UNIVERZITA KARLOVA V PRAZE

FAKULTA FILOZOFICKÁ

Ústav informačních studií a knihovnictví

Studijní program: informační studia a knihovnictví
Studijní obor: informační studia a knihovnictví

Martin Kubelka

Sociální a technologické aspekty informací a jejich komunikace, dopad těchto informací na člověka.

Bakalářská práce

Praha 2009

Vedoucí bakalářské práce: **Doc. PhDr. Vladimír Smetáček, CSc.**

Oponent bakalářské práce:

Datum obhajoby:

Hodnocení:

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a že jsem uvedl všechny použité informační zdroje.

V Praze 24. května 2009

Martin Kubelka

Bibliografický záznam

KUBELKA, Martin. *Sociální a technologické aspekty informací a jejich komunikace, dopad těchto informací na člověka. [Social and technologic aspects of the information and their communication, influence of these information to the people.]* Praha, 2009. 50 s. Bakalářská práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí diplomové práce Doc. PhDr. Vladimír Smetáček, CSc.

Abstrakt

Práce si klade za úkol popsat vliv výpočetní techniky, zejména pak moderních technologií komunikace, na člověka, a to jak z pohledu technologického (technického), tak sociologického. V práci budou zmíněny jak pozitivní dopady spojené zejména s větší otevřeností a snadnější dostupností informací, tak i dopady zcela záporné související především se zneužitím komunikace, neoprávněným užití informací a ilegální činností v této oblasti. Mimo jiné se práce zaměří na překážky, zneužití a svobodu komunikace, problémy v komunikaci a šíření informací (dezinformací) spojené se zdánlivou anonymitou prostředí Internetu, jakožto hlavního komunikačního média současnosti.

Abstract

This work wants to describe the influence of computers, especially modern communication technologies on people from technological and sociological perspective. There will be involved positive influences connected with openness and accessibility of the information even negative influences connected with information abuse and illegal manners in information area. This paper will be aimed on communication problems, communication abuse and illegal use of information, freedom of communication and dissemination of the disinformation connected with anonymous environment of the Internet.

Klíčová slova

Informace, komunikace, technologie, zneužití, sociální aspekty, informační chování, sociální sítě, počítačová kriminalita, osobní údaje, hacking, svoboda

Key words

Information, communication, technology, misusage, social aspects, information behavior, social network, computer crime, private information, hacking, freedom

PŘEDMLUVA

Tato bakalářská práce si bere za úkol co nejlépe shrnout a globálně popsat problematiku komunikace informací v prostředí elektronických médií, zejména pak internetu, a analyzovat dopad těchto informací na člověka. Zahrnut bude pohled na rizika chování uživatelů v „pustém“ a zdánlivě anonymním elektronickém prostředí a důsledky tohoto chování v reálném světě (právní dopady, ekonomické dopady, sociální dopady atd. …). Za tímto účelem bude provedena bibliografická rešerše v odborných databázích informační vědy (např. LISA, LISTA), počítačové vědy, technologických databázích a ostatních zdrojích zabývajících se tématikou komunikace informací. Okrajově budou použity též zdroje z oblasti sociálních věd a práva.

Na celou problematiku i na jednotlivé kapitoly bakalářské práce bych se chtěl podívat z několika odlišných pohledů, za účelem vytvoření ne zcela běžného „průniku“ do tohoto velice zajímavého tématu. Rád bych se soustředil zejména na oblast svobody uživatelů v cyberprostoru reprezentovaného Internetem, zneužití informací (z několika různých pohledů), ať už v podobě porušování práva, neoprávněného získání osobních údajů, zahrnutí uživatelů nežádoucími (nechtěnými) informacemi a v neposlední řadě bych nerad opomenul velmi aktuální problém dnešní doby a to hacking a cyberterorizmus, jakožto globální celosvětovou hrozbu. Celá práce bude členěna a organizována dle těchto jednotlivých oblastí, které budou rozděleny do příslušných kapitol.

Bakalářská práce bude zpracována v rozsahu cca 40 normostran dle platných požadavků na rozsah bakalářských prací na Ústavu informačních studií a knihovnictví, za použití co možná nejrelevantnějších zdrojů dostupných k tomuto tématu, řádně odcitovaných dle platných norem ISO 690 a ISO 690-2.

- ISO 690:1987. *Documentation – Bibliographic references – Content, form and structure.* 2nd ed. Geneva : ISO, 1987. 11 s. Výtah textu normy dostupný také z WWW: <http://www.collectionscanada.gc.ca/iso/tc46sc9/standard/690-1e.htm>.

- ISO 690-2:1997. *Information and documentation – Bibliographic references – Part 2: Electronic documents or parts thereof.* 1st ed. Geneva : ISO, 1997. 18s. Výtah textu normy dostupný také z WWW: <http://www.collectionscanada.gc.ca/iso/tc46sc9/standard/690-2e.htm>.

Poděkování

Na tomto místě bych rád poděkoval všem, kteří mě při psaní této práce jakkoli podpořili ať již svojí trpělivostí, tak svými cennými radami a připomínkami. Především bych rád poděkoval svojí rodině a nejbližším za zázemí, bez kterého by tato práce nikdy nemohla vzniknout a v neposlední řadě také mému vedoucímu práce za nespočet otázek, kterými mě přivedl na mnoho zajímavých myšlenek a cest pohledu na věc.

Definice a základní pojmy problematiky komunikace informací

Informace

Abychom mohli začít uvažovat o problematice komunikace informací, musíme si nejdříve jasně definovat pár základních pojmů přímo se vyskytujících v této bakalářské práci. Jako příručka nám poslouží terminologická databáze knihovnictví a informační vědy, která v nejobecnějším slova smyslu informaci chápe jako údaj o reálném prostředí, o jeho stavu a procesech v něm probíhajících. Informace snižuje nebo odstraňuje neurčitost systému (např. příjemce informace); množství informace je dáno rozdílem mezi stavem neurčitosti systému (entropie), kterou měl systém před přijetím informace a stavem neurčitosti, která se přijetím informace odstranila. V tomto smyslu může být informace považována jak za vlastnost organizované hmoty vyjadřující její hloubkovou strukturu (varietu), tak za produkt poznání fixovaný ve znakové podobě v informačních nosičích. V informační vědě a knihovnictví se informací rozumí především sdělení, komunikovatelný poznatek, který má význam pro příjemce nebo údaj usnadňující volbu mezi alternativními rozhodovacími možnostmi. Významné pro informační vědu je také pojetí informace jako psychofyziologického jevu a procesu, tedy jako součásti lidského vědomí. V exaktní vědě se např. za informaci považuje sdělení, které vyhovuje přísným kriteriím logiky či příslušné vědy. V ekonomické vědě se informací rozumí sdělení, jehož výsledkem může být zisk nebo užitek. V oblasti výpočetní techniky se za informaci považuje kvantitativní vyjádření obsahu zprávy. Za jednotku informace se ve výpočetní technice považuje rozhodnutí mezi dvěma alternativami (0, 1) a vyjadřuje se jednotkou nazvanou bit. (KTD, Informace)

Komunikace

Stejně tak můžeme v databázi knihovnictví a informační vědy najít velice srozumitelnou definici komunikace, jakožto každá reakce organismu na vnější podnět. V užším slova smyslu se za komunikaci považuje proces interakce, při němž si partneři komunikace (lidé, počítače) vyměňují informace. Komunikace má

obvykle následující strukturu: mluvčí (komunikátor) -> záměr sdělení -> formulace sdělení -> vlastní sdělení -> příjemce sdělení (komunikant) -> interpretace sdělení a záměru mluvčího -> reakce příjemce sdělení (komunikanta). Podle druhu nosiče se rozlišuje komunikace znaková (řeč, písmo) a neznaková (gesta, intonace hlasu apod.). Podle míry bezprostřednosti se člení komunikace na formální a neformální. Ze sociologického hlediska se rozlišuje komunikace interpersonální a skupinová, podle způsobu percepce vizuální, auditivní a audiovizuální. (KTD, Komunikace)

Uživatel

Pro potřebu této práce si též definujme „uživatele“, jakožto osobu využívající jakýkoli informační systém (technický, technologický), pro náš případ převážně v elektronické podobě, za účelem komunikace informací, jejich předání, získání, archivování. A to z jakéhokoli důvodu (osobní, zájmové, zábavní, pracovní, edukační). Tohoto uživatele není dále potřeba definovat například věkem, pohlavím nebo mírou zkušeností práce v informačním prostředí, protože v jednotlivých oddílech budou specifikována rizika, která mohou čekat jen na některé skupiny uživatelů nebo naopak rizika globální.

Digitální prostředí - Internet

Dále si musíme jasně definovat oblast, kterou se tato bakalářská práce zabývá a to je digitální prostředí, zejména pak prostředí internetu, které je definováno jako globální síť vzájemně propojených počítačů, umožňující uživatelům sdílet informace prostřednictvím mnoha různých informačních kanálů. Obvykle počítač připojený do internetu má přístup k informacím umístěných v obrovském poli serverů rozmístěných po celém světě, tím že tyto informace přemísťuje z jejich úložiště do svojí lokální paměti. V současnosti se jedná nejvíce o vzájemně propojené hypertextové dokumenty v prostředí World Wide Web - WWW. Počítačoví uživatelé tyto informace získávají prostřednictvím internetového prohlížeče (tj. programu interpretujícího digitální data uživateli do jemu srozumitelné podoby). Dále pak jako hlavní nositele informací můžeme považovat emailové klienty (programy umožňující zasílání elektronické pošty včetně multimediálních příloh), online chatovací programy (komunikace – dopisování si

v reálném čase) a programy na sdílení a přenos digitálních dokumentů (file sharing and file transfer programs). Technicky přenos dat po síti internet probíhá za pomoci standardizovaných protokolů přenášejících datové packety, zejména pak pomocí protokolů rodiny TCP/IP (více v kapitole 1.4.2). Tato síť se skládá z milionů menších soukromých, veřejných, akademických, obchodních a státních sítí, vzájemně propojených měděnými a optickými kabely případně za použití bezdrátových přenosových technologií. (Wikipedia, Internet)

Historie Internetu

Ačkoli se za místo vzniku internetu povětšinou bere USA, tak první podobný projekt začal být uskutečňován již začátkem 60. let ve Velké Británii. Jednalo se o 1. pokusnou síť nainstalovanou počátkem roku 1968 v Národní fyzikální laboratoři. Avšak plně funkční síť byla uvedena do provozu až v roce 1969 v USA národní vojenskou agenturou DARPA (Defense Advanced Research Project Agency) jako společný projekt s universitami zabývajícími touto tématikou. Název této sítě byl ARPANET a propojovala 4 základní internetová sídla (uzly) a to na Univerzitě v Utahu, University of California v Santa Barbaře, University of California v Los Angeles a Stanfordském výzkumném institutu. Přenosová rychlost byla na tehdejší dobu úžasných 50kb/s, což naprosto postačovalo potřebě komunikace převážně textové podoby. V této době síť sloužila převážně k armádním a studijním účelům. Rozvoj této sítě byl v následných letech dosti strmý, za další 3 roky už síť čítala bezmála 20 uzlů a v roce 1985 se už mohla chlubit více než 1200 uzly. Základní principy internetu zde byly už zcela patrné a dochovaly se až do dnešní doby (rovnost v síti, žádný centrální prvek - rovnocennost uzlů). V Evropě se první počítačová síť spouští až v roce 1984 pod názvem EARN (European Academie and Research Network). Tehdejší ČSSR je zapojena do sítě EUNET až koncem roku 1988.

Postupem času bylo potřeba sjednotit komunikaci v síti a definovat základní standardy. Za tímto účelem byl vytvořen Transmission Control Protocol (TCP), na

jehož základě funguje celý internet dodnes. Ten definuje základní principy bezchybného odesílání a přijímání datových paketů (jakýchsi balíčků dat, do kterých jsou rozděleny větší objemy dat, soubory atd.…) Následně pak byl zaveden protokol IP, který řeší směrování a vedení těchto balíčků dat mezi odesílatelem a příjemcem (tzv. Routing – směrování). Protokoly rodiny TCP/IP se tak staly hlavním standardem ať již ARPANETU, tak později internetu. V roce 1983 dochází tak ke klíčové události, kdy se ARPANET rozděluje na MILNET (svojí armádní část) a ARPANET zůstává od té doby zcela civilní sítí. Tato chvíle je všeobecně uznávaná za moment vzniku Internetu. Téhož roku se ARPANET spojuje se sítí BITNET, což je další obrovská počítačová síť propojující převážně počítačové uzly v University of New York a Yale University. Tato počítačová síť později také přijímá pro svou komunikaci standardy TCP/IP a tímto umožňuje další prudký rozvoj právě se rodícího Internetu. Začátkem 90. let už mluvíme o více než 10 000 počítačů propojených v globální síti. V roce 1994 je pak uveden do praxe systém DNS (Domain Name Server). Server přidělující doménová jména, čímž značně šetří pohodlí používání sítě. Tento server se stará o překládání číselných adres (IP adres) na jejich jmennou podobu tzn., že uživatelé při komunikaci nemusí znát přesné číslo uzlu, s kterým chtějí komunikovat, toto číslo za ně DNS přeloží ze jména této domény. Začátkem 90. let též Tim Berners-Lee vynalézá hypertextově orientovaný systém sdílení informací později nazvaný WWW a spouští první WWW server ve Švýcarském institutu pro jaderný výzkum. Za pomoci všech těchto technologií zažívá Internet doslova raketový rozmach a počty počítačů připojených k internetu prudce rostou. V roce 1995 se odhaduje, že přístup k internetu má zhruba 20 milionů uživatelů, v roce 2000 už hovoříme o 300 milionech. O službu WWW se od roku 1994 stará firma WWW Consorcium (W3C), sídlící v institutu CERN a ředitelem tohoto konsorcia není nikdo jiný než již zmiňovaný Tim Bernes-Lee. Hlavním úkolem tohoto uskupení je správa všech standardů, které služba WWW využívá ke své funkčnosti.

Technická struktura internetu

Dnešní internet se technologicky dělí do jednotlivých celků (menších či větších sítí) podle jejich velikosti, rozsahu a počtu jednotlivých uzlů. Jedná se prakticky o vzájemně propojené menší

sítě. Takováto jednotlivá síť se bere jako určitý počet samostatných počítačů navzájem propojených některou z komunikačních technologií (metalické spoje, optické spoje, bezdrátové spoje). Aby samotný internet mohl dobře fungovat, musí platit základní pravidlo, že dvě na sobě nezávislé sítě spolu musí komunikovat navzájem dvěma a více linkami, aby byla zabezpečena komunikace i v případě výpadku některé z částí sítě. Technologicky je přenos dat v síti zajišťován několika základními prvky, kterými jsou speciální servery plnící funkci tzv. počítačové brány (gateway), směšovače (routery) a ostatní serverové a klientské počítače. Počítačové brány se starají o vzájemné propojování sítí různých druhů, routery pak mají za úkol směrovat jednotlivé pakety dat sítí tak, aby vždy došly v pořádku od odesílatele k příjemci za pomoci tzv. směrovacích tabulek, podle kterých snadno poznají nejkratší cestu sítí mezi dvěma komunikujícími body.

Podle velikosti se sítě rozdělují takto:

- **WAN (Wide Area Network)** Největší z jednotlivých druhů sítě. Většinou bývá členěna jako jedna „národní síť“ na území jednoho státu. Internet jako celek se pak skládá z takto propojených národních sítí jednotlivých států (pro Českou republiku je zajišťována sítí CESNET).

- **MAN (Metropolitan Area Network)** Síť pokrývající nějakou větší oblast, povětšinou město (podle toho také metropolitan). Ve své struktuře propojuje jednotlivé menší sítě. Sítě MAN jsou mezi sebou propojovány většinou vysokorychlostními optickými propojkami nebo bezdrátovými spoji zaručujícími potřebnou propustnost a rychlost sítě – tzv. páteřní linky.

- **LAN (Local Area Network)** Jedná se o jednotlivé místní sítě ve struktuře sítě MAN. Tyto menší sítě se skládají z mnoha počítačových míst (nodes), které jsou navzájem propojeny mnoha druhy komunikačních technologií (metalické spoje, optické spoje, bezdrátové spoje). Jednotlivé prvky těchto sítí jsou už konkrétní počítače, uživatelské stanice, servery plnící mnoho funkcí (od přístupu k internetu až po DNS, routing – směrování, funkci webových serverů, elektronické pošty, databázové servery apod.) a ostatní HW vybavení.

1.4. Deep vs. Surface Web

Jako další velice důležité rozdělení informačního prostoru musíme zahrnout členění z hlediska dostupnosti informací a to v tzv. povrchovém (volně dostupném) webu a tzv. hlubokém webu.

Takzvaný hluboký nebo také neviditelný, skrytý a temný web je součástí obsahu World Wide Webu, který není indexovaný běžnými vyhledavači jako tzv. povrchový web, ke kterému mají volní přístup všichni uživatelé internetu. Z tohoto pohledu bylo vyhledávání na internetu přirovnáno k jakémusi lovu na povrchu oceánu. Mnoho může být uloveno, avšak nedozírné množství obsahu se skrývá pod povrchem, příliš „hluboko“ na to aby to bylo objeveno. A stejně tak i mnoho důležitých a relevantních informací je skryto běžnému uživateli hluboko v internetové síti - ve zdrojích ke kterým nemá volný přístup. Většinou se dokonce ani o těchto informacích nedozví, protože tyto informace nejsou registrovány konvenčními vyhledavači (např. Google apod.) V roce 2000 byl obsah hlubokého webu odhadován na zhruba 7500 terabytů dat uložených v 550 miliardách jednotlivých datových souborů. V dnešní době se však rozsah hlubokého webu odhaduje již na 91 000 terabytů! Pro srovnání objem dat přístupných v povrchovém webu, snadno vyhledatelných internetovými vyhledavači, činí zhruba 167 terabytů a rozsah fondů Library of Congress v roce 1997 byl asi 3000 terabytů.

Zdroje hlubokého webu můžeme zařadit do několika základních skupin (Wikipedia, Deep Web):

- **Zdroje s dynamickým obsahem**: jejich struktura a obsah není pevně daný, je vygenerován z hledisek požadavků konkrétního uživatele. Jelikož je takováto informace proměnná, tak nemůže být indexována vyhledavači.

- **Zdroje s nepropojeným obsahem**: takovéto zdroje nemají návaznost na jakékoli jiné zdroje, jejich odkazy nejsou „prolinkované“. Takovéto zdroje jsou pro indexovací roboty prakticky neviditelné, protože jsou odmítnuty jejich vnitřními algoritmy.

- **Soukromé weby**: informační zdroje, jejichž obsah je chráněn přístupovým heslem, případně jinou formou autorizace.

- **Kontextové weby**: informační zdroje, jejichž obsah je proměnný z hlediska způsobu přístupu ke zdroji (geografická poloha, IP adresa, dřívější navigační postup k tomuto zdroji).

- **Zdroje s limitovaným přístupem**: stránky, které technicky limitují přístup ke svým zdrojům (technicky znemožněno vyhledávacím enginům indexování).

- **Skriptované stránky**: informační zdroje přístupné pouze prostřednictvím linku vygenerovaného pomocí některého dynamického skriptovacího jazyka (JavaScript, Flash, AJAX).

- **Zdroje nekompatibilní s formátem HTML**: veškeré zdroje jiného formátu nežli HTML (pro indexovací robotu nečitelné).

2. Pohled na svobodu komunikace v Internetu jakožto cyberprostoru.

Filosofie internetu v jeho počátcích

Když se v USA v 80. letech začínal rozšiřovat internet, jako pouze propojení několika vládních (armádních) a universitních počítačových sítí, byl brán jako naprosto svobodné médium bez jakékoli regulace. Na tento problém se můžeme podívat z více pohledů. Jedním z nich je jednoznačně názor, že se nejedná o problém nýbrž o hlavní devizu tohoto internetového prostředí. Tento cyberprostor bez jakékoliv regulace mohl takto fungovat do té doby, než byla prolomena určitá hranice počtu uživatelů. Ze začátku mělo k internetu možnost přístupu pouze velmi omezené množství uživatelů, převážně odborného zaměření (počítačový odborníci, profesoři, studenti). V této komunitě nebylo zapotřebí jakékoli regulace, navíc když bereme v úvahu fakt, že internet v té době sloužil jen jako komunikační médium a to komunikaci interpersonální (online chat, posílání zpráv atd.…). Vláda USA v té době štědře dotovala rozvoj tohoto média, ale ještě pořád v něm neviděla takový potenciál, zejména pak potenciál ekonomický. Do této doby byl celý internet pod vedením tzv. otců internetu, počítačových odborníků a vizionářů. Ve chvíli, kdy se začaly v tomto novém a slibně se rozvíjejícím médiu točit relativně obrovské sumy peněz (ze začátku se jednalo např. jen o zpoplatnění přidělení vlastního jména domény 2. stupně jmennou autoritou), tak se vláda Spojených států začala výrazně zajímat o kontrolu nad těmito příjmy a jako reakci na to ihned převedla tyto pravomoci na státem vlastněnou firmu zřízenou za tímto účelem. To byla ale jenom špička ledovce a příjmy, které tvořily jen zanedbatelnou částku z celkových sum, se začaly na internetu „točit“ během dalších let. Ani ne tak z pohledu ekonomického, ale spíše z pohledu filosofického a sociálního se toto chovaní nelíbilo původním zakladatelům internetu, a tak je znám případ, kdy Jon Postel, jeden z „otců internetu“ a hlavní odborná autorita v oblasti přidělování doménových jmen, jednoho dne zaslal dopis 8 z 12 společnostem starajících se o jmenný prostor s žádostí, aby nastavily jako root (hlavní/první počítač celé struktury) jeho počítač na Stanfordské univerzitě v Silicon Valley. Tímto odvážným činem tak ukázal, že jeho jméno v počítačové branži ještě pořád něco znamená, ale z důvodu obrovského

tlaku americké vlády na něj a na jeho domovskou universitu musel ustoupit a vrátit vše do původního stavu, opět pod kontrolu státní firmy. (Goldsmith, 2008, s. 60)

Sporné výklady platnosti legislativy

Původní myšlenka byla taková, že internet reprezentující globální „síť sítí“ bude jakési místo svobody nebo alespoň takto se tvářil. Toto nové médium mezilidské komunikace si od počátku svého vzniku žilo takříkajíc vlastním životem. S masivním nástupem komerce a podnikání na internetu nastala situace, kdy začalo být potřeba tento tok informací nějakým způsobem regulovat, jak již z pohledu technického, tak z pohledu právního a sociálního. V tuto chvíli vyšel na povrch problém, který do dřívější doby nikdo neřešil a to důležitost zeměpisné polohy. Mnozí internetoví odborníci této otázce zprvu nepřikládali žádný význam, protože internet byl brán způsobem, že je naprosto jedno odkud se uživatel připojí, ale problém nastal ve chvíli, kdy začaly být vedeny spory jaké zákony se mají na internet vztahovat. Je znám soudní proces mezi americkou společností Yahoo a Francouzskou vládou o to, zda-li je možné, aby americká společnost nabízela na svých stránkách zboží s nacistickými symboly. (Goldsmith, 2008, s. 21) Americká ústava tento případ nikterak nepostihuje, avšak francouzské zákony takovéto jednání tvrdě postihují, jakožto propagaci hnutí potlačujících základní lidská práva a svobody. Servery, které spravovaly tyto internetové stránky, byly sice umístěny na území Spojených států, ale jejich obsah byl přístupný všem uživatelům sítě bez výjimky. Rozsudek zněl, že společnost musí neprodleně implementovat nový systém umožňující detekci zeměpisné polohy uživatele dle jeho IP adresy (adresy počítače v internetu). Od této chvíle začaly být mezi odborníky pře o to, jaké by měly platit zákony v internetu. Dokonce padlo i několik šílených nápadů, že by měly platit právní regulace všech států, ze kterých je možné se připojit na internet. Tento opravdu zavrženíhodný plán, který kdyby byl uveden do praxe, tak by znamenal s určitostí zánik celého internetu, protože by natolik zkomplikoval jakoukoliv činnost na něm, nebyl nikdy přijat.

Důležitost fyzické geografické polohy v cyberprostoru

Tento případ ale ukázal ještě na jiné aspekty komunikace v síti. Z technologického hlediska celý internet, fungující převážně na protokolu TCP/IP, je navržen tak, aby data proudící sítí rozdělená do malých datových celků vždy dorazila od odesílatele k příjemci. (více v kapitole 1.4 o struktuře a historii internetu) Každý takovýto „balíček“ dat může ale od odesílatele ke svému příjemci putovat zcela jinou cestou. Logika věci dává jasně znát, že nejkratší cesta bude ta nejrychlejší. Z tohoto důvodu je velice důležité být schopen analyzovat polohu uživatele v síti a zvolit pro přenos dat prostředky jemu nejbližší a šetřit jak kapacitu sítě, tak uživatelův čas. Dnešní technologické řešení určování geografické polohy počítačů v internetu je založeno právě na sledování putování těchto datových balíčků v síti. Tento pohyb lze přirovnat k pohybu auta po placených úsecích dálnic, kde musí platit u jednotlivých mýtných bran. Zpětnou analýzou projetých bran lze zjistit výchozí body cesty, čili v našem případě odkud kam proudí data (Goldsmith, 2008, s. 79). I když budeme vycházet z předpokladu, že každá regulace je špatná, tak z hlediska tohoto pohledu se nejedná ani tak o regulaci, jako spíše o usměrnění datového toku (přenesené informace) za účelem zefektivnění přenosu a šetření systémových prostředků. Ve výsledku uživatel obdrží to co si přál (například si stáhne do svého počítače nějaký nový program, svou oblíbenou písničku apod.) a to, že byla zjištěna jeho poloha a byl tak technologicky omezen jeho výběr zdroje, se ani nedozví.

Z dalšího pohledu je regulace přímo žádoucí, protože v dnešní době informační přesycenosti je jednoznačné identifikování fyzické polohy uživatele zcela klíčové pro výběr informací, které na něj budou cíleny. Jedná se o tzv. personalizovaný web. Dá se jen těžko předpokládat, že by člověka připojujícího se z Prahy zajímaly ceny vstupenek na večerní zápas anglické fotbalové ligy, případně počasí nad New Yorkem. Takovýto přístup k uživateli například informačních webů s nejnovějšími zprávami je oboustranně výhodný pro obě strany. Člověk se opět může cítit regulován, protože mu nejsou nabízeny všechny informace, ale zároveň berme v úvahu, že je to stále lepší, než-li být zavalen nepřeberným množství zcela irelevantních informací, které jdou mimo všechny informační potřeby daného jedince. Z pohledu druhé strany (provozovatelé webů, firmy apod.) je tento fakt

velice důležitý z hlediska cílení reklamy a nabídky svých produktů, služeb a informací. Pro normálního člověka je věčně se objevující reklama otravná, jelikož je převážně na věci, které vůbec nechce. Jestliže může tato technologie reklamu alespoň trochu cílit, lze získat stav, který zdaleka není ideální, ale alespoň není kritický - chvíle, kdy je člověk zavalen reklamou a marně hledá obsah. Tento pocit se často dostavuje například při listování časopisy „moderního člověka“, kde již obsah naprosto pozbyl svojí roli a čtenáři spíš připadá, že si koupil hodně tlustý a drahý reklamní leták na zboží, na které stejně nebude mít nikdy dostatek prostředků.

Problematika vymahatelnosti práva v cyberprostoru mimo území svého státu/oblastního území

V průběhu času bylo i mnoho pokusů jak omezení obejít nebo se vyhnout zákonům dané země. Nejnázornějším příkladem může být tzv. „datový ráj“, místo mimo hranice působnosti legislativy státu, který se snaží komunikaci ilegálních informací (např. pornografie, rasistické weby, teroristické weby apod.) blokovat. V historii ale pokaždé takováto snaha ztroskotala, protože i když stát nemůže nikterak postihnout přímo zdroj informací, může legislativně postihovat zprostředkovatele informací na svém území. Jack Goldsmith dává příměr v levné asijské výrobě, napodobenin značkového zboží. Například Americká vláda nemůže postihnout továrny v Číně za jeho výrobu, ale může postihovat distributory tohoto zboží na svém území, čímž jeho prodej značně reguluje. (Goldsmith, 2008, s. 85) Další otázkou je pak vymahatelnost a efektivnost této represe. Například by se dala postihovat nejen distribuce ilegálních kopií zboží (jako zboží si můžeme představit značkové oblečení nebo klidně i nelegálně šířený software na internetu, hudební soubory, multimédia atd.…), ale i jeho držení. Vymahatelnost tohoto zákona by však byla natolik nákladná, že by byl ve své podstatě velice neefektivní. Konkrétně ale například americká administrativa praktikuje tvrdé represe proti různým formám podnikání na internetu (převážně v případech, kdy tratí na daních – alkohol, cigarety), tuto formu regulace vymáhá nepřímo, čili nezakročuje proti samotným prodejcům, ale různými nařízeními znemožňuje nebo znesnadňuje předmět jejich podnikání (zákaz placení elektronickými platebními kartami přes internet za tabákové výrobky a podobně. (Goldsmith, 2008, s. 96)

Pokusy o tvrdou cenzuru a omezení v Českém internetu:

Z tohoto pohledu a z mnoha dalších se zdá naprosto hrůzný návrh českých poslanců o regulaci, anebo úplném zákazu pornografie na internetu. (Peterka, 2009) Jednalo se o vsuvku do zákona **č. 202/1990 Sb., (o loteriích a jiných podobných hrách), do kterého měla být vpravena část již dříve neschváleného zákona č. 480/2004 o některých službách informační společnosti**. Konkrétně tyto body:

Provozovatel elektronických prostředků je povinen zajišťovat nemožnost připojení uživatele ke stránkám elektronických prostředků

a/ s pornografickým obsahem,

b/ nabízejícím a umožňujícím účast na loteriích a jiných podobných hrách podle zvláštního předpisu prostřednictvím sítě internet, a

c/ podporujícím jiné zakázané služby a činnosti včetně reklamy na takové služby a činnosti

Tento dodatek zákona nakonec nebyl schválen a všichni poslanci, kteří ho předkládali, od něj dali ruce pryč, ale je již zarážející, že někoho takováto regulace může vůbec napadnout.

Když si odmyslíme to, že regulace je nebezpečná již sama o sobě a budeme pracovat s představou, že pornografie je obecně špatná věc (což si někteří lidé opravdu asi myslí), tak automaticky dojdeme k několika zásadním problémům tohoto zákona. První je, kdo a jakým způsobem bude určovat co je pornografie a co už ne. Co se může jednomu člověku zdát jako vrchol nechutnosti a nevkusu, opravdu ohrožující obsah pro člověka a společnost, tak pro druhého může být velmi zajímavé umělecké dílo. Je pak velmi na zváženou jakým způsobem se určí škodlivost a komu se tato obrovská pravomoc regulace svobody uživatelů na sítí a svobody získávání informací dá do rukou. Druhá velmi sporná otázka je otázka proveditelnosti této regulace. Z hlediska dnešní technologie je možné určovat obsah na síti způsobem metadat, tagů a klíčových slov, jaké si jednotlivé typy dokumentů v sobě nesou z důvodu vyhledatelnosti. Fyzická kontrola všech nekonečně rostoucích informací na internetu je zcela nereálná, čili regulovat „škodlivý obsah“ lze pouze za použití filtrů těchto metadat. Každý poskytovatel připojení do internetu by tak musel mít nastaveny nějaké jednotné filtry obsahu, které by byly uplatněny

na všechny uživatele. Mimo to, že takovéto opatření s sebou nese nemalé náklady spojené s provozem, které poskytovatelům ve výsledku nezaplatí nikdo jiný než jejich zákazníci (vzniká tak bizarní situace, kdy člověk platí za to, aby byl „ochuzen“), tak je zřejmé, že může snadno nastat situace, kdy nějaká v reálu naprosto neškodná data ponesou znaky nevyhovující filtru a uživateli budou automaticky odepřena. (snadno si lze představit např. píseň v elektronické podobě v jejímž názvu bude slovo „sex“) Třetím a zdaleka nejzávažnějším problémem této represe je otázka „Co bude nevyhovovat příště…?“

Co je to svoboda, jsme a můžeme vůbec být svobodní?

Na úplný závěr této kapitoly si musíme položit úplně základní otázku. „Jsme svobodní na internetu?“ A co vůbec můžeme všechno chápat pod slovem „svoboda“? Doby začátku internetu jsou ty tam a počáteční doba zavádění nové technologie a anarchie spojená s tímto obdobím je už dávno za námi. V současnosti nic takového jako svoboda neexistuje. Člověk je regulován, omezován a kontrolován ve svém přístupu k informacím na každém rohu, při jakékoliv činnosti na síti. Důvodů k tomu je hned několik. Stát nastavuje laťku svými zákony. Tyto zákony pak musí provozovatelé služeb v síti plnit nebo by vystavovali sebe postihu. Za tímto účelem jsou v internetu často regulovány i informace, které ve své podstatě vůbec ilegální (škodlivé) nejsou. Provozovatel se pouze jistí, aby sám nemohl být postihnut. Váže tak uživatele k odsouhlasení milionů smluvních podmínek, které většina uživatelů zřídka kdy vůbec přečte, za vstupy pouze po registraci, autorizované služby a podobně. Všechny tyto snahy se mohou chápat jako omezení volnosti, svobody v síti a nastolení monitoringu, kontroly a umělé represe vůči jednotlivci. Tyto naprosto „nesvobodné činnosti“ může aplikovat proti uživateli mnoho různých subjektů, provozovatelem služby počínaje, státem a jeho trestními orgány konče. V této době moderních technologií si člověk (když není zrovna počítačový odborník a i za tohoto předpokladu nejspíš už ne stoprocentně) nemůže být nikdy jist zdánlivou anonymitou sítě a už vůbec ne tím, jestli není sledován nebo nejsou neoprávněně monitorována jeho osobní data nebo činnost (zájmy) na síti, které následně mohou být zneužity. Člověk by na základě všech těchto předpokladů byl a mohl se chovat svobodně pouze, kdyby mohl vystupovat anonymně a měl přístup úplně ke všem informacím. Ale všechny tyto represe a omezení vůči

uživatelům jsou často maskovány za zkvalitnění služeb, podporu většího bezpečí a podobně. Je tomu ale opravdu tak?

Když se na tuto problematiku podíváme z druhého úhlu pohledu, tak svoboda je luxus, který si asi nemůžeme, v době každodenní hrozby zločinů a terorismu, dovolit. Vždy v tomto případě platí „něco za něco“. V některých případech je prostě kontrola a omezení nutností. Ať už jde o omezení rychlosti připojení k internetu uživatelům, kteří soustavně stahují obrovské objemy dat za účelem prevence zahlcení sítě (tento problém je spíše technického rázu a ubrání tak ostatní uživatele před tím, aby na úkor někoho jiného nebyli schopni běžného užívání internetu). Nebo například monitoring a omezování podvodných obchodujících na aukčních serverech typu eBay (v ČR např. Aukro). Kdyby se totiž tyto služby chovaly pouze podle předpokladu, že lidé jsou dobří, tak sebemenší podvodníček bude moci svobodně páchat činy na úkor druhých. Budou ale ti, kdo aplikují tato omezení také čestní? A budou jimi navrhovaná opatření spolehlivá a účinná? A nebudou až zbytečně moc zasahovat do práv jednotlivců? Toto jsou všechno otázky, na které si každý může odpovědět po svém, ale každému rozumně uvažujícímu člověku vždy vyjde, že nečestní lidé a špatné nebo mylné činy se nevyhnou žádné oblasti lidské činnosti. Ve výsledku tyto represe a regulace se nemůžou odehrávat bez podložení v platných zákonech, protože bez hrozby postihu, kterou má nad jednotlivcem stát, by absolutně neměly účinek. Málokomu záleží na jeho virtuální identitě, kterou může mít každý den jinou tak jako na něm samotném v reálném světě.

Z tohoto všeho jednoznačně vychází, že svoboda ve virtuálním cyberprostoru je relativní pojem, stejně tak jako svoboda, ve které žijeme v reálném světě. Tento virtuální prostor se postupem času a celkového rozvoje a vývoje stále více diverzifikuje a to hned ze tří hlavních důvodů. Prvním důvodem jsou odlišné sociální, jazykové, kulturní a historické odlišnosti samotných národních sítí (a jejich uživatelů), ve které se Internet jako globální síť postupem času vyčlenil. Obsah těchto sítí je zaměřen na jednotlivce, kteří v tomto prostředí žijí a zájmy jsou tak z toho hlediska velmi odlišné. Druhým důvodem jsou stále se rozvíjející technologie a možnosti jejich uplatnění ze stran jak poskytovatelů připojení (technologické důvody), tak samotných států (právní důvody). Jedná se zejména o technologie

detekce geografické polohy uživatele a následné filtrování informací a upravování obsahu. Třetím důvodem jsou odlišné zákony platící na území různých států a jejich vymahatelnost v globální síti, (tento bod úzce souvisí s předchozími dvěma body) působnost těchto zákonů a odlišnost hodnot, které tyto jednotlivé legislativní regulace chrání, zastávají a uplatňují na uživatelích. (Goldsmith, 2008, s. 178) Řešením je pak najít nějaký bod rovnováhy mezi těmito vlivy a co největší svobodou pro uživatele, což ale není úkol ani v nejmenším jednoduchý. V důsledku tak internet na místo, aby sjednocoval (ať už sám sebe, tak uživatele), jak to bylo v původních vizích zakladatelů a vizionářů tohoto média, tak se čím dál tím více diverzifikuje v důsledku externích vlivů, nátlaku jak již ze strany různých zájmových skupin, tak zejména ze strany státních represí a regulací, které jsou činěné z důvodu zcela odlišných zájmů. V současnosti internet v USA není to co internet v Evropě a už vůbec ne to co internet například v Číně. Bohužel ze všech těchto předpokladů jasně vychází to, že Internet jako svobodné informační médium, jako dnešní největší virtuální prostor určený ke komunikaci informací jednoznačně končí, ba možná už skončil. Už pouze čas ukáže, kam se celý tento nekonečný virtuální prostor vyvine, případně jaká nová technologie ho postupně nahradí nebo s jakou technologií se sloučí. (příklad můžeme vidět v dnešní digitalizaci televizního vysílání, které neodvratně spěje k jedinému cíli a to sloučení se s Internetem a nabídnutí uživateli nový rozměr interaktivní zábavy)

Ještě k daleko horším následkům diverzifikace může dojít například v případě, kdyby se realizovala myšlenka implementace tzv. non-ASCII znaků v názvech domén. Jak všichni ví, tak v současnosti veškeré doménové názvy jsou ochuzeny o speciální „národní“ znaky, což se sice může zdát jako veliké omezování a pitvoření národních jazyků, ale zároveň, kdyby tomu tak nebylo, došlo by k tak rozsáhlé diverzifikaci národních internetů, že by se většina obsahu stala globálně skoro nepřístupná. Kdyby například v českých webových stránkách byly umožněny čárky a háčky, tak první následek, který to ponese, bude takový, že všichni majitelé již existujících názvů domén bez diakritiky by si museli zakoupit ještě všechny ostatní možnosti zapsání svého názvu domény, protože jinak by se uživatel při nesprávném zapsání na jejich internetovou službu nedostal. Mohlo by tak docházet k obrovským spekulacím s doménovými názvy zavedených firem, jejichž obsah je velice žádaný. Tento černý trh internetových spekulantů a vyděračů funguje již

dnes, ale po zavedení non-ASCII znaků by mohl nabýt zrůdných rozměrů. Dalším a snad ještě závažnějším problémem by byla transkripce doménových názvů z různých druhů písma do latinky, kdy by mohlo docházet k mnoha chybám a nechtěným přesměrováním. Zároveň by se pro většinu „západních“ států stal například ruský nebo japonský web naprosto nepřístupný, už jen proto, že na svojí klávesnici nemáme patřičná písmenka, pro zapsání odpovídajících názvů domén. Tímto způsobem by došlo k ještě masivnějšímu vyčleňování národních webů z globální sítě a nabourána by tím byla samotná architektura a filosofie Internetu. V důsledku toho by byl člověk zcela fatálně omezen na přístupu k informacím, protože by, leč zdánlivě naprosto svobodný, neměl potřebné znalosti ani technické prostředky k prolomení těchto komunikačních bariér.

2. Hacking a cyberterorizmus a jeho dopady na společnost

Tato kapitola bude cílena zejména na zneužívání informací, počítačové zločiny a cyberterorizmus. V této oblasti je nejmarkantnější dopad na člověka, protože se zde setkáváme s jeho fatální podobou. Přeci jen se nedá srovnat omezení člověka na přístupu k informacím, nebo filtrování informací s přímým útokem, vedeným ať už proti jedinci, tak třeba proti nějaké větší organizaci, firmě apod. Osobní, ekonomický a právní dopad je při tomto jednání zcela zjevný. Ale můžeme se na tento „problém“ podívat též z jiného pohledu, který staví celou problematiku do zcela jiného světla a to pohled na hacking jako na společnosti prospěšnou činnost.

2.1. Hacker

Přímo navazujíc na kapitolu svobody informací v cyberprostoru musíme také poukázat na činnosti ilegálního zacházení s informacemi, které může být přímo i nepřímo nebezpečné pro jednotlivce, tak i společnost, nebo alespoň může panovat takovýto názor ve společnosti. Tento názor však bývá povětšinou mylný, protože v této oblasti dochází k nesprávnému výkladu pojmů. Pro tento účel si nejdříve musíme určit kdo je to hacker a jaké ho k jeho činnosti vedou okolnosti. Pro tento

účel nám poslouží Jargon File, jeden z celosvětově nejuznávanějších webů o hackerství.

Podle tohoto dokumentu je hacker:

1. Člověk, který se vyžívá v bádání po detailech programových systémů a překračování jejich schopností, což je odlišné od jednání většiny uživatelů, kteří se raději naučí jen nutné minimum. V dokumentu RFC 1392 (Internet Users' Glossary) hackera popisují jako člověka, který má potěšení z detailních znalostí vnitřních pochodů systému, počítačů a počítačových sítí.

2. Ten kdo programuje se zanícením (někdy s posedlostí), nebo ten kdo má požitek spíše z programování samotného, než z pouhého teoretizování o programování.

3. Osoba schopná pochopit/ocenit hodnotu hacku.

4. Člověk zdatný v rychlém programování.

5. Expert na určitý program, nebo někdo, kdo tento program často užívá. (Definice 1 a 5 si jsou podobné a lidé je spojují dohromady)

6. Expert nebo nadšenec v čemkoliv. Například astronomický hacker, elektrotechnický hacker, síťový hacker atd.

7. Někdo kdo si užívá intelektuální výzvu v překonávání, nebo obcházení limitů.

8. [-nesprávně-] Škodlivý slídil, který se „šťouráním“ snaží odhalit citlivé informace. Použito např. v názvech programů jako "Hence password hacker", "network hacker" - správně se ale člověk zabývající takovou činností nazývá cracker.

Označení "hacker" současně znamená členství v globální komunitě. Je lepší být označován jako hacker ostatními, nežli se tak označovat sám. Hackeři se považují za elitu, což je založeno na jejich schopnostech. Je zde tedy jakési ego satisfakce, když sebe identifikujete jako hackera. Když tvrdíte, že jím jste a přesto to

není pravda, tak budete bleskurychle označeni za „boguse“ = podvodník. Těmto lidem se také říká „wannabee“ (ti, kteří by rádi byli hackery, ale nejsou jimi). Zdá se, že tento termín byl poprvé přijat za vlastní v 60. letech jako znak pro hackerskou kulturu v okolí TMRC a MIT AI Lab. Podle některých zpráv to bylo použito ve smyslu blízkém tomuto záznamu, a to mladými radioamatéry a elektronickými spojovači v polovině 50. let. (The Jargon File, Kdo je to Hacker?)

2.2. Hackerství a etika

Hackeři jakožto profesionálové svého oboru mají svojí specifickou etiku a filosofii, kterou se řídí při svém konání. Nejjednodušeji jí popisují následující body:

1. Hackeři věří, že je správné sdílet informace. Je etická povinnost hackerů, aby sdíleli svou odbornost psaním open-source (otevřených) kódů a usnadnili přístup k informacím a počítačovým zdrojům všude tam, kde je to možné.

2. Věří, že crackování systémů pro zábavu je eticky v pořádku do té doby než crackerství přejde v zlodějství, vandalismus nebo poškození funkčnosti systému. Oba z těchto etických principů jsou brány obecně, ale v žádném případě nejsou všeobecně akceptovány mezi hackery. Většina hackerů akceptuje etiku popsanou v 1. bodě a na důkaz toho píší open-source software. Pár jich k tomu dále prohlašuje, že by veškeré informace měly být veřejně přístupné a zdarma, přičemž jakákoli vlastnická pravidla jsou podle nich špatná.

Smysl 2. bodu etiky je více sporný. Někteří lidé mají za to, že cracking je neetický, především opakované nabourávání a přistupování k systémům. Ale věří, že etické crackování s rozumným chováním a vyloučením destrukce systému, je gestem "laskavého crackera". Jedna z největších laskavostí hackera je, když se naboura do systému a pak vysvětlí administrátorovi (raději emailem), jak to udělal a jak odstranit chybu. Většina solidních manifestací dalších verzí hackerovy etiky je taková, že téměř všichni hackeři jsou ochotní podělit se o technické triky, software a (je-li to možné) o počítačové zdroje s ostanímy hackery. Ohromné spolupracující

sítě, jako například Usenet, FidoNet a Internet díky tomuto rysu mohou fungovat bez centrální kontroly. (Kdo je hacker?)

Nejvíce o hackerské komunitě vypovídá jeden ze stěžejních dokumentů tohoto oboru s názvem „Svědomí hackera“ (anglicky The Conscience of a Hacker), také známá pod názvem Hackerův manifest (anglicky The Hacker Manifesto). Krátká esej, napsaná 8. ledna 1986 hackerem, jenž si říká The Mentor (jeho reálné jméno je Loyd Blankenship). Autor jej napsal po svém zatčení a uveřejnil jej v undergroundovém hackerském Magazine Phrack v 1. díle 7. vydání, souboru 3/10.

Dnes je zkopírován na nespočet webových stránek. Tento článek je považován za jeden ze základních kamenů kultury hackerů a poskytuje určitý náhled do filosofie raných hackerů. Říká se, že zformoval komunitu a její pohled na sebe samu a své motivace. Manifest tvrdí, že hackeři hackují, protože je to pro ně způsob, jak se učit a protože jsou frustrováni a znuděni vzdělávacím systémem. Vyjadřuje také osvícení hackera v realizaci jeho potenciálu v počítačovém prostředí. (Wikipedia, Hackerův manifest)

Český překlad hackerova manifestu je přístupný na stránkách Britských listů.

„Svědomí hackera

Dneska chytli dalšího. Jsou toho plný noviny. "Mladík odsouzen za Skandální Počítačový Zločin", "Hacker zatčen za průnik do banky"...

Zatracený děti. Všechny jsou stejný.

Ale zkusili jste se někdy s tou svou trojitou psychologií a technomozkem padesátejch let podívat očima hackera? Položili jste si někdy otázku, jaká síla ho zformovala, co vytvářelo jeho osobnost?

Jsem Hacker. Vstup do mého světa...

Můj život začíná školou... Jsem chytřejší něž většina ostatních děcek, ty kecy co nám vykládají mě nudí...

Zatracenej flákač. Všichni jsou stejný.

Jsem na gymplu nebo na střední. Učitelka už po patnáctý vysvětluje, jak se krátí zlomek. Chápu to. "Ne, slečno Smithová, nepsal jsem postup. Udělal jsem to z hlavy..."

Zatracený děcko. Nejspíš to někde opsal. Všichni jsou stejný.

Dneska jsem udělal objev. Objevil jsem počítač. Počkej chvíli, to je skvělý. Dělá to, co chci. A když to udělá chybu, tak je to kvůli tomu, že jsem něco zvoral. A ne jenom proto, že mě nemá rád...

...nebo se cítí být mnou ohrožený...

...nebo si myslí, že jsem vypočítavej parchant...

...nebo že nemám rád učení a neměl bych tu bejt...

Zatracený děcko. Furt jenom hraje samý hry. Všechny jsou stejný.

A pak se to stalo... otevřely se dveře do světa... elektronický signál se řítí telefonní linkou jako heroin žilou narkomana, nachází úkryt před ubíjející každodenností... nachází board.

"To je to místo... sem patřím..."

Každýho tu znám. I když jsem je v životě neviděl, nikdy jsem s nima nemluvil, a možná že už o nich nikdy neuslyším... Znám vás všechny...

Zatracený děti. Furt jenom obsazujou linku. Všechny jsou stejný...

Vsaď boty, že jsme všichni stejný!

Ve škole jste nás krmili po lžičkách dětským jídlem a my chtěli steak... kusy masa, který k nám proklouzly byly předžvýkaný a bez chuti. Ovládali nás sadisti a ignorovali tupci. Bylo pár těch co nás mělo učit a našlo v nás ochotné žáky, ale těch bylo jako kapek vody v poušti.

"Toto je teď náš svět... Svět elektronů a spínačů, krása baudu. Využíváme existujících služeb bez placení, mohly by být skoro zadarmo, kdyby nepatřily šmelinářským hltounům, a vy nás nazýváte zločinci. My objevujeme... a vy nás nazýváte zločinci. Dychtíme po vědomostech... a vy nás nazýváte zločinci. Existujeme bez barvy pleti, bez národnosti, bez náboženských předsudků a vy nás nazýváte zločinci. Vy stavíte atomové bomby, vy vedete války, vy vraždíte, podvádíte a lžete nám a chcete, abychom věřili tomu, že je to pro naše vlastní dobro, přesto jsme my zločinci.

Ano, jsem zločinec. Mým zločinem je zvědavost. Mým zločinem je posuzování lidí podle toho co říkají a co si myslí a ne podle toho, jak vypadají. Můj zločin je to, že jsem chytřejší než ty, což je věc, kterou mi nikdy neodpustíš. Jsem Hacker a toto je můj manifest. Můžete zastavit jednotlivce, ale nemůžete nás zastavit všechny... konec konců, všichni jsme stejní.

The Mentor“

Napsáno 8. ledna 1986 jako Hackerův manifest – prohlášení nezávislosti (Mentor, 1986)

Způsoby a druhy hackingu a jejich dopady

Na celou problematiku lze dále pohlížet z pohledu dopadu na společnost a etiku celého působení a následků činů hackerů. Zjednodušeně lze říci, že hackeři (crackeři) jednají eticky, když důvody jejich prolamování bezpečnostních bariér systémů jsou vedeny z důvodů zvídavosti a jakési osobní prestiže, nikoli však za účelem osobního zisku nebo se záměrem poškodit cíl svého útoku. Na tomto místě bychom si měli uvést pár příkladů a způsobů ilegálního hackingu a cyberterorismu. V širším slova smyslu hacking zahrnuje záležitosti sahající od zneužívání či napadání telefonních systémů - obvykle s cílem bezplatného volání apod. (tzv. pheaking), dále přes shromažďování a šíření nelegálního software (tzv. warez), překonávání různých ochran komerčních SW produktů, DVD disků ap. (tzv. crackování) až po „tradiční“ průniky do počítačových systémů nebo sítí. V tomto článku budu pojem hacking používat právě pro ono „tradiční“ napadání a pokusy o neautorizovaný přístup k počítačovým systémům. (Miko, 2003)

Metody průniků

Prakticky každý útok hackera zneužívá nějakou slabinu, kterou může být:

- chyba výrobce (přímo v aplikaci, operačním systému),
- chyba dodavatele nebo administrátora (špatné nastavení),
- chyba uživatele – tato „slabina“ se narozdíl od předchozích dvou velmi obtížně řeší.

Základní druhy některých útoků:

- **Buffer Overflow (BOF)** – poměrně velký okruh slabin, jejichž příčinou je programátorská chyba díky níž dochází za jistých okolností k nežádoucímu přepsání paměti, čehož lze zneužít pro spuštění vlastního kódu.
- **Zneužití chyb ve WWW aplikacích** – nejčastěji SQL injection či podobné variace, kdy opět díky chybě programátora lze prostřednictvím manipulace s dynamickými parametry WWW stránek (příp. cookies) proniknout na sever či neoprávněně získat data.
- **Síťové techniky – Sniffing** (odposlech síťové komunikace), Spoofing (předstírání cizí identity, obvykle IP adresy).
- **Denial of Service (DoS) útoky** – Flooding (zahlcení linky, zahlcení systému požadavky, zahlcení e-mailovými zprávami, …), distribuované DoS (při současných technologiích prakticky není obrany).
- **Útoky na heslo** – hádání/lámání hesel. Bohužel na rozdíl od výkonu počítačů schopnosti lidí pamatovat si delší hesla stagnuje, proto tato velmi stará metoda je stále velmi účinná.

Karel Miko ve svém článku považuje za největší slabinu v drtivé většině případů lidský faktor (tj. vlastní zaměstnance), z konvenčních hrozeb vidí jako nejzákeřnější chyby ve WWW aplikacích či jiných systémech vyvíjených na zakázku – jedná se o jedinečné chyby programátora (vlastní zaměstnanec, či pracovník dodavatele), které žádný běžně dostupný scanner obsahující databázi jen těch nejrozšířenějších chyb neodhalí a často je vytvořena falešná iluze bezpečí. (Miko, 2003)

Příklad konkrétního ilegálního hackingu/crackingu

Zde bychom si měli uvést alespoň jeden konkrétní příklad hackerského útoku, který je zářnou ukázkou porušení veškeré etiky, která je popisována v předešlé kapitole. Jako velmi dobrý příklad jsem zvolil kauzu Alexeje Vadimiroviče Ivanova, ruského počítačového hackera z Čeljabinsku, který ve svůj prospěch získával celosvětově peníze od bohatých firem takovým způsobem, že vnikl na jejich servery, zkopíroval si privátní data dané firmy a následně kontaktoval tuto firmu emailem pod hlavičkou fiktivní „Expertní skupiny pro ochranu před hackery“ s požadavkem uhrazení nemalé sumy peněz výměnou za odhalení bezpečnostních rizik jejich systému zabezpečení. V případě, že daná firma odmítla zaplatit danou sumu, tak zaslal výhružný email popisující to, jak je snadné proniknout do firemního systému, stáhnout si jejich utajený software, kontakty o klientech a obchodních partnerech a pak jen zadat příkaz o kompletní vymazání dat ze zdrojových databází. Takovémuto nátlaku valná většina firem podlehla, protože v případě toho, že by se daný scénář uskutečnil, tak by jeho důsledky vážně existenčně firmu poškodily. Firmy, které přesto odmítly zaplatit, tak v krátkém čase přišly o veškerá data, případně například Ivanov zveřejnil citlivé informace o klientech na stránkách firmy. Tohoto jednání si nemohla nevšimnout americká FBI, které musela uskutečnit protiopatření v podobě vylákání Ivanova na území USA, protože s Ruskou federací nemá dohodu o vydávání zločinců. S fiktivní záminkou pracovní nabídky pozvala Ivanova do USA, kde pomocí jeho vlastních zbraní, metodou snímání stisků klávesnice, ho požádala, aby prokázal svoje umění a následně sama provedla protiútok na základě takto získaných přístupových hesel na

jeho počítače v Rusku, kde získala patřičné důkazy jeho ilegální činnosti, na jejichž základě byl později souzen. (Goldsmith, 2008, s. 194)

Kybernetická válka, hrozba zničení samé podstaty sítě

Oproti následujícímu příkladu se vedení hackerských útoků z předchozího odstavce může stát pouze malichernou záležitostí, která poškozuje pouze několik jednotlivých subjektů (osoby, firmy) v kyberprostoru. Jedná se zde o globální útok vedený zejména způsobem DoS (Denial of Service) popisovaný v podkapitole o možnostech vedení hackingových průniků a útoků. Při tomto útoku jsou využívány zdánlivě legitimní požadavky na systém v takové míře, že dojde k jeho zahlcení a následné nečinnosti online služby (například pád webových stránek). Proti správně připravenému útoku tohoto druhu se nelze bránit, protože jeho podstata je zakotvena v samotné filosofii internetu. Samotné provedení spočívá v infikování co možná největšího počtu nechráněných počítačů škodlivým kódem, který umožní v okamžiku aktivace soustavné „bombardování“ napadeného cíle zdánlivě legitimními požadavky. Zpravidla se jedná o obrovské množství počítačů umístěných po celém světě, takže během chvíle dochází ke zhroucení cíle. Následná oprava není vůbec snadná, protože i po restartu útok trvá a problém se ihned opakuje. Jediná obrana je pak odpojení služby od sítě, což je zpravidla cíl, kterého útočící hacker chtěl dosáhnout. Samotní správci sítě přirovnávají tento typ útoku k živelné katastrofě, které se nedá vyhnout nebo bránit, ale může na ní být člověk co nejlépe připraven (záložní systémy apod.). V budoucnosti se tak snadno může stát, že ať chceme nebo ne, bude potřeba změnit samotnou architekturu a podstatu dnešní sítě, protože není vůbec nereálné, že bude přibývat kybernetických válek znepřátelených skupin hackerů nebo profesionálních hackerů najatých vládními/nevládními organizacemi za účelem zničení/ poškození /vypnutí/vyřazení protivníkových systémů. (Goldsmith, 2008, s.229) Vůbec nejsme daleko od pravdy, když budeme předpokládat, že válečné pole budoucnosti bude virtuální prostředí, na kterém již dnes záleží fyzická existence a funkčnost tolika reálných věcí, že v případě jejich nefunkčnosti se naše společnost, jak jí známe z každodenního života, ve chvíli zcela zhroutí a nebude fungovat zhola nic. V tomto pohledu tak vidíme hackera jako moderního válečníka nové informační doby, virtuálního

teroristu, který rozhoduje o životech lidí stejně tak fatálně jako člověk nastražující nálože výbušniny na plném fotbalovém stadionu při zápase 1. ligy. Má tedy v dnešní společnosti takovýto patologický jev právo na život?

3. Problematika sociálních sítí z pohledu ochrany osobních údajů, ztráta soukromí a identity

Dnešní doba zažívá doslova boom sociálních sítí a podobných elektronických služeb vycházejících z přirozené potřeby lidí budovat si mezi sebou kontakty a udržovat se ve spojení s blízkými lidmi, kteří díky dnešní „moderní“ době nám začínají být čím dál tím více vzdálenější. Tato technologie je dnes velice rozšířená a vyladěná do takové podoby, že svůj profil si dokáže vytvořit i začátečník v práci s internetem a počítači obecně. Na takovéto uživatele pak čeká ve „spárech“ sociálních sítí mnoho nástrah. Jedná se zejména o nerozumnou ventilaci osobních informací jednotlivých uživatelů a jejich následné zneužití.

Mnoho nezkušených uživatelů tak dává všanc mnoho svých soukromých osobních údajů a vůbec si neuvědomuje hrozby, které jim bezprostředně hrozí. Mnozí pod matnou iluzí anonymity ve virtuální síti na sebe prozrazují informace, které použité v reálném světě můžou způsobit nedozírné důsledky. Celý tento jev jasně vyplývá ze snahy uživatelů se co nejvíce prezentovat ve virtuálním prostředí, protože toto prostřední je této prezentaci velmi nakloněno. Ještě nikdy v historii nebylo tak snadné prezentovat sama sebe, svojí tvorbu nebo svoje názory tak širokému spektru ostatních osob.

Co je to sociální síť a její klady a zápory a bezpečnostní rizika

Jak již bylo řečeno, tak sociální síť řeší potřebu vzájemné komunikace uživatelů a dává jim možnost budovaní seznamu svých známých a přátel ať už reálných nebo pouze virtuálních. Tato síť funguje na principu provázané pavučiny kontaktů lidí navzájem sdílejících informace protkaných a propojených virtuální pavučinou, která může značit jejich příslušnost k určité komunitě, zájmové skupině,

pracovní skupině – ve vzájemném vztahu. Díky takto vytvořené síti si jednotliví uživatelé můžou nadefinovat svoje takzvané uživatelské profily, které reprezentují jejich osobu ve virtuálním světě. Uveřejněním co největšího počtu osobních údajů získává tak uživatel možnost co nejlépe vyhledávat osoby s podobnými zájmy jako má on sám, či rozvíjet diskuse k různým publikovaným informacím (obsahu). Zároveň ale tímto způsobem člověk přichází o své soukromí. Je obecně známo, že na sebe takto často lidé prozradí informace, které by ostatním nesdělili ani při přátelské rozmluvě někde „u piva“. Je známo mnoho konkrétních případů, kdy neopatrný uživatel o sobě do „zdivočelého“ virtuálního prostoru uvedl nečekaně detailní osobní až intimní informace, na jejichž základě byl pak obtěžován jak ve virtuálním prostředí, tak tato agrese přerostla do reálného světa.

Když se k tomuto rizikovému chování přidá ještě nezodpovědnost v přidělování přístupových práv (nastavení, kdo se na můj „profil“ může podívat a kdo ne, případně které skupiny ostatních uživatelů vidí které osobní informace), tak si už tento člověk doslova „koleduje“ o zneužití osobních informací. Tento problém může snadno nastat i když nějaký váš přítel, který je ale pouze „přítelem“ uveřejní veřejně nějaké informace, data (např. digitální fotografie), která vás jako žijící osobu mohou snadno poškodit a důsledky tohoto konání můžou mít vážné následky v reálném světě. Mnohá data uveřejněná na síti mohou mít zcela nevhodný či dokonce poškozující nebo kompromitační obsah. (obrázky, videosoubory atd..) V důsledku takovéhoto jednání již došlo k mnoha fatálním následkům v reálném světě, kdy na internet unikly například fotky určité osoby zobrazujících jí v různých nevhodných situacích, zejména se sexuálním podtextem. Dotyčná osoba pak celou situaci a ostudu u ostatních neunesla a celý případ skončil sebevraždou. V současnosti je tento problém spojený například s takzvaným „sextováním“, kdy si zejména mladí lidé posílají za pomoci moderních telefonů vybavených digitálními fotoaparáty svoje fotografie erotického až pornografického charakteru. Děje se tak mezi partnery, tedy lidmi navzájem blízkými, ale po rozchodu nezřídka kdy jeden z partnerů zveřejní fotografie na internetu, čímž se zaprvé dopouští trestného činu, navíc však nedomýšlí vůbec následky tohoto konání, protože stejně jako vyřčené slovo a vystřelený šíp, tak ani digitálně zveřejněná a kopírovatelná data již nikdy není schopen odstranit.

Nezodpovědné zveřejňování osobních informací a dopady na člověka

Rizikem pro všechny doslova hloupé uživatele je publikování informací o jejich, ne zrovna legálním, chování. Takovýto člověk by měl zvážit, co o sobě prozrazuje na sociálních sítích, a zda je vůbec rozumné tam mít svůj účet. Právě to se totiž před pár dny vymstilo australským chytrákům, kteří utekli z restaurace bez zaplacení. Australané byli přesvědčeni o tom, že jejich plán musí vyjít. Vybrali si jednu dražší restauraci na melbournském Southbanku, a dali si pořádně „do nosu". Na stole se střídala drahá vína, ryby, ústřice. Po hostině si šli ven zakouřit… a v chůzi pokračovali. Do podniku, kde po nich zůstal nezaplacený účet, v přepočtu za bezmála sedm tisíc korun, se už nevrátili. Majitele restaurace to pochopitelně rozčílilo. Pak si ale vzpomněl, že se jeden z pětice mladých lidí ptal zkraje večera na servírku, která zrovna neměla směnu. Poté, co jí vysvětlil, co se stalo, napadlo je použít k identifikaci Facebook. Když se podívali na seznam jejích kontaktů, za chvilku dva z neplatičů našli. Mladík a jeho dívka měli ve svém profilu dokonce uvedené, že pracují v nedaleké restauraci. Netrvalo tedy dlouho a své peníze, i s velkorysým dýškem, dostal okradený muž zpět. Oba podvodníci navíc přišli o práci. Jejich zaměstnavatele, kterého majitel restaurace kontaktoval, totiž strašlivě dopálilo, že okradli kolegu z branže. O práci už díky svému chování na sociální síti přišel také jeden zaměstnanec call centra, který svému šéfovi tvrdil, že je nemocný. Ve svém statusu na Facebooku přitom jásal nad tím, že je stále ještě opilý z předešlé noci, a jak je skvělé, že nemusí do práce. (Zychová, Být či nebýt na Facebooku)

Falešná identita ve virtuálním prostředí a její dopady na realitu

Dále se pak také setkáváme se situací, kdy se uživatelé záměrně maskují, mění nebo se vydávají ve virtuálním prostředí za někoho zcela jiného za účelem nějakého osobního prospěchu. Toto konání může být buď pouze neetické, nebo dokonce velice nebezpečné a ilegální. Případ, kdy se na virtuálním seznamovacím serveru vydáváme za dvacetiletou sexy blondýnku bez závazků a ve skutečnosti jsme vdova se 4 dětmi nebo dokonce muž, tak tato situace je na svědomí každého z uživatelů. Tento případ se ale snadno může „zvrtnout" v takzvaný cybergrooming, při kterém se někteří lidé vydávají ve virtuálním světě za někoho jiného s úmyslem

se setkat s danou osobou v reálném světě. Stává se tomu tak zejména v případech následného zneužití dětí a mladistvých. Takovéto chování je velmi vážný zločin, který se bohužel nedaří zcela adekvátně trestat. Pachatelé se spoléhají na nezkušenost v používání a velikou důvěřivost těchto věkových skupin a celkově je tento čin velmi nebezpečný pro společnost.

Když virtualita nahradí realitu

Poslední a nejvíce závažný problémem je, když virtuální budování přátelství a sdílení informací zcela nahradí tuto činnost v reálném světě. Mnozí lidé tráví pak u počítače doslova 24 hodin denně a jejich reálný život se promění ve virtuální existenci. Jejich fyzická existence pak značně strádá a postupem času se jejich život změní pouze v chorobnou závislost na technologii. Pozbudou tak veškerého umění konání a navazování vztahů v reálném světě a odsoudí se tak pouze na život ve své virtuální realitě, ve které sice mohou být tím, kým chtějí, odstranit tak všechny své reálné nedostatky, ale připraví se tak o všechny tělesné požitky spojené s prostou existencí na této planetě. Je pouze filozofickou otázkou, zda-li je toto dobře nebo špatně. Za předpokladu, že takto žijící člověk je šťastný, tak proč by nemohl žít způsobem, jaký si sám zvolil. Na druhou stranu jaký je pak jeho přínos pro společnost? Osobně si myslím, že na světě stále (naštěstí) žije valná většina lidí, kteří rádi vyrazí za svými reálnými přáteli, jdou si spolu popovídat, vezmou svojí přítelkyni/přítele na rande, sednou si na skleničku… Nedokážu, a ani nechci, si představit realitu, kdy každý bude ve světě pouze reprezentován určitými daty sdílenými v síti a veškeré vzájemné interakce budou realizovány pouze digitálními přenosy dat – signály putujícími virtuálním cyberprostorem. Tato vize, která doufám, že nikdy nenastane, byla například dobře ztvárněna ve filmu Matrix režisérů bratrů Larryho a Andyho Wachowskich, kde jednotlivé lidské bytosti byly pouze v roli jakýchsi baterií, kterým byl přímo do mozku promítán virtuální svět, ve kterém žili jako v jakési iluzi, potom co reálný svět byl zcela zničen. Člověk jako jedinečná existence a jeho názory, myšlenky a reakce byly zcela potlačeny a kontrolovány jakýmsi „velkým bratrem“. Z tohoto pohledu můžeme v této postapokaliptické vizi vidět jasnou analogii s fungováním totalitního státu. V tomto místě se opět dostáváme k problému svobody. Člověk, který je na čemkoli závislý, nemůže být nikdy svobodný, nikdy se nemůže svobodně rozhodovat. Závislost na

technologii tak může člověka snadno zbavit veškeré jeho osobní volnosti, jako tomu může být například u závislosti na drogách nebo alkoholu.

Specifickou podskupinou příkladu virtuální existence jsou online počítačové hry. (MMORPG - **Massively-Multiplayer Online Role-Playing Game) V těchto tzv. „hrách na hrdiny“ si hráč již v prvopočátku zvolí svojí postavu, tzv. avatara, který je pak jeho virtuální reprezentací v virtuálním světě. Takovýto hrdina není pak nositelem vlastností daného člověka v reálném světě, ale je to spíše takový únik reálného člověka do digitální podoby, podněcující jeho fantazii a dávající mu možnost žít nereálné příběhy, které jsou v reálu neuskutečnitelné. Virtuální svět je pak plný takovýchto postav, které spolu vzájemně komunikují a vytvářejí mnohé interakce (rozhovory, souboje, obchod apod.). Hráči v těchto hrách jsou motivovaní k dalšímu hraní rozvíjejícím se příběhem, získáváním nových předmětů, které jim umožňují uskutečňovat nové akce a rozvojem schopností postavy závislém na plnění úkolů, které se odvíjí od příběhu. Celý tento koncept virtuální existence může mít ale až takovou chytlavost, že se často stává pro hráče až zhoubnou záležitostí v podobě závislosti na hraní a snadno může mít stejné následky jako problém odloučení reálné existence od té virtuální, který je popsaný v předchozím odstavci.**

4. Nevyžádané a klamné informace

V poslední kapitole budou nastíněny základní rizika nevyžádaných, záměrně zavádějících a matoucích informací a dopad těchto informací na člověka. Rizika těchto desinformací se mohou zdát zanedbatelná, avšak mnoho lidí není schopno informace správně interpretovat a vyhodnocovat jejich důležitost, pravdivost a relevanci. Tito jedinci jsou pak nejvíce ohroženi stálým přívalem informačního toku, který na ně dopadá ze všech stran a je jen na schopnostech, zkušenostech a možná dnes i štěstí každého z nás nenechat se ovlivnit.

Spam

Samotný název termínu je odvozen ze značky amerických konzerv lančmítu (překlad „haše“ v televizních titulcích je nepřesný), která se vyrábí od 30. let dodnes (v současnosti ale výrobce trvá na psaní velkým písmem SPAM) a za 2. světové války a po ní byla hojně rozšířená a stále méně oblíbená ve Velké Británii. Proto se objevuje v závěrečném skeči 25. dílu seriálu *Monty Pythonův létající cirkus*, kde všechny položky jídelního lístku v restauraci obsahují spam, i mnohokrát opakovaně, a spory zákazníků s číšnicí o objednávky přerušuje skupina Vikingů zpívajících „Spam, spam, spam…“

Označení tak bylo přijato nejprve pro praktiku mnohonásobného rozesílání téže zprávy na Usenetu, ale pak se význam posunul pro zneužívání skupin k šíření různých nepřípadných textů a přímo reklamy a zachoval se i poté, co se těžiště takových aktivit přesunulo do e-mailu. (Wikipedia, Spam) V současnosti je ale tento jev spojován převážně s hromadně šířenou nevyžádanou reklamou pomocí emailové služby. Zdánlivě nenápadný problém tak dnes přerostl do obrovských rozměrů, kdy zhruba 90% emailové komunikace je nevyžádaný obsah. Tímto způsobem tak není zatěžována pouze samotná komunikace sama o sobě, ale zároveň je velmi zatěžován samotný adresát zprávy, protože se snadno stává obětí informačního přesycení. Ve chvíli kdy i relevantních informací je dnes tolik, že není v silách jednotlivce tyto informace zpracovat, tak nevyžádané informace jsou už jen jakýsi hřebíček do rakve v orientaci člověka. Ve chvíli kdy 9 z 10 přijatých zpráv je nechtěných, nastává riziko, že osoba jednající automaticky nedokáže rozeznat zprávu od spamu a snadno tak přichází o důležité informace. V opačném případě je člověk natolik zaměstnán analýzou příchozích zpráv, že ztrácí zcela zbytečně drahocenný čas, který by mohl věnovat smysluplné činnosti. A z jakého důvodu? Zde narážíme na další aspekt, který s sebou nese spam a to je jeho účinnost. Je dokázáno, že svůj účel splní zhruba asi tak 1% spamových zpráv, čili zbylých 99% je zcela zbytečných. Adresnost informací je u spamu absolutně minimální, respektive žádná, protože jsou zcela chaoticky šířeny sítí. Samotní adresáti jsou vybírání speciálním softwarem, který doslova těží emailové adresy z obsahu celé sítě a nemalou mírou mohou přispět i tzv. hoaxy (hromadné emaily – viz. bod 5.2), které jsou rozesílány samotnými uživateli na adresy jejich přátel. Z čehož vyplývá, že obrana proti spamu je velice obtížná, jelikož i když vy jako konkrétní uživatel se budete chovat na síti co možná

nejzodpovědněji, tak stačí aby nějaký váš známý/přítel/kontakt někde použil vaši emailovou adresu a v zápětí se ocitáte na seznamu pro spamování. V následujícím přehledu bude nastíněno několik způsobů ochrany proti škodlivému spamu. Žádný z nich, ani jejich kombinace, ale nejsou prozatím 100% účinné.

Způsoby částečné ochrany proti spamu:

Blacklisting - rozhoduje, zda dopis je nebo není spam, podle adresy odesílatele (která může být zfalšována), nebo lépe podle IP adresy, ze které dopis přišel na cílový SMTP server. Blacklisty obsahující IP adresy, ze kterých bylo zaznamenáno rozesílání spamu, bývají zveřejňovány nejčastěji pomocí systému DNS. Výskyt adresy v blacklistu může mít za následek buď přímé odmítnutí (nepřevzetí) dopisu ještě během SMTP relace, nebo může být informace z blacklistu použita jako dodatečná informace při následné filtraci podle obsahu.

- **Greylisting** rozhoduje také podle IP adresy a emailové adresy odesílatele a adresáta, ale dělá to dynamicky. SMTP server, který provozuje greylisting, udržuje databázi, kde pro trojici (IP adresa, odesílatel příjemce) je uvedeno, zda dopis s těmito atributy má být převzat k dopravě, nebo zda jeho převzetí má být *dočasně* odmítnuto. První dopis je odmítnut a je zaznamenán čas, kdy k tomu došlo. Po určitou dobu (typicky několik desítek minut) pak jsou dopisy s týmiž atributy odmítány. Po uplynutí této doby, pokud se původní SMTP server stále pokouší o odeslání dopisu, je záznam v databázi potvrzen a dopisy jsou naopak přijímány a dopravovány bez zdržení. Po další době (typicky několik málo týdnů) je záznam z databáze odstraněn, takže příští dopis bude opět pozdržen. K odstranění záznamu z databáze dojde také v případě, že v příslušném intervalu, kdy byly dopisy odmítány, se nepokusí původní SMTP server o znovudoručení.

- **Filtrace podle obsahu** - Automatické rozpoznávání nemůže z principu fungovat dokonale, protože názor, zda konkrétní dopis je spam, je individuální. Přesto filtrování podle obsahu dává použitelné

výsledky a hojně se používá. Existují dvě základní metody, některé antispamové programy je kombinují.

- **Filtry založené na pravidlech** - vyhledávají v dopisech rysy, které jsou pro spam typické. Jde jednak o některá slova (např. viagra) a slovní spojení, jednak jsou vyhledávány chyby pro spam typické. Příkladem je třeba datum odeslání v budoucnosti, nedovolené znaky v hlavičce, chybně označený MIME-typ zprávy apod. Za každý rozpoznaný rys je dopisu přiděleno bodové ohodnocení, body se zpravidla sečítají, a pokud součet přesáhne hranici, je dopis pokládán za spam. Rozpoznávané rysy jsou definovány pomocí pravidel, která je třeba pravidelně aktualizovat a přizpůsobovat praktikám spammerů. K vytváření a údržbě souboru pravidel je třeba mít znalosti, není to práce pro běžného uživatele, laika.

- **Filtry založené na učení** (často nazývané bayesovské) využívají triky z oblasti umělé inteligence. V režimu učení se filtru předkládají dopisy explicitně označené jako spam a ham (ne spam), filtr z předložených dopisů extrahuje informace, které si ukládá do databáze. Nejčastěji je dopis rozkládán na slova (popř. jiné úseky textu) a pro jednotlivá slova se statisticky zjišťuje pravděpodobnost, že dopis, který toto slovo obsahuje, je spam. V režimu rozpoznávání pak filtr využívá nashromážděné informace a testovanému dopisu přiřadí pravděpodobnost, že je to spam. Nejčastěji se pro výpočet pravděpodobnosti používá vzorec, který navrhl matematik Bayes. Velkou výhodou je, že filtr může učit i uživatel – laik. Učící se filtry jsou nejúčinnější, učí-li je přímo sami koncoví uživatelé podle svého individuálního názoru, co je spam a co ne. Přesto se bayesovské filtry používají i na serverech, kde učení probíhá pro všechny uživatele serveru společně.

(Wikipedia, Spam)

Hoax aneb fáma na internetu

Hoax, neboli jakási legrácka, klamná informace, vtípek, fáma na internetu, záměrná mystifikace nebo také novinářská kachna je jedním z velice závažných problémů dnešní komunikace. Ve své podstatě se jedná o desinformace záměrně šířené sítí, které zbytečně zatěžují uživatele nebo mají v úmyslu jim dokonce uškodit. V počítačové terminologii je tímto míněno zejména smyšlené varování před neexistující hrozbou (např. nový počítačový vir apod.). Pro co nejlepší popis tohoto komunikačního problému jsem si vybral specifikace zveřejněné na českém největším webovém serveru zabývajícím se touto tématikou www.hoax.cz. Typický hoax poznáme podle serveru http://www.hoax.cz zejména podle následujících specifik:

- **Popis nebezpečí (viru)**: Smyšlené nebezpečí (vir) bývá stručně popsané, v případě viru bývá uváděn i způsob šíření.

- **Ničivé účinky (viru)**: Zde záleží převážně na autorově fantazii. Ničivé účinky mohou být celkem obyčejné, třeba zformátování disku nebo už míň důvěryhodné - zběsilý útěk myši do ledničky, roztočení HDD opačným směrem, výbuch počítače...

- **Důvěryhodné zdroje varují**: Ve většině případů se pisatel poplašné zprávy snaží přesvědčit, že varování přišlo od důvěryhodných zdrojů ("IBM a FBI varují" nebo "Microsoft upozorňuje" atd...)

- **Výzva k dalšímu rozeslání**: Tento bod hoax vždy obsahuje! Mnoho nezkušených uživatelů se nechá zprávou napálit a bez přemýšlení výzvu uposlechnou. Právě proto se tyto nesmysly lavinovitě šíří.

Jako hoax můžeme také označit šířenou zprávu, která obsahuje nepřesné, zkreslující informace, účelově upravené polopravdy nebo směsku polopravd a lží. V praxi můžeme použít následující pravidlo: jestliže zpráva obsahuje výzvu k hromadnému rozeslání na další adresy, je to podezřelé a s největší pravděpodobností hoax. Občas to také může být původně opravdová prosba o pomoc, ale i ty svého největšího šíření dosáhnou v době, kdy jsou již neaktuální.(www.hoax.cz, Co to je hoax)

Typickými příklady hoaxů podle serveru www.hoax.cz jsou:

- **Varování před smyšlenými viry a různými útoky na počítač** Nejčastější typ poplašných e-mailů.
- **Popis jiného nereálného nebezpečí**: Zprávy varují před vymyšleným nebezpečím z běžného života - mimo oblast výpočetní techniky. Často obsahují směs lží a polopravd, které nezasvěcený člověk nemůže s jistotou posoudit.
- **Falešné prosby o pomoc**
    - Kdysi skutečná prosba o pomoc, většinou se masově rozšíří až po její aktuálnosti. Typickým příkladem jsou prosby o darování krve pro nemocného člověka.
    - Trapný pokus o žert, který útočí na základní lidské city.
- **Fámy o mobilních telefonech:** Vymyšlené, zkreslené nebo neúplné informace o mobilních telefonech. Většinou bývají také masově šířené.
- **Petice a výzvy**
    - Smyšlená petice jako žert.
    - Nedomyšlená snaha boje za určitou věc. Petice šířená e-mailem často neobsahuje potřebné údaje podepisujících se (pokud je lze takto označit), aby petice byla platná. Naopak, jestliže ke jménu připojíte další osobní údaje, dáváte je k dispozici komukoliv, kdo e-mail dostane. Zpráva s vašimi údaji se šíří pyramidovitě v mnoha různých variantách na další adresy. Kdykoliv může být změněn i text údajné petice a váš podpis může být pod něčím, s čím nesouhlasíte.
- **Pyramidové hry a různé nabídky na snadné výdělky**

- Většinou to jsou různé obdoby pyramidových her. Podle našich zákonů jsou pyramidové hry zakázány, proto se je organizátoři snaží maskovat jako prodej různých produktů. Tyto nabídky mají stejný základ: koupím produkt od zapojeného účastníka(ů), tím již zapojené členy posunu o pozici výš a snažím se přesvědčit jiné, aby produkt koupili a moji pozici také vylepšili. Pokud je trh nasycen - a to díky pyramidovému způsobu je poměrně rychle - poslední mají minimální šanci, že někdo další se připojí, a jsou to pouze jejich peníze, které pomohly alespoň částečně vrátit náklady zapojeným předchůdcům.

- Nabídky na odměnu nebo slevu na služby za hromadné rozeslání e-mailů. Pořádně si rozmyslete, jestli je slíbená odměna dostatečnou kompenzací za obtěžování vašich přátel.

- Žertovná zpráva, ve které se slibuje za její další rozeslání lákavá odměna.

- **Řetězové dopisy štěstí:** Čínské modlitby a různé dopisy štěstí šířené z pověrčivosti nebo z neznalosti.

- **Žertovné zprávy:** Různé žertovné zprávy, které si posílají kamarádi a známí. Zde bych pouze připomněl, že ne všichni mají stejný smysl pro humor, a proto není vhodné je hromadně šířit na všechny adresy.

Hlavní škodlivost a technické a sociální dopady pak tyto zprávy mají zejména protože:

- **Obtěžují příjemce:** Opakovaný příjem nesmyslných zpráv je pro mnohé uživatele nepříjemné, zejména v době epidemie, kdy se v e-mailových schránkách objevuje stejná zpráva několikrát denně. V této době se stává, že uživatel prakticky nedělá nic jiného, než že maže nechtěné informace a tím pádem přichází o čas, který by mohl věnovat práci/zábavě atd.

- **Zbytečně zatěžují linky a servery:** Přestože výkonnost serverů a rychlost vzájemného propojení se zvyšuje, je také nutné si uvědomit, že

zatížení sítí také narůstá. Vyšší nároky na sítě jsou dány nejen narůstajícím počtem uživatelů, ale také stále větším počtem šířících se škodlivých kódů a hlavně různého spamu. V dnešní době tvoří spam přes 90% veškeré e-mailové komunikace! Proč zbytečně tento počet navyšovat zbytečnými hoaxy a řetězovými zprávami.
Velké množství hoaxů rozesílají uživatelé způsobem předat dál a na všechny adresy. Tím dochází k postupnému přidávání adres k textu zprávy a samozřejmě narůstá velikost zprávy, často až do velikosti přesahující 100 kB. Pro porovnání, běžný e-mail mívá velikost 2-6 kB, e-mail s přiloženým dvoustránkovým doc dokumentem přibližně 65 kB. V součtu pak jejich velikost může dosáhnout i mnoha MB. Masivní šíření takovéhoto množství dat pak má za následek značné zpomalení internetové komunikace a zvyšuje náklady provozovatelů internetového připojení a přenosu, kteří si tyto peníze ale vždy nakonec vymůžou od uživatelů.

- **Šířením hoaxu můžete vyzradit důvěrné informace**: Typický hoax je vždy přeposílán způsobem „pošli alespoň 10ti kamarádům“, dává tak k dispozici obrovský seznam e-mailových adres náhodným příjemcům. Kvůli lavinovitému šíření zprávy nemůžete vědět, komu v dalších úrovních bude e-mail doručen. Seznam adres je rájem pro spamery, kteří pak mohou na získané adresy posílat nevyžádané e-maily. Někteří uživatelé se nestačí divit, jak mohli spammeři získat jejich adresu, kterou svěřili pouze několika známým. Ve skutečnosti stačí, aby se hromadně rozeslaný e-mail dostal na počítač infikovaný škodlivým kódem, který z něj dokáže vysbírat adresy a dále je zneužít.
Další nepříjemná situace by mohla nastat, kdyby se Váš seznam adres klientů a obchodních partnerů dostal ke konkurenci.
V případě různých petic nebo smyšlených podpisových akcí se požaduje vyplnění různých osobních údajů včetně adresy a rodného čísla. Opět nikdy nemůžete vědět, kdo si Vámi vyplněné informace přečte a jakým způsobem je zneužije.

- **Může přímo poškodit jinou osobu nebo společnost**: Některé hoaxy nebo řetězové zprávy uvádí úplné kontakty nebo třeba jen telefonní čísla na osobu, která sice se zprávou nemá nic společného, ale přesto se na ni v textu odvolává. Typickým příkladem je nabídka štěňátek, kdy jsou uvedeny telefonní čísla, kam případní zájemci mohou volat. Často jsou to kontakty na lidi, kteří nikdy žádného psa neměli, ale třeba z pomsty nebo škodolibosti vypustí e-mail do světa. V době masového rozšíření zprávy je telefon postiženého prakticky nepoužitelný.
  Také šíření nepravdivých, polopravdivých nebo zkreslených informací o různých společnostech jim mohou způsobit různé nepříjemnosti. Například poškození dobrého jména, ale také zbytečné zahlcení zákaznických linek, kam lidé na základě informací v e-mailu volají.

(www.hoax.cz, Čím hoax škodí)

Jediným způsobem, jak tomuto nebezpečí ze strany klamných informací čelit, je ho včas odhalit a v žádném případě dál nešířit!!! Celý tento problém internetové komunikace je zakořeněný v samotných lidech a není žádným novým problémem. Již odnepaměti si lidé sdělovali informace a každý si tyto informace nějak přibarvil. Takto vznikaly fámy, které se šíří mezi lidmi jako lavina. Stejně tak jako u výše zmíněných hoaxů každé takovéto vyprávění se vždy opíralo o „spolehlivý zdroj“ vždy uvedený s jakousi neurčitostí alias „kamarád kamaráda má tetu, která…“. Takovýto úvod za účelem získání důvěryhodnosti získá v adresátovi zájem o příhodu a o to více pak ji šíří dál. Tímto způsobem se pak k lidem dostávají na první pohled uvěřitelné příhody o „ukradené ledvině“ nebo například poutavá story o záhadné infekci pocházející z mrtvých těl. Mnoho lidí do dneška věří v to, že jim škvor vleze do ucha a propíchne ušní bubínek, nebo že by měli před konzumací banánu odlomit jeho špičku, protože exotické hady nebaví nic jiného, než testovat svoje jedové zuby na koncích tohoto oblíbeného ovoce. Veškeré tyto příběhy byly vždy jakousi lidovou tvořivostí a svým důsledkem byly prakticky neškodné, ale už v historii se našly příklady, kdy určitá fáma mohla poškodit jednotlivce nebo zejména nějakou společnost (příběhy o uříznutých prstech v konzervách od fazolí nebo o záhadně mizejících slečnách v převlékacích kabinkách společnosti nabízející dámskou konfekci). Je vždy na posouzení každého jednotlivce, zdali se nechá

takovouto informací ovlivnit nebo jí dokonce jako zaručenou pravdu šíří dál. Prevence v tomto případě neexistuje, záleží jen na důvěřivosti a zkušenostech každého z nás, ať už v reálném životě, nebo při konání ve virtuálním světě.

ZÁVĚR:

V práci, na jejímž konci se nyní nacházíte, se autor pokusil co nejlépe zmapovat prostředí komunikace informací 21. století a jevy s tímto problémem spojené. Hlavní zřetel byl kladen na nastínění stavu, v kterém se nachází svoboda informací v digitálním prostředí a který se stejně tak promítá i do reálného světa, neb jest jakýmsi jeho virtuálním obrazem. Hlavní snahou bylo prezentovat negativní jevy, které se v tomto prostředí odehrávají a sociologický dopad těchto jevů na společnost i na jedince. Za pomoci konkrétních příkladů i mnohých zamyšlení nad stavem věcí, jsou předkládány i některé důležité otázky do budoucna, které tato práce zajisté nevyřeší, ale snad bude alespoň podnětem k přemýšlení nebo

zajímavým pohledem na věc zase z trochu odlišného úhlu pohledu. Celá práce a všechny její kapitoly naráží na problematiku svobody komunikace informací, protože v průběhu informační přípravy k jejímu sepsání byl autor velice zaujatý touto tématikou a z názorů zde prezentovaných lze snadno vycítit, že svoboda ať již v digitálním, tak v reálném světě, je pro něj hodně důležitá i za cenu možných patologických jevů, ke kterým mohou mnozí svobodu zneužít. Na tomto místě už netřeba psát nějaké další závěry či otázky, neboť všechny jsou průběžně rozmístěny v jednotlivých kapitolách.

Seznam použité literatury:

1. CEJPEK, Jiří. *Informace, komunikace a myšlení : úvod do informační vědy*. 2., přeprac. vyd. Praha : Karolinum, 2005. 233 s. ISBN 80-246-1037-X.

2. Co to je hoax. *hoax.cz* [online] Akt. 2009 [cit. 2009-05-20]. Dostupný z WWW: <http://www.hoax.cz/hoax/co-je-to-hoax>.

3. Česko. Zákon č. 202 ze dne 17. května 1990 o loteriích a jiných podobných hrách. In *Sbírka zákonů České republiky*. 2007. Dostupný také z WWW: <http://portal.gov.cz/wps/WPS_PA_2001/jsp/download.jsp?s=1&l=202%2F1990>.

4. Česko. Zákon č. 480 ze dne 29. července 2004 o některých službách informační společnosti. In *Sbírka zákonů České republiky*. 2008. Dostupný také z WWW: <http://portal.gov.cz/wps/WPS_PA_2001/jsp/download.jsp?s=1&l=480%2F2004>.

5. Čím hoax škodí. *hoax.cz* [online] Akt. 2009 [cit. 2009-05-20]. Dostupný z WWW: <http://www.hoax.cz/hoax/cim-hoax-skodi>.

6. *Deep web*. In Wikipedie: Otevřená encyklopedie. c2008. Datum poslední revize 19.4.2009 [cit. 20.4.2009]. Dostupný z: <http://en.wikipedia.org/wiki/Deep_Web>.

7. GOLDSMITH, Jack; WU, Tim. *Kdo řídí internet?: Iluze o světě bez hranic*. Praha: Dokořán, 2008. 271 s. ISBN 80-7363-184-0.

8. Hackerův manifest. In Wikipedie: Otevřená encyklopedie. c2008. Datum poslední revize 19.4.2009 [cit. 21.5.2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Hackerův_manifest>.

9. *Internet*. In Wikipedie: Otevřená encyklopedie. c2008. Datum poslední revize 19.4.2009 [cit. 20.4.2009]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Internet>.

10. JAIN, Ravi. Hacking--Ethical or Criminal A Legal Quandary. *ICFAI Journal of Information Technology* [online]. 2008:49-56. [cit. 2009-05-10] Dostupný z WWW: <http://search.ebscohost.com.onelog3.ruk.cuni.cz/login.aspx?direct=true&db=iih&AN=32563334&site=ehost-live>.

11. KAPFERER, Jean-Noel. *Fáma, nejstarší médium světa*. Praha : Práce, 1992. 244 s. ISBN 80-208-0262-2.

12. KATUŠČÁK, Dušan; MATTHAEIDESOVÁ, Marta; NOVÁKOVÁ, Marta. *Informačná veda: terminologický a výkladový slovník*. Bratislava : Slov. pedag. nakl., 1998. 375 s. ISBN 80-08-02818-1.

13. Kdo je hacker? *Security-portal.cz* [online] Akt. 2005-02-27 [cit. 2009-05-02]. Dostupný z WWW: <http://www.security-portal.cz/clanky/kdo-je-hacker>.

14. *KTD – Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. [cit. 2009–04-20]. Dostupný z WWW: <http://www.nkp.cz>.

15. MENTOR. *1986 - Hackerův manifest.* Britské listy [online] Akt. 2003-07-07 [cit. 06-05-2009]. Dostupný z WWW:<http://www.blisty.cz/2003/7/7/art14662.html>.

16. MIKO, Karel. *Nebezpečí zvané hacking*. In Business World [online] 2003-08-01. [cit. 2009-05-10]. Dostupný z WWW:<http://www.businessworld.cz>.

17. NAIK, Dilip C. *Internet: Standardy a protokoly.* Brno : Computer Press, 1999. 302 s. ISBN 80-7226-146-0.

18. Netiketa. *hoax.cz* [online] Akt. 2009 [cit. 2009-05-20]. Dostupný z WWW: <http://www.hoax.cz/hoax/netiketa>.

19. PETERKA, Jiří. *Stalo se: český Senát chce zakázat (stránkované) porno.* In Lupa.cz [online].[cit. 05-05-2009]. Dostupný z WWW: <http://www.lupa.cz/clanky/stalo-se-cesky-senat-chce-zakazat-porno/>.

20. SKLENÁK, Vilém; et. al. *Data, informace, znalosti a Internet.* Praha: C.H. Beck, 2001. 507 s. ISBN 80-7179-409-0.

21. Spam. In Wikipedie: Otevřená encyklopedie. c2008. Datum poslední revize 19.4.2009 [cit. 20.5.2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Spam>.

22. The Jargon File, version 4.4.7. *The Jargon File, version 4.4.7* [online] Akt. 2003-12-01 [cit. 2009-05-14]. Dostupný z WWW :< http://catb.org/jargon/>.

23. ZYCHOVÁ, Barbora. *Být či nebýt na Facebooku?* In Lupa.cz [online]. Akt. 2008-12-03. [cit. 2009-05-05] Dostupný z WWW:<http://www.lupa.cz/clanky/byt-ci-nebyt-na-facebooku/>.

Evidence výpůjček:

Prohlášení:
Dávám svolení k půjčování této bakalářské práce. Uživatel potvrzuje svým podpisem, že bude tuto práci řádně citovat v seznamu použité literatury.

V Praze 24. května 2009

Martin Kubelka

Jméno	Katedra / Pracoviště	Datum	Podpis
