailně nevyplňovat profily na chatových webech, nepředávat heslo k vlastním profilům apod. Dále je dobré obeznámit děti s tím, jak fungují jednotlivé komunikační služby a jaké nabízejí možnosti obrany proti obtěžujícímu chování jiných uživatelů.

Rodič v tomto případě představuje jeden z hlavních zdrojů informací. Právě on by měl svého potomka seznámit s podobnými nebezpečími, měl by mu předat znalost nejrůznějších obran proti nim, především pak zdůraznit neanonymitu a dohledatelnost veškerých informací v tomto prostoru.

Na oplátku by zase dítě mělo mít možnost kdykoli si s rodičem pohovořit o problémech tohoto média. Tento fakt snad ani nelze dostatečně zdůraznit. Je však podmíněn tím, že na jedné straně bude respektován věk a individualita dítěte, na straně druhé dítě musí věřit v rodičovu orientaci a znalost tohoto prostředí. Vzájemná důvěra tedy v žádném případě nesmí chybět. Děti totiž dokážou své aktivity před rodiči skrývat a ti pak mají často pocit, že ví, co jejich dítě dělá. Ony samotné nevnímají nebezpečí

hrozící na internetu a uvádějí ho často jako zdroj svých informací, aniž by si ověřily jejich pravost. Na základě sesbíraných dat jsem usoudil, že o této problematice se v rodinách ví, ale situace se často podceňuje a bagatelizuje. Pro rodiče by mělo být alarmující už to, když dítě tráví převážnou část svého volného času na internetu, zhoršuje se jeho chování v rámci rodinných vztahů, zhoršuje se jeho školní prospěch, vzrůstá agresivita, své kamarády a koníčky vymění za přátele na webu, odmítá opouštět svůj pokoj a jezdit kamkoli, kde není připojení. V konečném důsledku to totiž pro dítě znamená problémy v budoucím soukromém a profesním životě. Pokud chceme mít ve věcech internetu před dětmi autoritu, musíme internet sami dobře a bezpečně ovládat.

RESUMÉ

Ve své bakalářské práci jsem se věnoval problematice kybernetické kriminality v souvislosti s využitím internetového média. O tom, že žijeme v informační společnosti, asi nikdo nepochybuje. Dokonce se dá říct, že žijeme ve společnosti postinformační, neboť od prostého zpracování informací směřujeme k práci se znalostmi. Je otázkou, jaký přínos to má pro budoucnost. To, že si každý z nás může najít informace na internetu, je sice pěkné, ale má to i neblahý vliv na samotnou psychiku člověka a především dětí. Řekl bych, že právě jim stačí najít jakoukoliv informaci, myšlenku na internetu, ale už nedovedou posoudit do jaké míry je relevantní. Kam tedy směřuje posun v této oblasti? A co bezpečnost samotného lidstva? Vždyť všechny ty krádeže, kyberšikana, vyhrožování, elektronické útoky spíše ubližují a decimují samotnou podstatu lidského bytí. Z mé bakalářské práce vyplývá, že do problematiky kybernality zasahují i společenské vědy, jako je sociologie, psychologie a právní věda. Právě v těchto oblastech dochází k velmi významným zjištěním, souvisejícím se změnami lidského chování a jeho promítání do právního pořádku.

Neustále skloňovaná bezpečnost a styl života dnešní společnosti, která „žije na webu“, hackeři v některých částech světa považovaní za patrioty, sofistikované útoky na různé systémy mi přišly nanejvýš aktuální a přivedly mě k napsání této práce. Rozdělil jsem ji na dvě části - teoretickou a praktickou.

V teoretické části jsem se zaobíral otázkami typu komunikace a informace ve spojení s informačními technologiemi, postavení internetu ve společnosti, trendy a problémy kybernality, nelegální aktivity, funkce a mechanismy útoků, co se skrývá za

nebezpečností kyberprostoru – virtuálního světa, děti a internet, hrozící následky a postihy za nepatřičné jednání dle trestního řádu.

V praktické části jsem provedl empirický výzkum týkající se přístupu mládeže k internetu, místa a frekvence připojení (z domova, ze školy, odjinud), chování v oblasti využití a aktivit tohoto média (používané služby), druhy komunikace (chaty, fóra, komunity), rizikové činnosti, stanovení pravidel pro práci na internetu – jejich dodržování, zajištění doma i ve škole.

Závěrem bakalářské práce bych ještě připomenul, že v současnosti spatřuji navíc nebezpečí ve světové ekonomické a finanční krizi, neboť připravila o práci plno kvalitních IT specialistů s rodinami a hypotékou. Ti, protože dobře znají tyto systémy, častou přejdou pracovat na druhou stranu.

ANOTACE

Kybernetická kriminalita – zkáza přichází z webu

Bakalářská práce se věnuje problematice kyberprostoru jako nejefektivnějšího komunikačního a informačního prostředku. Zabývá se výhodami i riziky tohoto fenoménu, zaměřuje se na kyberkriminalitu, definuje hlavní problémy, trendy, hrozby, nelegální aktivity, problémy policie, justice, společnosti i bezpečnosti. Dále popisuje kyberkriminalitu v souvislosti s mladší populací - jakému nebezpečí se dobrovolně vystavují, jaké jim hrozí následky a postihy za jejich jednání. Jedním z cílů této práce je připomenout, že klíčové a rozhodující zůstávají dobré vztahy a kvalitní komunikace v rodině.

KLÍČOVÁ SLOVA

Komunikace, informace, informační technologie, kyberprostor, sociální sítě, kyberkriminalita, hrozby, rizika, legislativa, ekonomika, hacking, cracking, spamming, cyberstalking, identita a anonimita, pornografie, extremismus – agresivita, závislost.

ANNOTATION

The Bachelor work deals with the problems of cyberspace as the most effective means of communication and inforamtion . It deals with the advantages and risks of this phenomenon and concentrate on the cybernatic criminality, defines the main problems such as trends, threats, illegal activity, problems the police, justice, society, and security. It also describes cyber-crime in connection with the younger population - what danger voluntarily expose themselves or what they face the consequences and penalties for their actions. One of the objectives of this work is also noted that the key and decisive remain good relations and good communication in the family.

KEYWORDS

Communication, information, information technology, cyberspace, social networking, cybercrime, threats, risks, legislation, underground economy, hacking, cracking, spamming, cyberstalking, identity and anonimita, pornography, extremism - aggression, dependency.

Seznam použité literatury - prameny

Zákony

- *Zákon č. 40/2009 Sb., Trestní zákoník*
- *Zákon č. 140/1961 Sb., Trestní zákon*
- *Zákon č.513/1991 Sb. ,Obchodní zákoník,*
- *Zákon č.40/1995 Sb., Zákon o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb. o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů*
- *Zákon č. 480/2004 Sb., Zákon o některých službách informační společnosti a o změně některých zákonů*
- *Zákon č. 398/2006 Sb., Úplné znění zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), jak vyplývá z pozdějších změn*

Literatura

CRAIG, P., BURNETT,M. *Softwarové pirátství bez záhad.* Praha Grada Publisching, a.s., 2008, s. 224, ISBN: 978-80-247-1765-4

ČERMÁK, J. *Internet a autorské právo.* Linde Praha, 2003, s. 252, ISBN: 80-7201-423-4

ČERMÁK, M. *Nikomu to neříkejte.* Extra Media, 2008, s. 88, ISBN: 978-80-903994-6-4

DIVÍNOVÁ, R. *Cybersex - forma internetové komunikace.* Triton, 2005, s. 168, ISBN: 80-7254-636-8

GOLDSMITH, J. WU, T. *Kdo řídí internet.* Argo, Dokořán, 2008, s. 230, ISBN: 978-80-7363-184-0

GREGUŠOVÁ, D., MORAVČÍKOVÁ, A., SUSKO, B. *Vybrané Kapitoly z právnej informatiky.* Bratislava: Právnická fakulta UK, 2000, s. 109, ISBN: 80-7160-144-6

GREGUŠOVÁ, D. *Počítačové právo.* A.G.A, Brno, 2002, s. 227,
ISBN: 80-86629-04-X

GŘIVNA, T., POLČÁK, R. *Kyberkriminalita a právo.* Praha: Auditorium, 2008, s. 220,
ISBN: 978-80-903786-7-4

JIROVSKÝ, V. *Kybernetická Kriminalita.* Praha: Grada Publisching, a.s., 2007, s. 520,
ISBN: 978-80-247-1561

LESSIG, L. *Free culture.* NEW YORK: The penguin press, 2004, s. 352,

MATĚJKA, M. *Počítačová kriminalita.* Computer Press, 2002, s. 106,
ISBN: 80–7226–419–2

SCAMBRAY, J., MCCLURE, S., KURTZ, G. *Hacking bez tajemství.* Computer Press, 2002, s. 620, ISBN: 80-7226-644-6

SUNN, F. *Internet - Šelma z Apokalypsy?* Eugenika, 2003, s. 127,
ISBN: 80-89115-10-1

TELEC, I. *Tvůrčí práva duševního vlastnictví.* Brno: Doplněk, 1994, s. 346,
ISBN: 80-85765-11-X

Odborné časopisy

BERÁNEK, J. Konec naivity. Internet si vzaly do parády kybermafie. In HN, 19.08.2009, s. 14-15

HRUŠKA, B. *Ami, go home.* In Ekonom, č.20 2009, s. 22

HUTAR, Z. *...e-Vánoce, přicházejí.* In ICTrevue, 2009, s.30-31, HN-028618

NYGRÝN, P. *Česko rozebrané na procenta.* In Computer, č.8 2009, s. 59

PUŽMANOVÁ, R. *Nové internety, Evropa a my.* In ICTrevue, 2009, s.20-22, HN-031279

PETERKA, J. *Stát a internet: Velký bratr byl břídil.* In ICTrevue, 2009, s.34-37, HN-029756

PIKORA, A. *Útoky proti bankám neustanou.* In Computer, č.4 2009, s.14

ŘEHOŘ, M. *Škodlivý kód, skvělý zdroj příjmů.* In Computer, č.4 2009, s.15

SLÁMA,D., BOČEK, M. *Mýty a pověry: rozpleťte síť autorského zákona.* In Computer, č.6 2009, s.18-21

ŠANTRŮČEK,P. *Obchod se strachem.* In ICTrevue, 2009, s.28-29. HN-028125

Internetové zdroje:

BARTOŠEK, M. (1995). *Krátce z historie Internetu.* [online],
Zdroj: http://www.ics.muni.cz/zpravodaj/articles/22.html.29 05.2009

BERÁNEK, J. (2009). *Konec naivity.* [online],
Zdroj: http://ekonomika.ihned.cz/c1-38092000-konec-naivity-internet-si-vzaly-do-parady-kybermafie. 20.08.2009

BLINKA, L. (2008), *Konference Primární prevence rizikového chování V.* [online],
Zdroj: http://www.muni.cz/research/publications/797187. 16.03.2009

BLINKA, L. (2008), *Generace závislých? Dospívající a online hry.* [online],
Zdroj: http://ivdmr.fss.muni.cz/info/storage/, 15.06.2009

BOČEK, J. (2008). *Historie počítačů I.-počítačový ptravěk.* [online],
Zdroj: http://www.extrahardware.cz/historie-pocitacu-i-pocitacovy-pravek. 15.10.2008

Časopis POLICISTA (2008). *Hacker.* [online],
Zdroj: http://web.mvcr.cz/archiv2008/casopisy/policista/2006/01/hacker.html.
15.03.2009

ČTK (2009). *Všeobecné zpravodajství.* [online],
Zdroj:
http://www.ctk.cz/sluzby/slovni_zpravodajstvi/vseobecne/index_view.php?id=373593.
01.05.2009

ČT24 (2009). *Nelegální stahování z internetu.* [online],
Zdroj: http://www.ct24.cz/media/internet/57785-kauzu-ceskych-internetovych-piratu-zacal-projednavat-soud. 10.07.2009

HRON, M. (2009). *Budoucnost Skypu je nejasná, právní spory ho možná pošlou ke dnu.* [online], Zdroj: http://mobil.idnes.cz/budoucnost-skypu-je-nejasna-pravni-spory-ho-mozna-poslou-ke-dnu-p8g-/mob_operatori.asp?c=A090804_185654_mob_operatori_hro. 10.08.2009

HYRMAN, M. (2009). *Kyberválka: Nové možnosti vedení boje v 21. století* [online],
Zdroj: http://www.zive.cz/clanky/kybervalka-nove-moznosti-vedeni-boje-ve-21-stoleti/sc-3-a-146695/default.aspx. 22.04.2009

JANSA, L. (2008). *Cybersquatting a jeho podoby.* [online],
Zdroj: http://www.pravoit.cz/article/cybersquatting-a-jeho-podoby. 15.03.2009

KAPOUN, J. (2008). *Věda a historie.* [online],Zdroj:http://businessworld.cz/veda-a-historie/historie-netscape-communications-corporation-1638. 30.09.09

KUČERA, J. (2008). *Tvůrce prvního počítače*. [online],
Zdroj: http://www.fi.muni.cz/usr/jkucera/pv109/vystavka/xnezerka_index.html.
11.07.2009

KULHAVÝ, V. (2007). *Skypování - telefonování prostřednictvím internetu.* [online], Zdroj: http://www.rozhlas.cz/vedaarchiv/technologie/_zprava/358497. 01.05.2009

LÁTAL, I. (2008). *Počítačová (informační) kriminalita a úloha policisty při jejím řešení.* [online], Zdroj: http://web.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html. 07.02.2009

NYGRÝN, P. (2009). *Historie počítačů.* [online], Zdroj: http://www.zive.cz/clanky/historie-pocitacu-od-elektronky-po-internet/sc-3-a-147343/default.aspx. 05.06.2009

NYKODÝMOVÁ, H. (2006). Botnety: n*ová internetová hrozba.* [online], Zdroj: http://www.lupa.cz/clanky/botnety-internetova-hrozba. 15.03.2009

OTEVŘEL, P. (2006). *Spamming a některé otázky šíření obchodních sdělení.* [online], Zdroj: http://www.pravoit.cz/article/spamming-a-nektere-otazky-sireni-obchodnich-sdeleni. 12.07.2009

PAUKERTOVÁ, V.(2006). *Elektronická informační kriminalita.* [online], Zdroj: http://www.ikaros.cz/elektronicka-informacni-kriminalita. 30.09.2009

PETRŽELKA, J.(2009). *Antika.* [online], Zdroj: http://www.phil.muni.cz/fil/antika. 11.07.2009

SLUNECNICE.CZ, (2009), *Bezpečnost dětí.* [online], Zdroj: http://www.slunecnice.cz/special/bezpecnost-deti/. 01.10.2009

SMEJAKL, V. (2004). *Normativní systémy a Internet.* [online], Zdroj: http://www.znalci.cz/cs/documents/articles/. 03.09.2009

SMEJKAL, V. (2003). *Specifické rysy kybernetických kriminálních aktivit.* [online], Zdroj: http://www.znalci.cz/files/PDF/Kyberprostor_2003.pdf. 05.04.2009

SMEJKAL, V. (2002), *Je Internet kriminogenní ?,* [online],
Zdroj: http://www.rodiny.cz/07/?IdPage=6. 16.03.2009

TECHNET.CZ, (2009), *Děti na internetu nejčastěji hledají youtube, google, facebook i porno.* . [online], Zdroj: http://technet.idnes.cz/deti-na-internetu-nejcasteji-hledaji-youtube-google-facebook-i-porno-1ir-/sw_internet.asp?c=A090811_193046_sw_internet_vse

VELINSKÝ, F., HADRAVOVI, A. a P. (2009). *Mechanismus z Antikithéry.* [online], Zdroj: http://www.rozhlas.cz/planetarium/historie/_zprava/629835. 30.08.2009

WERNER, L. (2009). *Kvůli Facebooku se propouští*. [online],
Zdroj: http://www.tyden.cz/rubriky/domaci/kvuli-facebooku-se-propousti-uz-i-v-cesku_129484.html. 24.07.2009

ZANDL, P. (2009) *Internetový provoz.* [online],
Zdroj: http://www.lupa.cz/zpravicky/internetovy-provoz-se-do-roku-2013-zvysi-4x. 14.07.2009

ZANDL, P. (2009) *Internet věcí.* [online], Zdroj: http://www.lupa.cz/clanky/internet-veci-internet-of-things/. 05.06.2009

http://www.dsm.tate.cz
http://www.microsoft.czom/cze/presspass/msg/20070917_news1.mpsx
http://www.gartner.com/technology/home.jsp
http://checkfacebook.com
http://www.frontex.europa.eu
http://www.eurojust.europa.eu
http://europol.europa.eu
http://cms.e-bezpeci.cz/
http://mobil.idnes.cz
http: //www.mediafax.cz
http://www.mvcr.cz
http:// eu2009.cz

http://www.bsa.org
http://www.blisty.cz/2009/5/29/art47090.html
http://thepiratebay.org
http://data.idnes.cz/soubory/prk-fakta/A080313_R00_BEZPECNOSTNI_STRATEGIE_CR.pdf
http://cpufilm.cz
http://cms.e-bezpeci.cz
http://www.play.cz/temata/rozsudek-nad-zakladateli-pirate-bay-padousi-nebo-hrdinove
http://www.park.cz/role_statu_na_ceste_k_informacni_spolecnosti
http://www.dsl.cz/clanky-dsl/clanek-870/P2P-site-bojuji,-jak-se-da
http://www.gartner.com/technology/home.jsp
http://www.stopnasilinadetech.cz/o-kampani
http://cms.e-bezpeci.cz/content/view/36/39/lang,czech/
http://www.socioweb.cz/index.php?disp=teorie&shw=274&lst=114
http://www.stoplus.cz/archiv/zavislost.html
http://www.internethelpline.cz/deti/pokladnice/problemy
http://www.iinfo.cz/vyhledavani/?qs=statistiky&diac=1&sort=0
http://www.lupa.cz/clanky/botnety-internetova-hrozba/
http://www.itbiz.cz/sniffing-odposlech-datove-komunikace
http://www.lupa.cz/clanky/botnety-internetova-hrozba/

Seznam příloh:

Příloha č. 1.: Slovníček pojmů

č. 2: Oskenovaný anonymní dotazník

Příloha č. 1: Slovníček pojmů

SLOVNÍČEK POJMŮ

Adware – za uživatelova vědomí, se do počítače dostává různá reklama. Oproti spyware je rozdíl v prováděných úkonech a škodlivosti. Nedochází ke sledování, naopak k otravování.

Bootnet – běžné uživatelské stanice, připojené do internetu, jejich počet může dosahovat několik desítek či stovek. Jejich výkon je tak srovnatelný s obrovským superpočítačem. Díky celosvětovému rozmístění s ním nelze bojovat konzervativním způsobem. Bootnety se v současné době soustředí na rozesílání spamu.

CCTV kamery – umožňují snímání - záznam obrazu v místě sledovaného prostoru, jeho přenos a zobrazení do stanoviště obsluhy bezpečnostního kamerového systému (dohledové centrum). Záznam je nejčastěji využíván ke zkoumání rizikových situací, případně plní roli důkazního materiálu.

DOS (Denial of service) – odmítnutí služby, útoky které se snaží znepřístupnit určitou službu, počítač, nebo dokonce síť.

Firewall – program, který staví mezi počítač a internet chytrou překážku; zabraňuje průniku útočníka do lokální sítě nebo počítače.

Gartner Inc. – konzultační a analytická společnost působící v oblasti ICT. (dříve Gartner Group).

HTCIA – High Technology Crime Investigation Association – specializované pracoviště, které poskytuje podporu, informace, metody, postupy a techniky vztahující se k vyšetřování pomocí pokročilých technologií. (http://www.htcia.org/)

Gartner Inc. – konzultační a analytická společnost působící v oblasti ICT. (dříve Gartner Group).

ISP- Internet service provider – tak označujeme zprostředkovatele připojení k internetu, které je realizováno různými technologiemi. Uživatelé se někdy spojují do skupin, aby ušetřili náklady nebo naopak dosáhli na dražší a rychlejší připojení.

Malware – vznikl složením anglických slov „malicious“ (zákeřný) a „software“ Souhrnný výraze pro jakýkoliv škodlivý program. Pojem zahrnuje počítačové viry, adware, spyware, červy, trojské koně a další.

P2P (Peer to peer) – počítačové sítě, ve kterých spolu komunikují samotní uživatelé, navzájem si mezi sebou vyměňují data s prakticky nulovou odpovědností. Často zneužíváno k nelegálním činnostem.

POP server – poštovní server pro přijímání a odesílání e-mailů.

Proxy server (zástupný server) – program určený pro zpřístupnění internetových služeb z lokální sítě chráněné Firewallem.

RFC – request for comments (žádost o komentáře) - používá se pro označení dokumentů popisujících internetové protokoly, systémy apod. Oficiálně jsou považovány spíše za doporučení než normy.

SANS Institute – System Administration, Networking, and Security- výzkumná a vzdělávací organizace v oblasti počítačové bezpečnosti, založení roku 1989 v USA

Skype – program, který slouží k textové, hlasové i obrazové komunikaci. Celkem ho využívá přes 480 mil. lidí, 40 milionů z nich pak denně. Odhaduje se, že přes něj směřuje až 8 % mezinárodní hlasové komunikace. Program je dostupný také na více jak 50 mobilních telefonech a herních konzolách.

Spyware – program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele.

TopSite server neboli „scénový server“ – je zjednodušeně řečeno počáteční distribuční stanice, na kterou jsou umísťovány nové, obvykle předpremiérové a novinkové tituly, které teprve odtud prosakují do rozličných výměnných sítí, kde si je následně stahují statisíce uživatelů přímo do svých osobních počítačů. Jedná se o FTP server s obrovským datovým prostorem umístěný na velmi rychlém páteřním připojení k internetu.

Underground – anglické slovo podzemí, u nás používáno v přeneseném významu, místo kde se odehrávají jevy nacházející se mimo všeobecně přijímané zvyklosti.

WEB server – prostor pro webovou prezentaci.

Wi-Fi – zajišťuje vzájemné bezdrátové propojení přenosných zařízení a dále jejich připojování do sítě internet.

Příloha č. 2: Oskenovaný anonymní dotazník

DOTAZNÍK

(DOTAZNÍK JE ANONYMNÍ, PROSÍM O PRAVDIVÉ VYPLNĚNÍ ÚDAJŮ)

VĚK : [12]

POHLAVÍ :

Holka [X] Kluk [ ]

POČET HODIN STRÁVENÝCH NA INTERNETU :

všední den (Po-Pá)

1 hod. [X] 2 hod. [ ] 3 hod. [ ]

více jak 4 hod. [ ]

víkend (So-Ne)

1 hod. [X] 2 hod. [ ] 3 hod. [ ]

více jak 4 hod. [ ]

JAKÉ VYUŽÍVÁŠ INTERNETOVÉ SLUŽBY :

e-mail - elektronická pošta [X]
chat, diskusní skupiny [X]
hledání informací, kontaktů [ ]
služby okamžité komunikace ICQ, SKYPE, MSN [X]
hraní her na Internetu [ ]
stahování her [ ]
poslouchání hudby přes Internet [X]
stahování hudby [X]
sledování filmů/ videa přes Internet [X]
stahování filmů/ videa přes Internet [X]
vyhledávání, nákup zboží, služeb [ ]
stahování software [ ]
tvorba vlastních webových stránek [ ]

CO DĚLÁŠ NA INTERNETU :

posílám svoje fotky, videa na Internet [X]
sděluji svoje osobní údaje na Internetu (věk, mobil, adresa) [ ]
otvírám přílohy, které přišly z neznámé adresy [ ]
odpovídám a přeposílám vulgární e-maily [X]
navštěvuji stránky, kde je násilí a extremismus [ ]
navštěvuji stránky s erotickým a podobně zaměřeným obsahem [ ]
sjednávám si schůzky s neznámými lidmi po Internetu [ ]
neříkám rodičů o tom co na internetu dělám [X]

KDE SE NEJČASTĚJI K INTERNETU PŘIPOJUJEŠ :

- doma [x]
- ve škole [x]
- v knihovně [ ]
- na veřeném místě (Internet. kavárny, restaurace) [ ]
- u kamárada [x]
- kdekoliv mobilně [ ]

JAK ČASTO SE K INTERNETU PŘIPOJUJEŠ :

- nikdy [ ]
- méně často [ ]
- 1 x za týden [ ]
- 2 - 3 x za týden [x]
- skoro denně [ ]
- denně [ ]
- vícekrát denně [ ]

UMÍSTĚNÍ POČÍTAČE NA KTERÉM PRACUJEŠ

- dětský pokoj [ ]
- společné prostory (obývací pokoj, jídelna, chodba) [x]
- jiné prostory [ ]

JAKÁ MÁŠ OD RODIČŮ STANOVENA PRAVIDLA PRO POUŽÍVÁNÍ INTERNETU :

- na Internetu mohu být jen omezenou dobu [ ]
- na Internet mohu jen v určitý čas [ ]
- nesmí navštěvovat určitý typ stránek [ ]
- nesmím nikde uvádět svoje osobní údaje (věk, telefon, adresu, foto) [ ]
- nesmím dělat některé věci (instalaci programů, stahování souborů a další) [ ]
- nemám stanovena žádná pravidla [x]

DODRŽUJEŠ STANOVENÁ PRAVIDLA DOMA:

ANO [ ] NE [x]

JAKÁ JSOU PRAVIDLA PRO POUŽÍVÁNÍ INTERNETU VE ŠKOLE :

- na Internetu mohu být jen omezenou dobu [ ]
- na Internet mohu jen v určitý čas [x]
- nesmí navštěvovat určitý typ stránek [x]
- nesmím nikde uvádět svoje osobní údaje (věk, telefon, adresu, foto) [x]
- nesmím dělat některé věci (instalaci programů, stahování souborů a další) [x]
- nemám stanovena žádná pravidla [ ]

DODRŽUJEŠ STANOVENÁ PRAVIDLA VE ŠKOLE:

ANO [x] NE [ ]

MÁTE DOMA NAINSTALOVANÝ PROGRAM - FILTR PRO BLOKOVÁNÍ NĚKTERÝCH WEBOVÝCH STRÁNEK NEBO NEVYŽÁDANÉ POŠTY :

ANO ☐ NE ☒

S KÝM KOMUNIKUJEŠ PŘES INTERNET :

spolužáci	☒
kamarádi, které osobně znám	☒
členové rodiny	☒
učitelé	☐
lidé mimo místo bydliště, které ale znám osobně	☒
přátelé, se kterými jsem ztratil(a) kontakt a jsem s nimi ve spojení pouze přes Internet	☒
lidé, které jsem viděl 1 - 2 x	☒
neznámí lidé (i ti kteří mě oslovili sami)	☒
virtuální lidé	☐
lidé, kteří mi byli doporučeni, ale nikdy jsem je neviděl	☒

JAK ČASTO VYUŽÍVÁŠ INTERNETOVÉ SLUŽBY

WEB, BROUZDÁNÍ

nikdy	☐	méně často	☐	1 x za týden	☐
2 - 3 x za týden	☐	denně	☐	vícekrát denně	☒

SOCIÁLNÍ SÍTĚ (FaceBook, Líbímseti)

nikdy	☐	méně často	☐	1 x za týden	☐
2 - 3 x za týden	☐	denně	☐	vícekrát denně	☒

E-MAIL, OUTLOK

nikdy	☐	méně často	☐	1 x za týden	☐
2 - 3 x za týden	☐	denně	☐	vícekrát denně	☒

SDÍLENÉ SÍTĚ P2P

nikdy	☒	méně často	☐	1 x za týden	☐
2 - 3 x za týden	☐	denně	☐	vícekrát denně	☐

CHAT - SKYPE, ICQ

nikdy	☐	méně často	☐	1 x za týden	☐
2 - 3 x za týden	☐	denně	☐	vícekrát denně	☒