Mezinárodní spolupráce při potírání počítačové kriminality

Bc. Vladimír Stojaspal

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Vladimír Stojaspal**
Osobní číslo:	**A13590**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Mezinárodní spolupráce při potírání počítačové kriminality**
Téma anglicky:	**International Cooperation in Combating Cyber Crime**

Zásady pro vypracování:

1. **Zpracujte rešerši literatury, která se vztahuje k aktuálním otázkám trendů mezinárodní spolupráce při potírání počítačové kriminality.**
2. **V rámci východiskové hypotézy vymezte fenomenologické a etiologické otázky spojené s vývojem mezinárodní spolupráce při potírání počítačové kriminality, včetně souvisejících právních aspektů a historických souvislostí.**
3. **Analyzujte současnou dynamiku počítačové kriminality, kontrolní a preventivní postupy včetně institucionálního zakotvení příslušných institucí, které se těmto aktivitám věnují, případně mají věnovat (bezpečnostní politika státu).**
4. **Zpracujte metodiku výzkumné části kvalifikační práce. Realizujte kvantitativní výzkum prostřednictvím dotazníkové metody.**
5. **Tvůrčí část diplomové práce zaměřte na syntézu – vycházejte ze specifikace analytických závěrů a výstupů, prezentujte vlastní návrhy a doporučení, která mohou nalézt uplatnění v bezpečnostní praxi.**
6. **Výstupy výzkumu a analytické části kvalifikační práce statisticky vyhodnoťte a zpracujte pomocí statistických metod do grafů a tabulek.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **KŘÍŽ, Zdeněk. 12. kongres OSN o prevenci kriminality a trestní justici: Salvador, Brazílie, 12.–19. dubna 2010, Praha: Institut pro kriminologii a sociální prevenci, 2010, 185 s. Prameny (Institut pro kriminologii a sociální prevenci). ISBN 978-807-3381-028.**
2. **MAŠTALKA, Jiří. Osobní údaje, právo a my. Vyd. 1. Praha : Beck, 2008. 212 s. ISBN 978-80-7400-033-1.**
3. **MATOUŠOVÁ, Miroslava; HEJLÍK, Ladislav. Osobní údaje a jejich ochrana. 2., dopl. a aktualiz. vyd. Praha : ASPI, 2008. 455 s. ISBN 978-80-7357-322-5.**
4. **NETOPILÍK, Petr. Realizace mezinárodní ochrany v ČR. Institut mezioborových studií, 2008. Bakalářská. UTB. Vedoucí práce Kejdová Miroslava.**
5. **PIKNA, Bohumil. Evropský prostor svobody, bezpečnosti a práva (prizmatem Lisabonské smlouvy). 3. rozš. vyd. Praha: Linde, 2012, 435 s. ISBN 978-80-7201-889-5.**
6. **Právní předpisy a jiné akty. Interinstitucionální spis: 2011/0166 (NLE), Brusel 12. září 2011, 12196/2/11 REV 2 (cs)**
7. **Sdělení komise Evropskému parlamentu, Radě a Evropskému výboru regionů k obecné politice v boji proti počítačové kriminalitě.**
8. **VESECKÁ, R., CHROMÝ, J. Kriminalita, veřejnost a media. Praha: Linde Praha, 2009. 125 s. 11-21 s. ISBN 978-80-7201-772-0.**

Vedoucí diplomové práce:	**PhDr. Mgr. Stanislav Zelinka** Ústav bezpečnostního inženýrství
Datum zadání diplomové práce:	**7. února 2014**
Termín odevzdání diplomové práce:	**27. května 2014**

Ve Zlíně dne 7. února 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl jsem seznámen s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

ABSTRAKT

Tato práce řeší problematiku mezinárodní spolupráce při potírání počítačové kriminality, její projevy, aktuální mezinárodní smlouvy a organizace, které se této problematiky přímo dotýkají. V práci budou též klasifikovány právní delikty spadající pod tuto problematiku. Praktická část diplomové práce bude zahrnovat rozbor Úmluvy Rady Evropy o počítačové kriminalitě a dotazník se zaměřením na rizika internetu a informovanost respondentů v oblasti počítačové kriminality.

Klíčová slova: mezinárodní spolupráce, kyberprostor, počítačová kriminalita

ABSTRACT

This thesis addresses the issue of international cooperation in combating cybercrime, its manifestations, current international agreements and organizations that directly affect this issue. In this thesis will also be classified legal offenses that deal with this issue. The practical part will include analysis of the Council of Europe Convention on Cybercrime and a questionnaire focusing on the risks of the Internet and awareness of respondents in cybercrime.

Keywords: International cooperation, The cyberspace, Cybercrime

Rád bych touto cestou poděkoval panu PhDr. Mgr. Stanislavovi Zelinkovi za trpělivost a čas, který věnoval vedení mé diplomové práce a mé manželce Kláře Stojaspalové za podporu a pevné nervy v době, kdy jsem tuto práci psal.

OBSAH

ÚVOD

V dnešním civilizovaném světě si život bez internetu a moderních technologií dokáže představit asi jen málokdo. Ale málokdo si dokáže uvědomit, jaká nová kriminální odvětví a technologie se tímto příchodem otevřely. Přínos těchto technologií má samozřejmě svůj každodenní vliv na rozhodovací schopnosti každého z nás a stal se standardem doby, ve které žijeme. Na tuto změnu musel reagovat jednak stát jako vymahatel pořádku a spravedlnosti, jednak celá mezinárodní scéna, neboť nové typy kriminálního jednání se musely rychle kriminalizovat a musela přijít protiopatření, aby se těmto útokům a hrozbám co možná nejvíce zabránilo a v co možná nejvyšší míře se jí dalo pomocí státních orgánů bránit. Při zásadních změnách v dnešní době, které způsobila digitalizace a konvergence pokračující globalizací počítačových sítí, jsou státy přesvědčeny o potřebě prioritního uskutečňování společné trestní politiky zaměřené na ochranu společnosti proti počítačové kriminalitě, zvláště pak přijetím příslušných právních předpisů a budováním mezinárodní spolupráce na maximální úrovni.

Politická scéna uznává spolupráci mezi státy a soukromými podnikateli při potírání počítačové kriminality a potřebu chránit legitimní zájmy při používání a rozvoji informačních technologií, neboť obecně počítačová kriminalita představuje obrovskou množinu všech aktivit, které jsou spojeny s počítačem jako nástrojem a s počítačem jako cílem trestné činnosti. Informační technologie zasahují do řady oblastí lidské činnosti, tedy i trestné činy od krádeží peněz po počítačové pirátství jsou obsaženy ve více sférách, proto nemůže ani proti počítačové kriminalitě existovat jednotný způsob boje.

Počítačová kriminalita se může jevit jako lehčí forma trestné činnosti pro člověka, který se v moderních technologiích dobře neorientuje, protože se většinou nejedná o odcizení movité věci. Nicméně i jedna elektronická součástka může obsahovat údaje o nové technologii, které mohou mít hodnotu několika milionů korun, přestože se nám to může jevit zcela nelogické.

Téměř všechny formy počítačové kriminality lze zařadit do již vniklých kategorií. Je tedy spíše nutné rozšiřovat kvalifikaci stávajících odborníků, než vytvářet nové struktury úzce profilované pro malou část kriminality, a to i v mezinárodním měřítku.

I. TEORETICKÁ ČÁST

1 PODLED DO HISTORIE

1.1 „Kyberprostor“

Když se v roce 1968 poprvé uskutečnilo v univerzitním prostření síťové propojení mezi čtyřmi počítači, došlo tím k položení základního stavebního kamene jedné z nejdůležitějších událostí moderních dějin v informačních a telekomunikačních systémech – ke zrodu sítě ARPANET. Nikdo si ani nedokázal představit, jak výrazný milník historie se v té chvíli odehrává a jaký bude mít dopad na každého z nás ve 21. století. Při vzniku dnes nejrozsáhlejšího komunikačního protokolu TCP/IP nebylo počítáno s tím, že se rozšíří do tak velkého prostoru a v takové míře jako je tomu nyní, proto nebyl kladen důraz na bezpečnostní charakteristiky sítí a protokolů.

Nicméně rychlost rozvoje technologií pokračovala mílovými kroky kupředu a jejich slabiny se staly cílem nelegálních aktivit. Vztah k elektronice a informačním systémům z historického hlediska nebyl tak pochopitelný jako v současnosti. Společnost nebyla zvyklá na tak rychlý rozvoj, tudíž reagovala se zpožděním. V globálním měřítku se historie kyberprostoru odehrála v druhé polovině minulého století. Vzhledem k rychlosti rozvoje je pochopitelné, že lidská společnost začala za postupem technologie zaostávat.

Pojem kyberprostor se na světlo světa dostal díky kyberpunkovému spisovateli Williamu Gibsonovi, který jej použil ve svém prvním románu nazvaném Neuromancer (1992). V tomto díle přiblížil svou vizi globální počítačové sítě, jež bude schopná propojit celý svět, stroje i informační zdroje. Prostor v tomto románu má velké ambice, neboť popisuje člověka připojeného do virtuálního prostředí, kde se nachází barvitý svět – Kyberprostor.

Síťový uživatel si uvědomuje to, čeho si mohli být vědomi uživatelé telefonické či telegrafické sítě. Počítačová síť není pouze zapojení počítačů a síťových zařízení, které slouží k přenosu dat a informací nebo sdílení dat pomocí „peer to peer“ rozhraní, ale je to něco víc.

Bruce Sterling definuje kyberprostor na tom, co bylo v tehdejší době zcela běžné – na telefonní síti: *„Kyberprostor je „místo“, kde se telefonní hovory stávají běžnými. Není to uvnitř tvého telefonu, plastickém zařízení na tvém stole. Není to uvnitř telefonu druhého účastníka, v jiném městě. Je to místo mezi telefony. Nedefinovatelné místo kdesi venku, kdesi tam, kde se dvě lidské bytosti setkávají a spolu komunikují.“*[13]

1.2 Počítačová kriminalita

Počítačová kriminalita je pojena se vznikem informačních a telekomunikačních systémů, zrodila se tedy v padesátých letech minulého století. Stav tehdejší techniky a jejího využití limitoval i možnosti zločinců. S historií (s trochou nadsázky můžeme říct i s budoucností) nás pojí jedno pojmenování – hacker. Toto označení vystihuje technicky vyspělého a šikovného jedince, který je schopen najít metody a prostředky pro překonání bezpečnostních pojistek v daném systému. Nicméně v minulosti tento pojem znamenal člověka, jenž dokáže zvýšit výkon svého radiovysílače.

Za pravý start počítačové kriminality můžeme považovat rok 1981, kdy vstoupil do prodeje osobní počítač. Největší rozvoj nastal hned v osmdesátých letech a s ním technologie zvaná BBS, tedy počítače, které uměly komunikovat s databází a s informacemi uloženými pomocí standardizovaných dotazů. To zapříčinilo vznik hackerských spolků a skupin, které s daty manipulovaly a dělily se s ostatními. Převážně se jednalo o hesla a bankovní účetnictví. Příkladem je případ Národní banky v Chicagu v USA, která po hackerském útoku přišla o 50 mil. dolarů. [12,24]

1.2.1 Počítačová kriminalita v ČR

Z důvodu politické situace v tehdejší ČSSR se do konce osmdesátých let minulého století o počítačové kriminalitě nedá ani polemizovat, neboť informační technologie patřily v té době do embargovaného zboží. Změna byla zaznamenána na přelomu devadesátých let, kdy se k nám začaly první počítačové sestavy pašovat. Mezi počáteční uznané případy patří zpronevěra spáchaná použitím počítače v zásilkové službě MAGNET, a to pracovnicí, jež měnila status objednávek z „nezaplaceno“ na „zaplaceno“ bez přijaté peněžní částky. Dle dřívějších zákonů se jednalo o porušení §132 trestního zákoníku – o rozkrádání majetku v socialistickém vlastnictví. Dnes by se jednalo o podvod nebo zpronevěru.

Zde jako historický mezník musíme uvést datum 13. 2. 1992, tedy den, kdy byla Česká a Slovenská Federativní Republika oficiálně připojena k internetu. V nadcházejících letech se na trhu začínají objevovat počítače s relativně výkonnou sestavou pro dané časové období, s operačním systémem Microsoft Windows a s nimi i významný nárůst počítačové kriminality. Z událostí za posledních 20 let se kromě pirátství, phishingu, pharmingu, sociálního inženýrství, padělání či šíření dětské pornografie začínají rozmáhat nové druhy a

formy počítačové kriminality jako kyberšikana, sexting nebo také sociální sítě, které významně přispívají k rozmachu tohoto problému. Reakcí na přibývající problémy bylo vytvoření zákonů a mezinárodních smluv, které určovaly, jakým směrem se bude kyberprostor monitorovat a jaké budou následovat postihy za nedovolené překračování těchto zákonů.[15,21]

Pravděpodobně nejznámějším aktem počítačové kriminality u nás se stal útok na CitiBank provedený pomocí phishingu, což bylo poprvé, co se tato metoda použila v ČR a v českém jazyce.

1.2.2 Útok na CitiBank

Phishingový útok (samotný druh útoku je definován níže v samostatné kapitole) započal na české emailové schránky 3. 2. 2006, kdy byla ze serveru „ppp-70-225-132-196.dsl.ipltin.ameritech.net“ odeslána emailová zpráva, která na první pohled vypadala jako oficiální zpráva ze strany CitiBank, o pohybu určité peněžní částky na příjemcův účet. Pro potvrzení se bylo potřeba přihlásit do prostředí internetového bankovnictví přes přiložený odkaz, jež směřoval na přihlašovací obrazovku internetového bankovnictví, která se téměř detailně podobala oficiálním stránkám.


Od: Citibank Online [alerts@citibank.cz]
Komu: Petr Nadenicek
Kopie:
Předmět: Important notice: Confirm Payment

citibank

Serial EM202-16

Vážený kliente Citibank Online®,

03/02/2006 na Váš běžný účet byl přijat převod v cizí měně na částku ve výši 2000 . Se shodou s *spotřebitelským souhlasem CitiBank® online*, je potřeba potvrdit tento převod pro jeho úspěšné zařazení na Váš běžný účet.

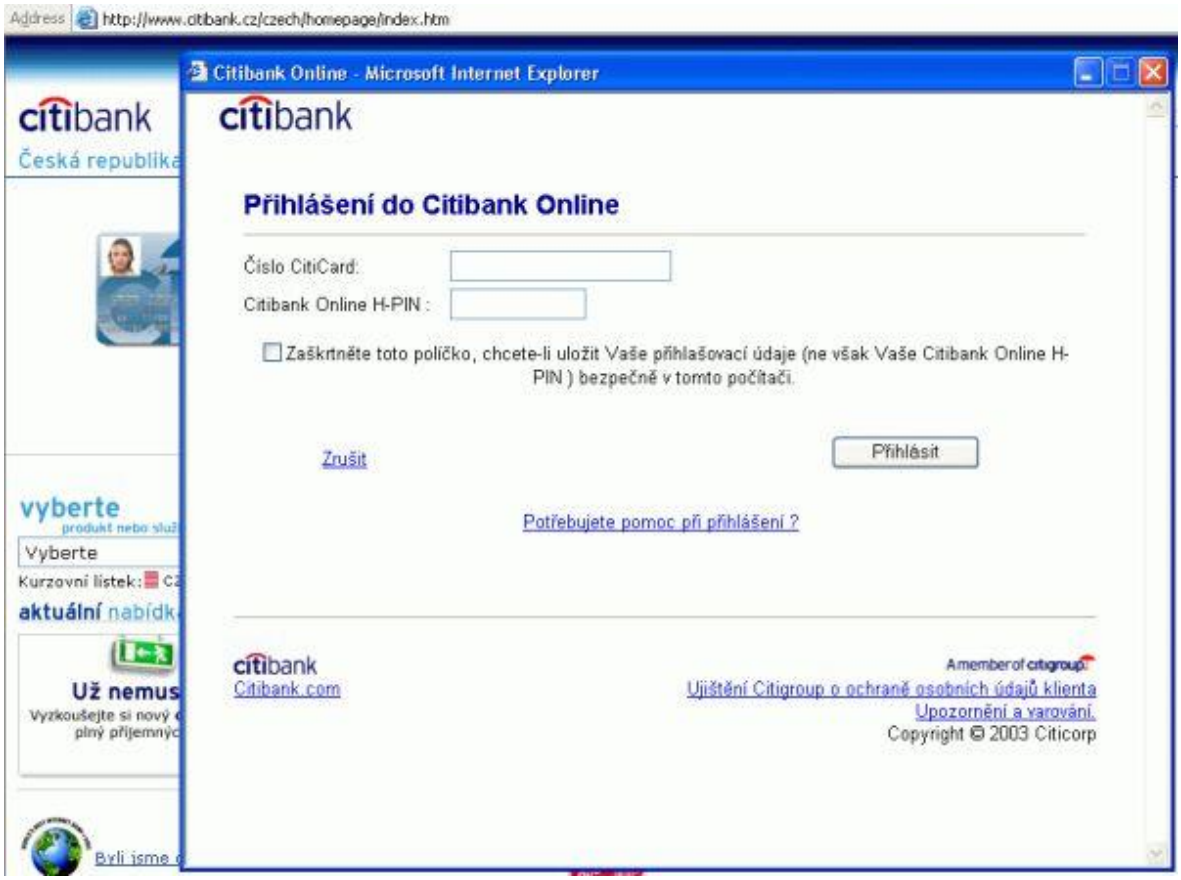
Pro potvrzení platby Vás prosím o návštěvu programu ovládání Vaším účtem CitiBank® online a dále postupujte podle předloženého návodu. V případě nepřijetí potvrzení v průběhu 48 hodin, bude částka vracena odesílateli.

Pro vstup do programu CitiBank® online, **klikněte sem** >>>

S pozdravem
Služba CitiBank® Alerting Service

Obr. 1 – Podvodný email

Text tohoto falešného emailu byl vytvořen na základě sociálního inženýrství. Člověk, který vlastní běžný účet u této banky a nemá osvojenou problematiku počítačové kriminality, ztratí ostražitost a může podlehnout. Následky tohoto činu jsou potom fatální. [23]



Obr. 2 – Přihlašovací nabídka z odkazu v emailu

1.3 Aktuální útoky

Aktuální útoky se od těch starších moc neliší, jedná se většinou o učebnicovou ukázku phishingu. Následující příklad popisuje „pokus“ o získání osobních údajů či finančních prostředků, v němž se útočník vydává za skupinu *Poisťovňa Genertel,* a to jako partner Generali Group. Emailová zpráva obsahuje podobné prvky, které používá pojišťovna Generali, útočník vystupuje pod podobným jménem, aby mohl zmást uživatele, a láká na výhru v určitém finančním obnosu.

odesílatel: **Poisťovňa Generteľ** <novinky@genertel.sk>
adresa pro odpověď: novinky@genertel.sk
komu: lada.stojaspal@seznam.cz
datum: 28. dubna 2014 11:31
předmět: Vladimír Stojaspal 150 € na nákup pre Vás
posíláno přes: seznam.cz
podepsáno od: seznam.cz

Dobrý deň **Vladimír Stojaspal**, získajte **nákup zadarmo!**

Zaujíma nás Váš názor. Preto ak odpoviete na pár jednoduchých otázok, môžete vyhrať **jeden z troch nákupov v sieti Kika v hodnote až 150 €.**

Ďakujeme za Vašu pomoc.

Tim Genertel

Áno, chcem vám pomôcť
a hrať o 150 € na nákup v Kika

Viac informácií nájdete na genertel.sk

Telefón: 0850 555 555
Web: www.genertel.sk
V prípade otázok nás neváhajte kontaktovať.

GENERALI Sme členom renomovanej skupiny Generali Group

Obr. 3 – Printscreen emailu autora práce

1.4 Mezinárodní smlouvy

Obecná mezinárodní politika neukládá zvláštní závazky státům v oblasti výkonu jejich trestní pravomoci. Stát tedy může stíhat jakýkoliv čin, ale může také ponechat činy jinak trestné páchané na území jiného státu bez trestu podle svého práva.

Státy převzaly některé specifické povinnosti k mezinárodní spolupráci kolektivními smlouvami (potírání zločinnosti přesahující státní hranice), které nemohou být účinně postiženy právě bez mezinárodní spolupráce: trestání i činů nespáchaných na jejich území, vydávání pachatele k potrestání, neudělování azylu, spolupráce výměnou informací a součinností policie k rychlejšímu a efektivnějšímu potírání otroctví, obchodu s bílým masem, pornografie, teroristických činů válečných zločinů, zločinů proti míru a lidskosti, zločinů rasové diskriminace a počítačové kriminality.

1.4.1 Přehled důležitých mezinárodních smluv:

- 1949 – dokument o vytvoření Rady Evropy, jejímiž představiteli jsou Belgie, Dánsko, Francie, Irsko, Itálie, Lucembursko, Nizozemsko, Norsko, Švédsko a Velká Británie
    - 1993 - Česká Republika se stává členem
- Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců se zřetelem na zpracování osobních dat a o volném pohybu těchto dat
- Nařízení Evropského parlamentu a Rady 97/66/EC ze dne 15. prosince 1997 vztahující se k nakládání s osobními údaji a k ochraně soukromí v telekomunikačním sektoru
- Rozhodnutí Evropského parlamentu ze dne 19. května 2000 k legislativní akci proti zločinu za použití vyspělých technologií
- Nejaktuálněji se určitým aspektům boje proti kybernetickým incidentům věnuje Rezoluce Rady bezpečnosti OSN č. 1624 ze dne 14. září 2005, která zavazuje členy Organizace k zákazu podněcování páchání aktů terorismu.
- Akční plán pro Bezpečnější Internet (Safer Internet Action Plan) pro roky 1999 – 2004 a na něj navazující materiál – Bezpečnější Internet plus (Safer Internet plus) pro roky 2005 – 2008, a to v rámci EU[10,19,22]

2 POČÍTAČOVÁ KRIMINALITA

Vymezit pojem počítačová kriminalita není tak snadné. Jeho význam se neustále v naší společnosti mění podle toho, v jakém stylu byl spáchán trestný čin či přestupek vzhledem k trestnímu zákoníku. Samotný výraz můžeme označit jako „terminus technicus“, jímž je označována skupina trestních činů, které mají pojící charakter. Dokud nebyla vytvořena obecná definice počítačové kriminality, často se používaly zaměnitelné pojmy:

- počítačová trestná činnost,
- trestná činnost v oblasti výpočetní techniky,
- trestná činnost páchaná s využitím špičkové techniky.

2.1 Definice

Pro přesnější vyjádření pojmu tedy vznikla definice, která říká, že počítačová kriminalita zahrnuje trestné činy spáchané s použitím elektronických komunikačních sítí a informačních systémů či trestné činy spáchané proti takovýmto sítím a systémům. Pro účely této práce tedy musí být také definovány pojmy „počítačový systém“ a „počítačová data“.

- **Počítačový systém**
  - je jakékoli zařízení nebo skupina zařízení, které jsou vzájemně propojeny, z nichž jedno nebo více zařízení provádí automatické zpracování dat podle programu.
- **Počítačová data**
  - jsou jakékoli informace, vyjádření faktu či pojmu ve formě vhodné pro zpracování v počítačovém systému s programy, které jsou způsobilé zapříčinit provedení funkce počítačovým systémem.

Z obecnějšího hlediska pojem počítačová kriminalita zabírá mnoho obecných deliktů ve smyslu porušení platné právní zákonné úpravy.

Velké množství definic se shoduje v tom, že je třeba rozdělit základní kategorie počítačové kriminality na několik stupňů.

2.2 Klasifikace

Pojem počítačová kriminalita se vztahuje na tři kategorie trestné činnosti.

- **Tradiční formy kriminality**

  - Na tomto prvním stupni se jedná o protiprávní jednání, v němž je počítač přímým cílem útoku – většinou se tedy jedná o server, který má na starosti počítačovou síť. Útok je pak směřován na odcizení dat, průmyslovou špionáž, padělání nebo krádež totožnosti.

- **Zveřejňování nezákonného obsahu**
  - Druhý stupeň můžeme naplnit skutky, které reprezentují protiprávní jednání vykonané s použitím informačních technologií, při nichž počítač slouží jako nástroj k trestné činnosti – zde máme na mysli porušování autorských práv, materiál týkající se pohlavního zneužívání dětí (dětská pornografie) či materiály podněcující rasovou nenávist.
- **Trestné činy postihující výlučně elektronické sítě**
  - Třetí stupeň zahrnuje napadání informačního systému útoky typu DOS a hackingu. Tyto útoky mohou být také cílené na kritickou infrastrukturu a mohou ovlivňovat systémy rychlého varování, což by mělo katastrofální následky pro celou společnost.

Z obecného hlediska můžeme útoky rozdělit na:

- útoky úmyslné proti vlastnímu nosiči informací, datům umístěným na něm s úmyslem jej zničit,
- obohacování se pomocí:
  - krádeží dat a programů,
  - krádeží strojového času,
- nezákonná manipulace s počítači, programy a daty. [20,26]

3 VZTAH MEZINÁRODNÍCH ORGANIZACÍ K POČÍTAČOVÉ KRIMINALITĚ

3.1 Evropská unie (EU)

Během činnosti EU byla vydána velká řada dokumentů, které souvisejí s problematikou počítačové kriminality, v jejímž rámci je EU už od svého vzniku koncipována, a to je třeba zdůraznit, jako bezpečnostní agenda. Za svůj cíl si klade zkvalitňovat bezpečnost informační infrastruktury z hlediska boje proti počítačové kriminalitě a povzbuzovat rozvoj členských států v kybernetickém prostoru a průmyslu. Další hlavní prvky boje, na které se EU dívá a snaží se je rozvíjet:

- zajištění bezpečného používání internetu jako zdroje informací a dalších technologií pro dálkový přístup k počítačovým systémům,
- pomoc v boji proti nelegálnímu obsahu na internetu se zaměřením na zvlášť nebezpečný obsah, který by mohl znamenat újmu dětem a mladictvím,
- snaha vytvářet a následně rozvíjet bezpečné prostředí – vytvoření jakéhosi etického kodexu – sepisování pomyslných černých listin subjektů, které odmítly spolupracovat.

Evropská unie vlastní další řadu dokumentů, které se týkají aktivit zaměřených na rozvoj informovanosti unijní společnosti. Jedná se o následující dokumenty:

- Usnesení Rady Evropské unie k Strategii pro bezpečnou informační společnost,
- řada Akčních plánů členských zemí, a to od roku 2002 – 2005.

3.1.1 Akční plány členských zemí eEuropa 2002 – 2005, kandidátské země 2003

Česká republika se připojila do těchto akčních plánů v roce 2001, konkrétně do balíčku eEurope+ 2003, čímž se zavázala v rámci kandidátských zemí EU právě k rozvoji ICT. Samotné plány zdůrazňují velkou důležitost bezpečnosti ICT technologií, zejména počítačových sítí, a boje proti počítačové kriminalitě. Tyto plány byly koncipovány na zvýšení bezpečnosti informačních struktur, zajištění běhu orgánů zainteresovaných v činně trestném řízení a požadavek zachování základních lidských práv a svobod. Zmíněny jsou také potřeby zvýšení bezpečí pro uživatele internetu – lepší a dokonalejší antivirové programy, firewally, šifrovací protokoly nebo šifrování pomocí veřejného klíče, biometrická identifikace osob,

bezpečnější přístup do objektů, kde se nachází počítače a servery, které by mohly způsobit újmu vlastníkovi, či ověření osoby v digitální sféře – digitální podpisy a certifikace.

Poslední akční plán, který byl přijat v roce 2002 a byl určen členským zemím eEurope 2005, popisuje i otázku monitoringu komunikace, kontrolu a zajištění odesílaných dat, anonymní přístup, užití zdrojů a praktickou spolupráci na mezinárodní úrovni. Dále uvádí, jakým způsobem se bude udávat hodnota počítačových dat v důkazním řízení, upravuje společná pravidla pro komunikační protokoly a věnuje se otázkám speciálního výcviku osob v této problematice.

3.1.2 ENISA

V roce 2004 spustila EU program Evropská agentura pro síťovou a informační bezpečnost na poskytování odborných informací a odborného poradenství pro komisi a členské státy Evropské unie, a to při vytváření informační bezpečnosti a při vyjednávání se zástupci soukromých průmyslových společností ve věci informační bezpečnosti. Mezi hlavní cíle patří:

- sběr a analýza dat, které souvisí s bezpečnostními incidenty v Evropě a z toho vyplývajícími riziky,
- zajišťování kooperace mezi veřejně-soukromým partnerstvím na poli ICT
- zvyšování schopnosti odolávat hrozbám v oblasti informační bezpečnosti.

Agentura získala mandát pouze do března roku 2011, ale během svého působení vypracovala rozsáhlou studii týkající se odolnosti a bezpečnosti informačních a bezpečnostních sítí.

Obr. 4 – Logo agentury ENISA

3.1.3 Projekt „Check the Web“

Obr. 5 – Logo projektu Check the Web

Projekt *Check the Web* je aktivitou EU v boji proti internetovému terorismu. Vznikl na základech, které položilo Německo ve svých plánech, jež chtělo realizovat během předsednictví Unie.

„Je konstatováno, že je bezmála nemožné, aby jeden každý členský stát Unie samostatně monitoroval všechny podezřelé a potencionálně nebezpečné aktivity, ke kterým v rámci Internetu dochází. Proto je více než žádoucí sdílet takové břemeno v rámci všech členských států Unie. Projekt je proto chápán jako nástroj pro vytvoření funkční dělby práce v uvedené oblasti, která by následně usnadnila postup proti nelegálnímu obsahu na internetu.“[14]

Aktuálně hlavní priority projektu jsou:

- zvýšení technických a jazykových dovedností nutných k porozumění získaných údajů,
- spolupráce zainteresovaných stran a vytvoření takového prostředí, ve kterém by bylo možné pružně analyzovat data – analýza konkrétních internetových stánek, sociálních sítí
- potírání obsahu, který může vést ke vzniku nebezpečných situací a výrobě domácích zbraní,
- pro potřeby Europolu vytváření hlášení na základě dosažených informací a zpráv od jednotlivých zemí, které by byly využitelné v rámci celé EU,
- společný postup proti nelegálnímu obsahu na internetu.

Postup realizace tohoto projektu spočívá na řadě dílčích kroků, jejichž splnění je dáno v určitém časovém intervalu. V prvním kroku by měly být stanoveny kontaktní sítě – skládají se z kontaktních bodů, které oznámí členské státy. Tyto body budou zodpovědné za navazující komunikaci a koordinaci konkrétní aktivity. Vytvoří je experti a zainteresované strany z řad technických a metodických odvětví prostřednictvím uspořádání semináře. Další krok

spočívá ve výměně informací o aktuálním personálním a technickém vybavení v zainteresované zemi Unie a zjištění regionálních aktivit a priorit jednotlivých zemí v uvedené oblasti.

Jedním ze stěžejních bodů v postupu proti nelegálnímu obsahu na internetu v projektu Check the Web je společný přístup k informacím, jejich výměna a aktualizace hlavně v zákonných možnostech jednotlivých členských států při blokování či zamezování přístupu na webové stránky s nelegálním obsahem. Dalším předpokladem je spolupráce s providery v jednotlivých zemích.

K tomuto projektu přispělo v roce 2008 také předsednictví Francie, které poukazovalo na to, že základem je zejména úsilí členských států o vytvoření jednotné (unijní) platformy pro nahlašování a potírání nelegálního a nežádoucího obsahu na internetových stránkách.

Nemůžeme nechat bez povšimnutí ani snahu vytvořit vazbu mezi ohrožením ze strany terorismu a hospodářským rozvojem Unie. Generální ředitelství a jeho experti z pracovní skupiny k problematice elektronického obchodu důrazně vyzývají k přijetí náležitých opatření, které by radikálně zamezily přístup a rekrutování do teroristických skupin prostřednictvím internetu. Na tento problém Unie zareagovala následovně. Členské státy Unie mohou, v případě, že si to vyžádá určitý veřejný zájem, omezit internetové služby – tím se myslí odstranění jejího obsahu – provozované z území jiného členského státu, užít sankcí nebo zahájit vyšetřování vůči tomuto poskytovateli. Určitý veřejný zájem je zde výslovně určen jako boj proti jakémukoli podněcování k nenávisti na základě rasy, náboženství, pohlaví či národnosti, taktéž jako činy neslučující se s lidskou důstojností.

3.1.4 Projekt „CI2RCO“

Critical Information Infrastructure Research Co-ordination, tedy Koordinace výzkumu v oblasti kritické informační infrastruktury, je název projektu, který byl spuštěn v březnu roku 2005. Věnuje se určitým aspektům kybernetické bezpečnosti a jeho hlavním úkolem je vytvoření a koordinace unijních úkolů s cílem zabezpečit evropský přístup ve výzkumu a vývoji kritické informační infrastruktury. Vzhledem k této souvislosti je mapován potenciál již existujících organizací, jež se příslušnou problematikou zabývají – dosavadní výsledky, hospodaření organizace, transparentnost, atd. Po prozkoumání všech zjištěných skutečností bude navrženo vytvoření „Unijní sítě pro výzkum a vývoj“, která poslouží pro vytvoření vazeb mezi zainteresovanými institucemi, budou uspořádána pracovní setkání zástupců vybraných institucí se záměrem inovovat podporu výměny informací z výsledků

prací a také se bude podporovat její činnost ustanovením internetového portálu, kde budou sdíleny získané výstupy.

Pro účastníky projektu se přepokládá vytvoření rady, která bude v rámci celé EU koordinovat projekty z oblasti vědy a výzkumu, dále zajišťovat výměnu informací v prostoru Evropských zemí a připravovat zprávy pro Komisi Evropské unie.

Evropská unie v oblasti ochrany kyberprostoru všeobecně zaostává za Spojenými státy americkými a zmíněný rozestup se stále zvětšuje. Tento efekt je způsoben tím, že se Unie rozhodla vydat se „vlastní cestou“ v boji proti počítačové kriminalitě a terorismu, jelikož klade větší důraz na ochranu základních lidských práv na rozdíl od postupu USA. Jako příklad uvádíme debaty z konce 20. století, jež proběhly v Evropském parlamentu, o nutnosti monitorování systému ECHELON provozovaném bezpečnostním úřadem v USA. Aktuální priority EU v uvedené oblasti můžeme plošně zobecnit do těchto bodů:

- vytvoření statistického pohledu na celou problematiku – tématem se věnuje systém Eurobarometer – klade veřejnosti řadu otázek v požadavcích ochrany kyberprostoru,
- vytvoření a šíření etického kodexu pro poskytovatele internetových služeb, a tím dosažení pokroku samoregulace,
- zvýšení prevence na veřejných místech, jako jsou školy, rodiny, mládežnické organizace, s cílem odhalit nástrahy internetu a přispět bdělosti před nástrahami kybernetických rizik,
- vytvoření horkých linek – trvalé mechanismy, jejichž prostřednictvím bude možné nahlásit nelegální obsah na internetu,
- snaha bojovat proti porušování autorských práv,
- zvýšení úsilí o spolupráci mezi nejvíce zainteresovanými stranami v oblasti boje proti počítačové kriminalitě,
- rozvoj spolupráce mezi státními a soukromími subjekty a zapojení nevládního neziskového sektoru,
- zapojování akademických obcí, v nichž je prováděn aplikovaný výzkum v zájmových oblastech,
- hledání nových technických řešení v boji proti počítačové kriminalitě,
- aktivity v oblastech sběru a analýzy dat z kybernetických incidentů a možných ohrožení, které z nich plynou,

- boj proti škodlivému a nežádoucímu obsahu na internetu, hledání postoje k nežádoucímu obsahu.

Při tom všem je třeba znovu zdůraznit, že EU stále zaostává za zaoceánskými kolegy z USA. Vláda USA – kongres – i občané sdílí s evropskou strukturou určité klíčové informace a technologie, ale nikdo nemůže zaručit, že Spojené státy budou i nadále velkoryse sdílet své technologicko-organizační výsledky v řešené problematice. Zároveň je zřejmé, že se bude prohlubovat technologická závislost na USA. Co se sdílení informací týče, případné ochlazení vztahů s USA by pro Evropu znamenalo nemalé komplikace ve snaze držet krok se světovými trendy.

Při pohledu na Českou republiku a její pozici v EU jako novějšího členského státu je jednodušší žádat o prostředky na nákup zařízení než vynakládat prostředky na vlastní aplikovaný výzkum v oblasti kybernetické bezpečnosti. Ochrana kyberprostoru však v ČR není vázána pouze na EU, ale usiluje se i o to, aby byla zajištěna přímá bilaterální spolupráce s jinými zeměmi (Japonsko, USA) i vlastní výzkum, jenž podpoří domácí ekonomiku.

3.2 Organizace spojených národů (OSN)

Udržování mezinárodního míru a bezpečnosti je jedním z hlavního úkolu OSN od jejího samotného počátku. Organizace od svého vzniku pomohla již několikrát zabránit válečným konfliktům, snaží se také regulovat míru kriminality v kyberprostoru. Potírání počítačové kriminality v dnešní době se řídí zejména předpisem Rezoluce Rady Bezpečnosti OSN č. 1624 ze dne 14. září 2005, která zavazuje členy k zákazu podněcování páchání aktů terorismu a dalších aktů proti lidskosti. Text vyzývá k přijetí nezbytných opatření na vnitrostátní úrovni:

- zákonem zakázat nabádání a obhajobu terorismu (taková aktivita nemůže být chápána jako naplňování práva na svobodu vyjadřování),
- provádět preventivní kroky v uvedené oblasti,
- provozovat výměnu informací a zkušeností souvisejících s násilím,
- podávat Radě Bezpečnosti zprávy o implementaci Rezoluce.

3.3 Rada Evropy

Rada Evropy projevila zájem o řešení problematiky počítačové kriminality koncem 80. let minulého století. V roce 1989 publikovala studii, která obsahovala doporučení pro

úpravy a vytváření nových zákonů v jednotlivých státech, určenou ke kriminalizaci činů spáchaných prostřednictvím počítačových sítí.

V následujících letech přišla další studie, která tentokrát obsahovala principy týkající se trestněprávního postupu souvisejícího s informačními a komunikačními technologiemi. V roce 1997 byla ustanovena skupina expertů proti zločinům v kyberprostoru. Výsledek její činnosti byl jasný: Úmluva o kyberzločinu (Convention on Cybercrime, ETS 185) přístupná od února 2005. K této úmluvě se mohou přidat i země, které nejsou členy Rady Evropy. ČR Úmluvu zatím nepodepsalo, s tímto krokem se počítá po implementaci skutkových podstat.

Úmluva patří mezi první mezinárodněprávní instrument, který je určen speciálně pro řešení problému mezinárodního vjemu s charakterem počítačového zločinu. Text požaduje, aby země, které Úmluvu podepíší, kriminalizovaly určitá jednání, jež je možné zařadit do oblasti počítačové kriminality, a aby tyto země přijaly normy umožňující postihovat takovéto protiprávní jednání.

V Úmluvě je také kriminalizován návod a napomáhání k takovým typům zločinů. Taktéž jsou uvedeny i principy a způsoby vzájemné pomoci mezi státy při vyšetřování počítačové kriminality včetně otázek vydání zadržovaných osob, jejich předání, zajištění dat a vytváření bodů pro nepřetržitý kontakt.

Další dokumenty Rady Evropy s tématy počítačové kriminality:

- Dodatkový protokol o kriminalizaci činů, spáchaných prostřednictvím počítačových sítích
- Doporučení Rady ministrů č. 13 roku 1995, týkající se trestního práva procesního
- Doporučení Rady ministrů č. 5 roku 1999, týkající se ochrany soukromí v počítačových sítích

3.4 INTERPOOL

INTERPOOL je největší policejní organizací na světě a jako mezinárodní a mezivládní organizace zabezpečuje policejní spolupráci v kriminální oblasti mezi smluvními státy. V současné době má 188 členských států. Je důležité zmínit, že INTERPOOL získal status stálého pozorovatele při OSN a funguje 24 hodin denně 365 dní v roce. Generální sekretariát sídlí ve francouzském Lyonu.

V souladu se statutem INTERPOOLu je hlavním zabezpečením spolupráce členských států v boji proti trestné činnosti při plném respektování priorit národního zákonodárství dané země a jejích závazků plynoucích z mezinárodních smluv. Využití INTERPOOLu v boji proti počítačové kriminalitě, podobně jako struktura Evropské Unie, je relativně všestranné. Prioritou je:

- boj proti počítačovým podvodům,
- boj proti hospodářské a finanční kriminalitě,
- vytvoření informačního systému o organizované počítačové kriminalitě,
- harmonizace právních předpisů.

INTERPOOL se stává globálním koordinačním orgánem pro detekci a prevenci digitálních zločinů prostřednictvím střediska INTERPOOL Global Complex for Inovations (IGCI), které se v současné době buduje v Singapuru. Klíčovým prvkem bude nové špičkové zařízení pro výzkum a vývoj. Bude zaměřeno na proaktivní výzkum nových oblastí a metod počítačové kriminality.

Harmonizace probíhá prosazováním práva jako základního prvku pro boj s digitálními hrozbami. Je třeba do ní zapojit všechny zúčastněné strany jak ze soukromého sektoru, tak z akademické sféry a veřejných institucí, kde pracují lidé na společných cílech za bezpečnějším kyberprostorem.

Mezi hlavní služby harmonizace patří:

- národní počítačová recenze
    - komplexní audit vnitrostátních právních předpisů, policejní infrastruktury a technických kapacit,
- vývoj kyberprostorové bezpečnostní strategie
    - práce s regulačními orgány, které se snaží vyvinout globální strategii a poradenství při prosazování práva.[8]

3.5 Organizace pro bezpečnost a spolupráci v Evropě (OBSE, OSCE)

Tato mezinárodní bezpečnostní organizace, která vznikla v roce 1995, a to transformací Konference o spolupráci v Evropě, sdružuje převážně evropské státy. Aktuální počet členských státu je 57, sídlo organizace leží ve Vídni v Rakousku.

Činnost OBSE můžeme roztřídit do tří aktivit. 1.) Otázka bezpečnosti a vojenské oblasti, která spadá do tzv. hard security, 2.) podpora ekonomického rozvoje, zajištění udržitelného rozvoje a 3.) podpora plného respektování základních lidských práv a svobod. Co se týká působnosti OBSE, můžeme říct, že organizace se aktivně zapojuje do těchto aktivit:

- správa hranic,
- boj proti terorismu,
- prevence konfliktů a jejich řešení,
- svoboda médií a jejich rozvoj,
- vzdělání,
- boj proti obchodu s lidmi,
- volby,
- lidská práva a rovnost pohlaví.

V kontextu s dokumenty Rady ministrů je klíčové rozhodnutí organizace „O boji proti používání internetu pro účely terorismu“, které vzešlo na popud ze zasedání se Sofií 17. 12. 2004 a které plynule navazuje na závěry konference, jež stejná organizace pořádala v červenci téhož roku k tématu souvislosti mezi zločiny z nenávisti a rasistickou xenofobní propagandou na internetu.

Obsah této konference byl důležitý zejména pro téma oprávněnosti převodu odpovědnosti za obsah internetových stránek z vlád na jejich poskytovatele. Jednotlivé členské země byly vyzvány k tomu, aby legislativní cestou vytyčily to, co považují za ilegální. Co není možné označit jako právně ilegální, by mělo být interpretováno jako využívání svobody slova. Na řadu přišla také prevence, jakožto důležitá součást vzdělání, zejména v oblasti zvyšování obecného povědomí o ohrožení ze strany kyberkriminality a kyberterorismu.[28]

3.6 Organizace pro hospodářskou spolupráci a rozvoj (OECD)

Posláním Organizace pro hospodářskou spolupráci a rozvoj je podporovat politickou situaci, která zlepší hospodářský a sociální blahobyt lidí po celém světě. Poskytuje fórum, na němž mohou vlády spolupracovat, vyměňovat si zkušenosti, hledat řešení společných problémů. Pracuje s vládami, aby pochopily, co pohání ekonomické, sociální a environmentální změny, měří produktivitu a globální tok obchodu a investic a v neposlední řadě analyzuje a porovnává data a budoucí trendy. Rovněž se dívá na problémy dnešní doby, které mají

přímý vliv na každodenní život. Organizace a její výbor pro informační, počítačovou a komunikační politiku, vydali v roce 2002 dokument „*Přehled: Bezpečnost informačních systémů a sítí: Směrem ke kultuře bezpečnosti*“. Text doporučuje členským státům tyto záležitosti:

- zřízení, posílení existujících zásad, praktik, opatřeních a postupů pro tuto tématiku; prostřednictvím jejího přijetí se prezentuje jako „kultura bezpečnosti“,
- koordinace postupu a spolupráce na národní a mezinárodní úrovni,
- šíření této ideje ve veřejném i soukromém sektoru,
- jednou za 5 let podání zprávy o plnění
    - popis toho, jak je v konkrétní zemi naplňována mezinárodní spolupráce v oblastech, které se vztahují k bezpečnosti informačních technologií a sítí.[28]

3.7 Severoatlantická obranná aliance (NATO)

Základním cílem Severoatlantické obranné aliance je ochrana svobody a bezpečnosti členských států politickými a vojenskými prostředky. NATO podporuje demokratické hodnoty a konzultuje o spolupráci v oblasti obrany a bezpečnosti, budování důvěry a v dlouhodobém horizontu předcházení konfliktů.

Z vojenského pohledu se NATO zavázalo k mírovému řešení sporů, pokud diplomatické snahy neselžou. Aliance má vojenskou kapacitu potřebnou k provedení krizového řízení operace. To je prováděno na základě 5. článku Washingtonské smlouvy – zakládající listina NATO, pod mandátem OSN nebo ve spolupráci s dalšími zeměmi a mezinárodními organizacemi.

NATO se řídí zásadou, že útok proti jedné či více členských zemí je považován za útok proti všem. To je princip kolektivní obrany, která je zakotvena v článku 5. Tento článek byl vyvolán pouze jednou, a to 9. 11. 2001 v reakci na teroristické útoky ve Spojených státech.

Kybernetická ochrana se stala součástí obranných kapacit v roce 2002, kdy bylo výboru NC3B uloženo, aby v rámci celé aliance prosadil adekvátní kybernetickou ochranu. V alianci již dříve vznikla asociace NOS – NATO Office of Security, která koordinuje dosahování schopností NATO a zaobírá se otázkou kybernetické ochrany. Kybernetickými útoky se zabývá Výbor pro plánování komunikací, který je k tomu stanovený v dokumentu EAPC(CCPC)D(2006)0002 z 2. února roku 2006. S tímto dokumentem souvisí také civilní

nouzové plánování, následky počítačové kriminality a informační zbraně na kritickou civilní infrastrukturu a službu. V letech 2007 – 2009 vytvořila pracovní skupina pro telekomunikace studii, která se zabývá problematikou kyberútoků a ochranou sítí elektronické komunikace a informačních systémů.

NATO se s kyberútokem poprvé setkala během kosovské krize v roce 1999, kdy se její počítače a webové stránky staly obětí srbských hackerů. Od té doby se aliance začala počítačovou kriminalitou, hlavně kybernetickou ochranou, zabývat a přijala řadu opatření včetně programu NCIRC (NATO Computer Incident Response Capability).

Přelom nastal, když aliance oznámila, že je připravena poskytnout pomoc v souladu se 4. článkem Washingtonské smlouvy, který říká, že členské státy mezi sebou budou konzultovat, pokud bude jejich nezávislost, územní celistvost nebo bezpečnost ohrožena. V letošním roce (2014) NATO schválilo novou politiku kyberochrany, ve které představilo subsidiarity. Aliance se tak nyní soustředí převážně na ochranu svých vlastních zařízení. Členské státy jsou pak odpovědné za ochranu vlastních systémů. To znamená, že NATO poskytne zařízení a technologie, ale členská země, která toho využije, plně zodpovídá za stav zařízení a hlavní zátěž stojí na ní.

3.7.1 CCD COE – Deset pravidel pro kyber-bezpečnost

Organizace CCD COE, která vznikla pod aliancí NATO, představila dokument Deset pravidel pro kyber-bezpečnost jako základní kámen pro utváření právního rámce v kyber-bezpečnosti. NATO však odkazuje na zmíněné ofenzivní využití internetu za účelem kyberochrany či na možnou aktivaci článku č. 5.

3.7.1.1 Deset pravidel pro kyber-bezpečnost

Deset pravidel pro kyber-bezpečnost se nezabývá jen zločinem na nízké úrovni (krádeže, špionáž, apod.), ale i chováním států v kyberprostoru. Snaží se najít normy, které by měly státy aliance dodržovat, a to i když je dokument nezávazný. NATO jej vnímá jako základ budoucího rámce. Lze však předpokládat, že u některých států narazí na odpor.

1) Pravidlo teritoriality
    a. Informační infrastruktura nacházející se na území jednoho státu je předmětem teritoriální suverenity onoho jednoho státu.
2) Pravidlo odpovědnosti

   a. Spáchání kyberútoku z počítače a jiného zařízení, které se nachází na území jednoho státu, je považováno za důkaz a tento útok může být tomuto státu připisován.

3) Pravidlo spolupráce
   a. Pokud byl útok spáchán z počítačového systému či zařízení daného státu, je tento stát povinen spolupracovat s obětí formou konzultací, výměny informací a dalšími způsoby.
4) Pravidlo sebeobrany
   a. Každý má v kyberprostoru právo na sebeobranu. Reakce silou je za některých okolností připuštěná.
5) Pravidlo ochrany dat
   a. Data získaná monitorováním internetu jsou považována za osobní a pracuje se s nimi dle právních předpisů dané země.
   b. Data mohou být poskytnuta třetí osobě za předpokladu, že zajistí stejnou míru ochrany.
   c. Monitorování internetu musí být v rovnováze s ochranou práv.
6) Pravidlo odpovědnosti se starat
   a. Každý má odpovědnost snažit se rozumným způsobem ochránit svá počítačová a komunikační zařízení.
7) Pravidlo včasného varování
   a. Každý má povinnost informovat potenciální oběť o chystaném počítačovém útoku, kyberhrozbě.
8) Pravidlo přístupu k informacím
   a. Veřejnost má právo být informováno o kyberhrozbách vůči životu, bezpečnosti, dobrému žití.
9) Pravidlo zákonnosti
   a. Každý stát je povinen zahrnout nečastější počítačové útoky do svého právního řádu.
10) Pravidlo mandátu
   a. Schopnost organizace jednat vždy vychází z rozsahu jejího mandátu.
   b. Na mezinárodním poli je nutné zastavit duplikaci schopností a úsilí.

3.8 Skupina osmi průmyslově vyspělých států světa (G8)

Francie, Itálie, Japonsko, Kanada, USA, Německo, Spojené království a Ruská federace mají nejsilnější ekonomiky světa. V roce 2011 tvořili 51% světového HDP. Sdružení nejvyspělejších států světa má nyní pouze sedm členů. Kvůli událostem posledních dní (dění na Ukrajině) bylo Rusku k 18. 4. 2014 pozastaveno členství jako reakce jeho angažování na Krymu. G8 je neformální sdružení, z čehož vyplývá, že organizace nemá žádnou vnitřní strukturu či hierarchii. Nemá stálý sekretariát nebo kancelář jednotlivých členských zemí. Změna předsednictva probíhá vždy k 1. lednu a členské země se pravidelně střídají. Setkání vrcholí summitem, který se převážně uskutečňuje v průběhu června.

Ministři spravedlnosti a vnitra zemí skupiny G8 přijali v roce 1997 na summitu ve Washingtonu deset principů, které shrnují „hi-tech“ zločiny. Dochází zde ke změně názvosloví, ale význam je stejný jako kyberzločin. Těchto deset principů bylo následně podepsáno na summinu v Birminghamu, a to následujícího roku (1998).

Obsah deseti principů v boji proti „hi-tech“ zločinům:

1) Pro ty, kteří zneužívají informační technologii, nesmí existovat bezpečné útočiště.
2) Vyšetřování a následné trestní řízení v oblasti počítačové kriminality musí být koordinováno mezi všemi státy, které se vyšetřování účastní, bez ohledu na to, kde se stala škoda.
3) Je zapotřebí dostatečné vybavení a vyškolení odborníků, kteří budou prosazovat právo v kyberprostoru.
4) Právo musí být vymahatelné, právní systém musí zaručit důvěrnost, integritu a dosažitelnost dat před neoprávněným narušením a zajistit, aby bylo jejich zneužití potrestáno.
5) Mezinárodní spolupráce musí zajistit včasný přenos informací a dat a jejich následné předání v případě, že se jedná o kyberzločin.
6) Zahraniční přístup orgánů prosazujících právo k veřejně dostupným informacím nesmí být podmíněno povolením od státu, ve kterém jsou data fyzicky umístěna.
7) Pro vyhledávání a zkoumání forenzních důkazů v elektronické podobě musí být vyvinuty a používány příslušné standardy.
8) Informační a komunikační systémy je zapotřebí navrhovat tak, aby přispívaly k obraně proti zneužití a jejich detekci, měly by usnadnit stopování zločinců a získávání důkazů.

9) Právní systém by měl zajistit uchování dat z komunikačního terminálu a rychlý přístup k nim, což je základní předpoklad pro úspěšné vyšetřování.
10) Aktivity spojené s touto činností je třeba koordinovat s činností mezinárodních fór, aby se zabraňovalo zdvojování těchto konkrétních aktivit.

V akčním plánu pro potírání počítačové kriminality byly principy následně konkretizovány (pro příslušné orgány zainteresovaných zemí jsou povinné):

- Ustanovit styčná místa, která budou dostupná 24 hodin denně a která budou ke svému provozu využívat již vybudovanou síť odborníků, aby byla zajištěna včasná a efektivní odpověď na nadnárodní případy počítačové kriminality.
- Zajistit prosazení mezinárodní spolupráce prostřednictvím příslušných orgánů jednotlivých států a dostatečně navýšit kapacity těchto orgánů, aby mohlo být právo náležitě prosazováno.
- Provézt revizi právního systému tak, aby byla zajištěna kriminalizace zneužití informačních a komunikačních systémů a dalších kyberzločinů.
- V otázkách vzájemné pomoci v duchu mezinárodní spolupráce vyjednávat dohody tak, aby byla otázka počítačové kriminality v této dohodě obsažena.
- Pokračovat ve zkoumání a vyvíjení metodik řešení, které se týkají zachování forenzních důkazů před vydáním soudního rozhodnutí, přeshraničních prohlídek, prohledávání dat v počítači v případě, kdy není známo umístění těchto dat.
- Vyvinout postupy, které by rychlou akcí získaly provozní data ze všech komunikačních prostředků v řetězci komunikace, najít způsoby urychleného přesunu těchto dat na mezinárodní úrovni.
- Vyvíjet nové technologie společně s průmyslovými odvětvími tak, aby bylo zajištěno, že tyto technologii usnadní boj proti počítačové kriminalitě.
- Vytvořit mechanismy, které by zajistily bezprostřední přijetí požadavků vzájemné pomoci v naléhavých případech, aby byla zajištěna zpětná a včasná vazba, pomocí rychlých a dostatečně spolehlivých prostředků komunikace – prostřednictvím hlasu, elektronické pošty, případně písemného potvrzení.
- Podporovat organizace, které se snaží svým fungováním a tvorbou mezinárodních standardů v oblasti telekomunikačních a informačních technologií trvale poskytovat veřejnému a privátnímu sektoru standardy technologií pro bezpečnou komunikaci a zpracování dat.

- Vyvinout kompatibilní forenzní standardy pro vyhledávání a ověřování elektronických dat při kriminálním vyšetřování.

3.9 Mezinárodní asociace internetových horkých linek

Internetová horká linka je kontaktní centrum, které přijímá hlášení o výskytu nezákonného a nevhodného obsahu na internetu. Nevhodný obsah je definován jako něco, co může negativně ohrozit vývoj a výchovu dětí nebo na nich může zanechat trvalé následky zejména psychického vjemu. Mluvíme zde o zesměšňování, šíření pomluv, kyberšikaně. Nezákonný obsah má většinou tyto specifikace:

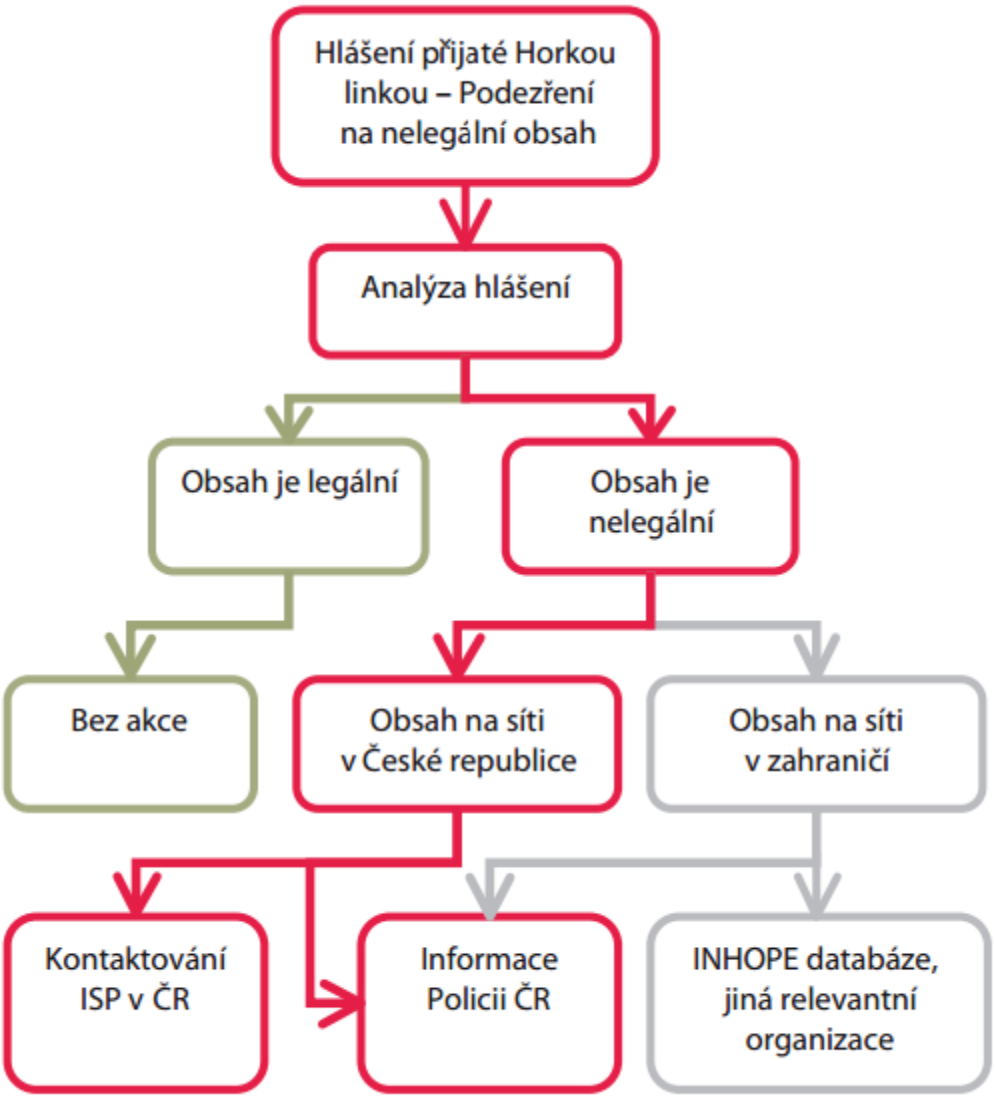
- dětská pornografie,
- prostituce,
- pedofilie,
- ostatní nelegální sexuální praktiky,
- rasismus,
- xenofobie,
- sebepoškozování,
- výzvy k násilí
- šíření drog.

Česká horká linka je součástí mezinárodní asociace INHOPE, v rámci které si partneři předávají informace a hlášení o nelegálním obsahu.

Hlášení, které přijmou střediska, jsou vyhodnocena vyškolenými pracovníky v souladu s platnými právními předpisy. V případě, že podezřelá adresa obsahuje nelegální obsah, je s ní nakládáno následovně:

- Adresa je předána kompetentnímu úřadu (v rámci ČR je to společnost ISP), na jehož server se obsah nahraje s žádostí o odstranění.
- U obsahu na síti v zahraničí žádost zpracovává partnerská horká linka.

V každém případě je informována Policie.

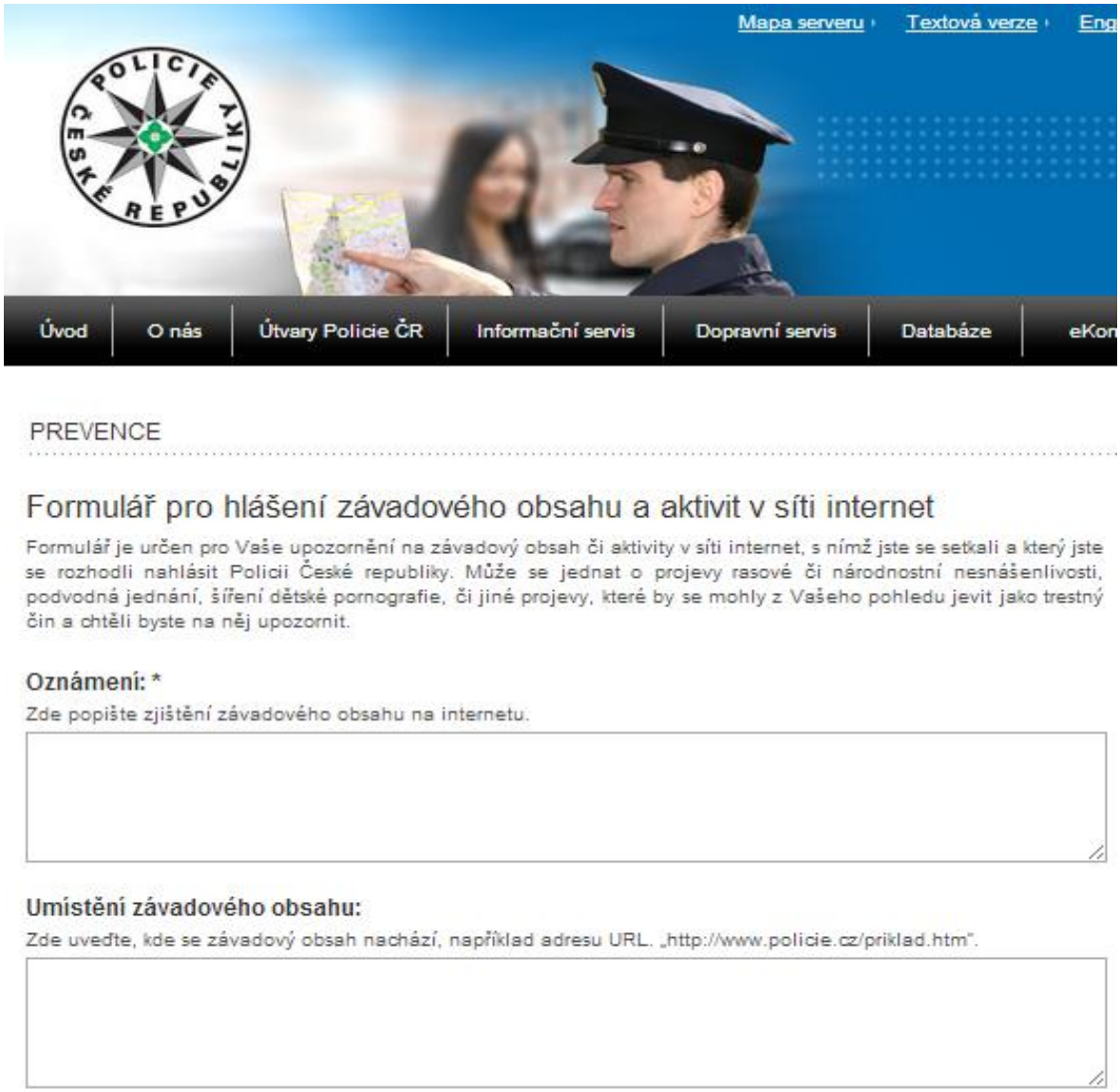


Obr. 6 – Grafické schéma práce horké linky

V České republice horká linka funguje od 1. dubna 2007, a to na stránkách Policie ČR http://aplikace.policie.cz/hotline/, kam lze nahlásit nelegální obsah.

Horká linka vznikla ve spolupráci předních světových finančních subjektů a představitelů internetového průmyslu spolu s Mezinárodním střediskem pro pohřešované a zneužívané děti a jeho sesterskou organizací, Národním střediskem pro pohřešované a zneužívané děti, aby společně bojovali proti dětské pornografii.

Iniciativa si stanovila nelehký cíl – vymýtit dětskou pornografii. Koalice navázala spolupráci s Mezinárodní asociací horkých linek. Jejich výsledkem je kampaň apelující na nejširší veřejnost v konkrétních zemích, kde je tato trestná činnost páchána nejvíce.[4,6,7,8,14,15,28]



Obr. 7 – Zadávací formulář na stránkách Policie ČR

4 PRÁVNÍ PŘEDPISY V ČR

V právním řádu České Republiky do roku 2009 zahrnovala problematiku počítačové kriminality pouze jedna norma, která explicitně popisovala „informační a informatickou kriminalitu“, a to podle zákona č. 140/1961 Sb.

Nejnovější zákony a předpisy vychází z trestního zákoníku č. 40/2009 Sb., kde je nově stanoven pojem počítačová kriminalita, který vychází z anglického slova „cybercrime“. Úmluva o počítačové kriminalitě byla schválená výborem ministrů Rady Evropy dne 8. 11. 2001 a definovala jasněji tyto pojmy. ČR tuto Úmluvu „přijala“ až v roce 2005 a do dnešních dnů bohužel stále neratifikovala, a to stejně jako několik dalších členských států Rady Evropy. Tato Úmluva neobsahuje jednotnou definici počítačové kriminality jako takové, ale souhrn aktivit, které by smluvní strany měly v rámci svého právního systému postihovat jako trestný čin, jedná se o:

a) protiprávní přístup a protiprávní zachycení informací,
b) zásah do dat, systému nebo zařízení,
c) falšování údajů souvisejících s PC,
d) trestné činy, které souvisí s dětskou pornografií,
e) trestné činy, které souvisí s porušením autorských práv a práv příbuzných.

4.1 § 230 Zákona č. 40/2009Sb.

„Neoprávněný přístup k počítačovému systému a nosiči informací.“

Zákon jasně definuje neoprávněný přístup k počítačovému systému a dalším nosičům informací. Rovněž hovoří o tom, jaké postihy v tomto případě ukládá za porušení tohoto zákona. § 230 jasně vytyčuje možné typy neoprávněného přístupu a další činy, které jsou postihovány v rámci tohoto paragrafu.

První článek § 230: *„Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“*

Za porušení zákona dle druhého článku hrozí odnětí svobody na dva roky, zákaz činnosti, nebo propadnutí věci či jiné majetkové hodnoty tomu, kdo:

- získá přístup k cizímu počítačovému systému nebo nosiči informací,

- neoprávněně vymaže data z počítačového systému nebo nosiče informací, poškodí, změní či sníží kvalitu nebo učiní data nepoužitelnými,
- padělá nebo změní data, která jsou uložena v počítačovém systému nebo na nosiči dat a informací, a to s podmínkou, že právě podle těchto dat bylo jednáno, jako by byla pravá bez ohledu na to, zda jsou data přímo čitelná a srozumitelná.
- neoprávněně vloží data do počítače nebo na nosič informací a taktéž jinak zasáhne do programového či technického vybavení počítače.

Odnětí svody na šest měsíců až tři roky, zákaz činnosti, nebo propadnutí věci jiné majetkové hodnoty hrozí pachatelům, kteří způsobí tyto trestné činy:

- způsobení škody nebo újmy a taktéž získání neoprávněného prospěchu sobě nebo jinému,
- neoprávněné omezení funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.

Odnětím svobody na jeden rok až pět let, nebo peněžitým trestem bude pachatel potrestán za to, když:

- jako člen organizované skupiny spáchá trestný čin,
- způsobí svým činem značnou škodu,
- způsobí svým činem vážnou poruchu v činnosti orgánu státní správy nebo územní celistvosti, soudu a jiným orgánům veřejné moci,
- získá svým činem pro sebe nebo jiného prospěch,
- způsobí vážnou poruchu v činnosti fyzické a právnické osobě, která je podnikatelem.

Odnětí svobody na tři roky až osm let je státním zastupitelem navrhováno tehdy, když:

- pachatel způsobí svým činem (uveden výše) škodu velkého rozsahu,
- pachatel získá svým činem pro sebe nebo jiného prospěch velkého rozsahu.

§ 230 je konstruován tak, aby především chránil informace uložené na počítačovém systému a nosiči informací. Tento paragraf vznikl sloučením a úpravou dvou paragrafů § 228 a § 229, které byly pozměněny podle Úmluvy o počítačové kriminalitě (Budapešť, 23. 11. 2001). § 230 je právní norma, která postihuje překonání bezpečnostního opatření a současně neoprávněné získání přístupu k počítačovému systému, jedná se tedy o jakýkoli počin, například počítačový útok hrubou silou nebo hacking.

Tento paragraf ale neřeší postižení pachatele, který použil podvodné techniky sociálního inženýrství a z postižené osoby vylákal takto informace, jež následně použil na své obohacení nebo ke způsobení újmy druhé osobě.

Další část § 230 řeší případné jednání osoby, která získala přístup k počítačovému systému. Není zde podstatné, jakým způsobem se dostala do počítačového systému, ale jestli užije, nebo neužije uložená data, ať už se jedná o jejich zneužití, padělání nebo vymazání těchto určitých dat.

Poslední část § 230 je zaměřena na skupinu pachatelů, kteří pomocí získaných dat a informací přišli ke svému či cizímu prospěchu nebo způsobili škodu a nefunkčnost daného počítačového systému. Taktéž řeší skutkovou podstatu činů, které byly spáchány jako organizovaný zločin. Vyšší sazba odnětí svobody je potom udělována za spáchání zvlášť větší škody nebo zisku.

4.2 § 231 Zákona č. 40/2009Sb.

„Opatření a přechovávání přístupových zařízení a hesla k počítačovému systému a jiných takových dat.“

§ 231 se skládá ze tří článků, ve kterých se jedná o hrubé nedbalosti a ochraně informací.

Článek 1 § 231: *„Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 180 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává zařízení nebo jeho součást, postup, nástroj.*

Odnětím jednoho roku svobody, propadnutím věci a jiné majetkové hodnoty, nebo zákazem činnosti se bude posuzovat trestná činnost, která souvisí:

- s vytvořením prostředku nebo přizpůsobení věci k neoprávněnému přístupu do sítě elektronické komunikace, počítačovému systému nebo jeho součástí,
- se zneužitím počítačového hesla, přístupového kódu a jiného podobného prostředku, pomocí něhož je možné dostat se do počítačového systému či jeho části.

Odnětím svobody na tři roky a zákazem činnosti, nebo propadnutím věci a jiné majetkové hodnoty bude pachatel trestán:

- za spáchání trestného činu podle odstavce 1, a to jako člen organizované skupiny,
- za to, že získá takovým činem pro sebe nebo jiného značný prospěch.

Výjimečným trestem je odnětí svobody až na pět let za to, že pachatel získá svým činem uvedeným v odstavci 1 pro sebe či jiného prospěch o velkém rozsahu.

Důvodem vytvoření tohoto paragrafu byla možnost, že nastane ohrožení při nedbalém nakládání s počítačovými systémy, které řídí výrobu zboží všeho druhu, finance, letový provoz a zdravotnické vybavení. Vzhledem k těmto skutečnostem by tedy ohrožení tohoto provozu mohlo znamenat ohrožení života, zdraví a majetku.

4.3 § 232 Zákona č. 40/2009Sb.

„Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.“

Článek 1 tohoto paragrafu hovoří o hrubém porušení pracovních povinností z nedbalosti, které vyplývají ze zaměstnání, povolání, postavení nebo funkce. Pojednává o tom, kdo tímto svým jednáním spáchá značnou škodu na cizím majetku. Toto překročení zákona se trestá odnětím svobody na šest měsíců, zákazem činnosti, nebo propadnutí věci či jiné majetkové hodnoty. Jedná se o:

- zničení či poškození dat, které se tímto způsobem stanou neupotřebitelnými, byla-li uložena v počítačovém systému nebo na nosiči informací,
- učinění zásahu do hardwarového či softwarového vybavení nebo do jiného technického zařízení pro zpracování dat.

Odnětím svobody až na dva roky a zákazem činnosti, propadnutím věci, nebo jiné majetkové hodnoty bude pachatel trestán, jestliže způsobí svým činem, který je uveden v odstavci 1, škodu velkého rozsahu. Značnou škodou se zde rozumí škoda, která byla větší než 500 000 Kč. Škoda velkého rozsahu je podle § 138 trestního zákoníku taková, která dosáhla částky nejméně 5 000 000 Kč.

K doplnění informací musíme definovat nedbalost, a to podle § 16 trestního zákoníku. Trestní čin z nedbalosti je, když pachatel:

- *„věděl, že může způsobem uvedeným v trestním zákoně porušit nebo ohrozit zájem chráněný takovým zákonem, ale bez přiměřených důvodů spoléhal, že takové porušení nebo ohrožení nezpůsobí, nebo*

- *nevěděl, že svým jednáním může takové porušení nebo ohrožení způsobit, ač o tom vzhledem k okolnostem a k svým osobním poměrům vědět měl a mohl.“*

4.4 § 270 Zákona č. 40/2009Sb.

„Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi.“

§ 270 o porušování autorských práv ukládá v prvním článku tresty ve výši odnětí svobody až na dva roky, zákazu činnosti, propadnutí věci, či majetkové hodnoty. První článek hovoří o neoprávněném zásahu do zákonem chráněných práv k autorskému uměleckému dílu, zvukovému a zvukově obrazovému záznamu, televiznímu a rozhlasovému vysílání či databázi.

Dále je trestáno odnětím svobody na šest měsíců až pět let, peněžitým trestem, propadnutí věci, či jiné majetkové hodnoty, když:

- bude čin uvedený v odstavci jedna vykazovat znaky obchodní činnosti nebo jiného druhu podnikání,
- získá touto činností značný prospěch pro sebe nebo jiného a způsobí škodu tímto jednáním,
- dopustí se takového činu ve značném rozsahu.

Nejvyšším možným postihem je odnětí svobody na tři až osm let, a to za následujících podmínek:

- Získá-li pachatel svým jednáním uvedeným v odstavci jedna pro sebe nebo někoho jiného prospěch velkého rozsahu a tímto činem způsobí jinému škodu velkého rozsahu.
- Dopustí-li se takového činu ve velkém rozsahu. [3]

5 PROJEVY POČÍTAČOVÉ KRIMINALITY

Obr. 8 – Schéma kategorií počítačové kriminality

TOP 5 hrozeb a ohrožení zabezpečení firem v roce 2013:

- Česká republika
    1. Kybernetické útoky zaměřené na krádež finančních údajů
    2. Ohrožení zabezpečení související s využíváním mobilních technologií
    3. Kybernetické útoky zaměřené na rušení chodu či poškození podniku
    4. Podvod
    5. Zastaralé kontroly či architektura informační bezpečnosti
- Střední Evropa
    1. Lehkomyslný přístup či nevědomost zaměstnanců
    2. Spam
    3. Kybernetické útoky zaměřené na rušení chodu či poškození podniku
    4. Ohrožení zabezpečení související s využíváním mobilních technologií
    5. Kybernetické útoky zaměřené na krádež finančních údajů[25]

5.1 Kategorie počítačové kriminality

5.1.1 Protiprávní jednání

5.1.2 Spamming

Pojem spamming je odvozen od výrazu *spam,* který značí nevyžádanou elektronickou poštu v emailové schránce. Tato činnost souvisí se získáváním emailových adres a jejich poskytováním spammerovi bez vědomí subjektů. Dále v této souvislosti můžeme hovořit o obchodu s emailovými adresami, jež spammer vytvoří v databázové struktuře a nabízí je k prodeji podnikům, které je dále využívají k vlastní reklamní kampani. Přestože vývojáři emailových schránek usilují o to, aby nevyžádaná pošta mohla být filtrována z jejich serverů, nedaří se jim to, jelikož spammeři vyvíjí stejným tempem postupy, jak prvky obrany obejít, a zaslat tak na cílenou adresu spam. Tato činnost se dá kriminalizovat jako pojednávání o neoprávněném nakládání s osobními údaji.

5.1.3 Cracking

Forma počítačové kriminality cracking označuje prolomení prvků elektronické ochrany a programových produktů s cílem jejich neoprávněného používání. Tato forma používá řadu metod od debugování spuštěného programu až do postupu reverse engineering. Cracking je nejčastěji používán při průniku do systému se záměrem zjistit důležité informace pro neoprávněný přístup do cílového systému – metoda „password cracking“ neboli zjišťování hesla pro přístup do systému.

Tato trestná činnost může být velmi těžce posuzovaná z hlediska trestního stíhání, neboť pokud fyzické či právnické osobě nevznikla hmatatelná škoda na hmotném či nehmotném majetku, nelze tuto formu považovat za trestný čin a od soudního stíhání může být zcela upuštěno. V ostatních případech se z pravidla jedná o zneužití a porušení autorského práva, nebo o neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 trestního zákoníku.

5.1.4 Sniffing

Tato ilegální činnost je způsobována odchytáváním dat a komunikací uživatelů na síti prostřednictvím internetu. Cizí osoba neoprávněně monitoruje elektronickou komunikaci a pohyb dat své oběti. Tímto způsobem může sniffer získat požadované informace (osobní údaje, obsahy emailů a odesílané či přijímané soubory), které aplikuje k přístupu ke službám,

jež právě používá sledovaná osoba, aby využil tyto osobní údaje ve svůj vlastní prospěch. Touto činností tedy narušuje osobní soukromí sledované osoby.

„Odposlouchání“ sítě si nevyžaduje žádné velké zkušenosti. Postačí k tomu pouze jeden program, který umožňuje odposlouchávání spustit, a sledování nešifrované komunikace probíhající přes určitou část sítě může začít.

Pokud si chce uživatel ověřit, jaká data a kam počítač odesílá, může využít programu Network monitor pro OS Windows nebo CommView pro OS Linux.

V právním řádě, konkrétně v trestním zákoníku, se dá sniffing zařadit do § 182 o porušování tajemství dopravovaných zpráv. Postih může dosahovat až dvou let odnětí svobody a zákazu činnosti.

5.1.5 Cyberquatting

Obětí cyberquattingu se stává většinou firma, která si chce vytvořit internetové stránky, nicméně doména s názvem dané firmy je již koupená, přestože se na ní nenachází žádný obsah. Firma pak vesměs nemá jinou možnost, než si tuto doménu odkoupit od soukromé osoby, která ji momentálně vlastní. Tato osoba však doménu nabízí třeba desetkrát dráž, než je původní cena od poskytovatele.

Princip je jednoduchý – pachatelé si včas zaregistrují a zakoupí internetové stránky s názvy firem, které mají (nebo se očekává, že budou mít) dobré jméno, a vyčkávají, dokud si daná firma nebude chtít onu adresu zaregistrovat. Poté, co firmy zjistí, že už je adresa s jejich názvem zaregistrovaná, většinou si tuto adresu za větší finanční obnos zakoupí, nebo mohou využít soudní cesty. V takových případech soudy převážně jednají ve prospěch firmy, o jejíž jméno se jedná.

5.1.6 Phishing

Název této kriminální techniky vznikl odvozením z anglického slova „fishing“, což je v překladu „rybaření“. Jedná se o podvodnou techniku, jejímž účelem je získat, nebo spíš vylákat z lidí, pomocí internetu citlivá data jako osobní údaje, údaje o bankovních účtech a platebních kartách. Tyto jsou následně použity ve prospěch útočníka. Ve světě je tato technika známa od roku 1995. Do České republiky se ve větší míře dostala v roce 2006, a to útokem na banku CitiBank – útok je popsán v dřívější kapitole. Phishing se šíří po internetu nejčastěji skrze podvodné emaily, které vypadají velmi podobně jako emaily od renomova-

ných značek, především bank. Primárními poznávacími prvky těchto podvodných emailových zpráv jsou gramatické chyby, často špatně přeložené texty z cizího jazyka psané bez diakritiky, a zadávání osobních údajů skrze formuláře obsažené přímo v emailu.

5.1.7 Pharming

Technika pharming je vylepšená verze phishingu s tím rozdílem, že pharming nerozesílá podvodné emaily, ale útočí na DNS server, na který se klient právě připojuje. Dojde k přesměrování internetové adresy z původní, jež zadal uživatel, na adresu, jež vytvořil útočník. Jako příklad můžeme uvézt připojení do internetového bankovnictví. Uživatel zadá do internetového prohlížeče adresu své banky, internetová stránka se otevře, na první pohled vypadá jako originál, ale ve skutečnosti se jedná pouze o její napodobeninu, jelikož došlo k přesměrování serveru DNS. Stránky potom vyzvou klienta k přihlášení do systému pomocí přihlašovacích údajů a kódů. Pokud takto klient učiní, předá své údaje útočníkovi a ten je následně může využít pro trestnou činnost.

Odhalit tento podvod je někdy obtížné i pro zkušeného informatika. Nebezpečí se dá mnohdy rozeznat podle chování stránky, která po vás může žádat více informací, než je obvyklé. Pokud se takto stane, je doporučováno okamžité opuštění internetové stránky a nahlášení problému pomocí telefonu na klientské středisko, které dále tento problém bude řešit s pověřenými orgány státní správy.

5.1.8 Carding

Carding je podvodná metoda, která funguje na principu kopírování údajů z platebních karet pomocí magnetických proužků. Její princip je jednoduchý. Stačí projet magnetickým proužkem karty přes čtečku, která je umístěna u čtecího zařízení, a následně tyto údaje nahrát na jinou prázdnou kartu.

S těmito případy se často setkáváme u bankomatů. Čtečka RFID karet se přiloží blízko k originálnímu terminálu tak, aby společně s bankomatem vypadala jako jeden celek. Čtečka taktéž obsahuje miniaturní kameru, která je schopna zaznamenat PIN kód zadávaný na klávesnici.

5.1.9 Kyberterorismus

Kyberterorismus je spojení klasického projevu terorismu a kyberprostoru, resp. terorismus v kyberprostoru. Tento nezákonný útok proti počítači, počítačové síti a nosiči informací má zastrašit nebo donutit vládu, příp. obyvatele k podporování sociálních či politických cílů.

5.1.10 Hoax

Tento zajímavý styl protiprávního chování je v kontextu s informačními technologiemi poměrně nebezpečnou záležitostí, která může způsobit nemalé potíže. Pojem hoax označuje zprávu s nepravdivým obsahem, která se snaží pomocí hromadné korespondence rozšířit mezi co možná nejvíce lidí a vyvolat mezi příjemci paniku. Zprávy mohou obsahovat různou tematiku od charitativní pomoci po nejrozličnější varování např. o nebezpečném hmyzu, o šíření života nebezpečných látek v poštovních zásilkách nebo o zapíchnutých injekčních stříkačkách v sedačkách MHD. Ve většině případů ve zprávě původní odesílatel žádá, aby byl daný text rozeslán co možná největšímu počtu lidí. Rozeznat hoax od pravé varovné zprávy však není vždy jednoduchá záležitost. K ověření slouží např. portál http://www.hoax.cz/cze/.

5.1.11 Tvorba škodlivých programů

Podle § 230 trestního zákoníku je trestná činnost manipulace s daty uloženými v počítačovém systému nebo nosiči informací, jejich mazání, nebo způsobení jejich nepoužitelnosti. Právě takovouto trestní činnost páchá ten, kdo vytváří a šíří elektronickým způsobem škodlivé programy, nejčastěji viry nebo trojské koně. Skutková podstata tohoto aktu nebude naplněna v případě, že se z napadeného počítače škodlivé programy samy automaticky rozešlou všem uživatelům, které má v kontaktním listě uložené uživatel napadeného počítače, nebo dojde-li k nechtěnému infikování počítačového systému přenosným úložným zařízením, jež se infikovalo v počítačovém systému druhé osoby.

5.1.12 Průmyslová špionáž

Průmyslová špionáž existuje od doby, kdy mezi sebou začaly soutěžit dvě konkurenční firmy. S příchodem informačních technologií se tato protiprávní činnost značně zjednodušila. Průmyslová špionáž obvykle kombinuje více metod počítačové kriminality s cílem

získat informace, know-how, postupy a data uložená na konkurenčních počítačových systémech k maximalizaci svých vlastních výrobních procesů a technologií. S touto činností se můžeme setkat např. u komerčního zpravodajství.

5.1.13 Padělání

Od dob, kdy nejlepšími padělateli byli zpravidla výborní rytci, zruční řemeslníci a kreslíři, prošlo toto „řemeslo“ velkými změnami. Dnešní padělatelé využívají ke své činnosti nejdokonalejší laserové tiskárny, grafické editory a jiné prvky moderních IT. Najdou se i amatérští padělatelé, kteří napodobují pomocí domácích tiskáren, ale jejich počínání má většinou brzkého konce. K často padělaným předmětům totiž patří bankovky, ty dnešní však mají množství bezpečnostních prvků a jejich duplikace vyžaduje více než domácí kopírku. Dalším problémem u padělání je kvalita papíru. Bankovky jsou vyráběny ze speciálního papíru, který se nedá normálně sehnat. Jediným způsobem je jeho složitá imitace nebo odcizení ve výrobnách.

Bankovky ale nejsou jedinými cennými papíry, které se padělají. Mnohem rozšířenější jsou padělky veřejných listin jako vysokoškolské diplomy, maturitní vysvědčení, osobní doklady či atestační listiny.

5.1.14 Peer-to-peer

Sdílení dat pomocí peer-to-peer sítí (p2p) je považováno za obrovský a zároveň expandující fenomén dnešní doby. Aniž by si to uvědomovali, tuto formu počítačové kriminality koná bezmála 40% uživatelů informačních technologií. Jedná se o systematické zveřejňování a zpřístupňování dat prostřednictvím přímého spojení, kdy se uživatelé z celého světa mohou pomocí programu mezi sebou spojit a stáhnout požadované soubory. [2,12,17,21]

II. PRAKTICKÁ ČÁST

6 ROZBOR ÚMLUVY RADY EVROPY O POČÍTAČOVÉ KRIMINALITĚ

6.1 Preambule

Členské státy Rady Evropy a další státy, které Úmluvu Rady Evropy o počítačové kriminalitě podepsaly, mají na zřeteli, že cílem této Úmluvy je snaha dosáhnout větší jednoty mezi jejími členy budováním spolupráce s těmito státy. Signatáři jsou přesvědčeni o potřebě prioritního uskutečňování společné trestné politiky zaměřené na ochranu společnosti proti počítačové kriminalitě přijetím příslušných právních předpisů a rozšířením mezinárodní spolupráce.

Naléhavost, s jakou je potřeba jednat, expanduje s rizikem, že počítačové systémy a elektronická data mohou být zneužita pro trestnou činnost a důkazy o těchto činech se mohou nacházet právě v počítačových systémech a nosičích informací.

Úmluva taktéž uznává spolupráci mezi státem a soukromými objekty při potírání počítačové kriminality a potřebu chránit zájmy při vývoji informačních technologií. Hovoří se o účinném boji proti počítačové kriminalitě, který vyžaduje urychlenou a hlavně funkční mezinárodní spolupráci v trestních věcech. Rada Evropy je přesvědčena, že skrze tuto Úmluvu získá nezbytné prostředky pro odrazení lidí od páchání trestných činů namířených proti integritě a bezpečnosti informačních technologií. Úmluva je zamýšlena a směřována také na doplnění dalších úmluv (Úmluva Organizace spojených národů o právech dětí z roku 1989, Úmluva Rady Evropy o ochraně jednotlivců při automatickém zpracování osobních údajů z roku 1981), aby byla účinnější trestní vyšetřování a trestní řízení, která se týkají trestných činů spojených s počítačovými systémy včetně všech aktivit OSN, EU, OECD.

Možnost rychlého připojení dalších zemí k této Úmluvě a vhodného nalezení řešení během následné spolupráce je klíčové pro účinné řízení mezinárodní spolupráce v boji proti počítačové kriminalitě i dalším právním deliktům.

6.2 Opatření na vnitrostátní úrovni

Úmluva představuje opatření, která jsou závazná po jejím podepsání. Jsou rozdělena do jednotlivých článků, které popisují podrobně počítačovou trestnou činnost a daly by se považovat za trestní zákoník Rady Evropy, jenž je cílený na počítačovou kriminalitu. Články Úmluvy tuto činnost popisují tak, aby členské státy mohly následně z tohoto dokumentu

vytvořit zákony, které by platily na vnitrostátní úrovni. Kategorie trestných činů je rozsáhlá a kvalitně zpracovaná, podobně jako trestní zákoník České republiky. Níže se budeme zabývat trestním právem hmotným, trestnými činy, které souvisí s počítačem a jeho obsahem, porušováním autorských práv a formami odpovědnosti a trestů. Úmluva je koncipovaná tak, aby si státy mohly svou vnitrostátní legislativu postavit podle svých potřeb a představ za předpokladu dodržení základní myšlenky obsažené v této Úmluvě. Česká republika přijala v roce 2009 trestní zákoník, který obsahuje základní poznatky, jenž vychází z této Úmluvy.

6.2.1 Trestní právo hmotné

Patří sem činy proti důvěryhodnosti, integritě a použitelnosti počítačových systémů a nosičů dat a právní delikty typu nezákonný přístup, odposlech.

6.2.1.1 Nezákonný přístup k počítačovému systému a jeho odposlech a zásah

Každý účastník dohody má považovat za trestný čin takové jednání, jehož důsledkem je neoprávněný přístup k počítačovému systému a jeho částí. Čin bude považován za trestný v případě, že dojde k porušení bezpečnostních opatření, odcizení počítačových dat nebo jinému nečestnému chování, které je spojováno s počítačovým systémem.

Za trestný čin se považuje neoprávněný odposlech neveřejného přenosu elektronických dat z jednoho počítačového systému do druhého a zachytávání elektromagnetického vyzařování pomocí technických prostředků. Právní legislativa může stanovit, kdy takovýto čin bude klasifikován jako trestný vzhledem k jeho úmyslu – zda je nečestný a v jakém vztahu je s počítačovým systémem. Dále uvádí doporučená legislativní opatření, která jsou nezbytná pro potrestání činů úmyslného a neoprávněného poškozování, vymazání, pozměnění či snížení kvality dotčených počítačových dat.

6.2.1.2 Zásah do systému a zneužití zařízení

Zásahem do počítačového systému se v tomto případě rozumí úmyslné a neoprávněné omezení funkčnosti vložením, poškozováním a zničením dat. Za zneužité zařízení se považuje to, na kterém bylo neoprávněně a úmyslně spácháno zpřístupnění výroby, prodeje, dovozu nebo distribuce zařízení (počítačového systému, programu) nebo vytvoření počítačového programu za účelem spáchání jakéhokoli trestného činu, který je definován v této kategorii.

6.2.2 Trestné činy, které souvisejí s počítačem a jeho obsahem

Tak jako v předchozí kapitole i zde se jedná o neoprávněné a úmyslné nakládání s počítačovým systémem, zejména pak o padělání a počítačové podvody. Zvláštní část zde tvoří trestné činy související s dětskou pornografií.

6.2.2.1 Počítačové padělání a podvod

Při spáchání trestného činu padělání hovoříme o vkládání a pozměňování, vymazání či potlačení počítačových dat s úmyslem vydávat je za pravá a používat je k právním účelům.

Za podvod je považováno způsobení škody na majetku jinému, a to jakýmkoli vkládáním, změněním a vymazáním počítačových dat nebo zásahem do fungování počítačového systému s vidinou zisku majetkového prospěchu pro sebe nebo jiného.

6.2.2.2 Trestná činnost související s dětskou pornografií

Dětská pornografie obsahuje pornografický materiál, který vizuálně zobrazuje nezletilou osobu, jež se účastní jednoznačného sexuálního chování a taktéž realistické zobrazení, které představuje nezletilou osobu a z něhož vychází jednoznačné sexuální chování. Úmluva jasně definuje trestné činy spojené s dětskou pornografií a doporučuje státům, aby tyto činy zařadily do svého trestního zákoníku. Jedná se o:

- výrobu a distribuci dětské pornografie,
- zprostředkování přístupu k dětské pornografii skrze počítačový systém,
- přenos dětské pornografie prostřednictvím počítačového systému,
- opatřování pornografie sobě nebo jinému,
- uchovávání těchto dat v počítačovém systému nebo na nosiči informací.

6.2.3 Porušování autorských práv

Definice porušování autorských práv pro potřeby této Úmluvy vychází z Pařížské revize z roku 1971 Bernské Úmluvy o ochraně literárních a uměleckých děl, dále z Dohody o obchodních aspektech práv k duševnímu vlastnictví a právu autorském podle Smlouvy Světové organizace duševního vlastnictví WIPO. Definice hovoří o tom, že pojem duševní vlastnictví je spojen s právem. Jedná se především o nehmotné statky – neuchopitelné věci, které nelze vyjádřit ve zhmotnělé podobě, ale jako výtvor lidských dovedností a myšlenek patřící tomu kdo je stvořil.

Jako trestný čin je tedy chápáno porušení autorských práv za předpokladu, že se autorská data záměrné používají k provozování komerční činnosti prostřednictvím počítačového systému bez autorova souhlasu k využívání a kopírování takovýchto dat a médií.

Trestný čin ve stádiu pokusu

Trestný čin, jenž je klasifikován jako čin ve stádiu pokusu, je jakákoli úmyslná forma účastenství na spáchání kteréhokoli trestného činu – v tomto případě hovoříme o trestných činech spáchaných s pomocí počítačových systémů, které jsou předdefinovány v této Úmluvě a které jsou kriminalizovány v trestním zákoníku České republiky.

Odpovědnost zainteresovaných osob

Za každý spáchaný trestný čin ustanovený touto Úmluvou, který je spáchán fyzickou osobou, může být přiřazena odpovědnost z právě vykonaného tohoto trestného činu osobě právnické, které po vykonání takovéhoto činu vznikl prospěch. Fyzická osoba musí mít předem definované pravomoci od právnické osoby, aby mohlo dojít k vyplnění skutkové podstaty u tohoto typu trestné činnosti. Mezi tyto pravomoci patří:

- jednat jménem právnické osoby,
- přijímat rozhodnutí jménem právnické osoby,
- vykonávat kontrolu v rámci právnické osoby.

Taktéž může být právnická osoba uznána odpovědnou v případě, že nedostatečnou kontrolou nebo dohledem nad fyzickou osobou umožnila spáchání trestného činu. Tento čin bude dále posuzován buď podle odpovědnosti trestní, správní, nebo občanskoprávní. Odpovědnost za spáchání takovéhoto trestného činu nebude mít vliv na trestní odpovědnost fyzické osoby.

Tresty

Úmluva vyzývá k tomu, aby každý trestný čin definovaný touto Úmluvou mohl být potrestán účinně, přiměřeně a s odrazujícím účinkem, např. trest odnětí svobody nebo peněžitý trest.

6.2.4 Právo procesní

V této části Úmluvy se uvádí souhrn právních procesů a postupů, které říkají, jak se domáhat svých práv. Tento typ práva je odvozený od práva hmotného. Příklad procesního práva je navrhování a uchovávání důkazů pro nějaké tvrzení.

6.2.4.1 Procesní ustanovení

Tak jako všechny ostatní části Úmluvy je i tato závazná po podpisu. Pravomoci a postupy jsou stanovené pro specifická trestní vyšetřování a řízení v problematice počítačové kriminality. Rozsah pravomocí je vymezen:

- trestnými činy uvedenými v kapitole 6.2.1 Trestní právo hmotné,
- trestnými činy spáchanými prostřednictvím počítačového systému,
- zajišťováním důkazů o trestné činnosti.

Podmínky

Každý stát musí zaručit, že vytvořené vnitrostátní právní předpisy budou postaveny na principu přiměřenosti včetně závazků na dodržení základních lidských práv a svobod, které vychází z Úmluvy Rady Evropy na ochranu lidských práv a svobod z roku 1950 a dalších mezinárodních dokumentů o lidských právech. Tyto podmínky musí být dodrženy s ohledem na pravomoci nebo postupy příslušného orgánu a budou zahrnovat soudní či jiný nezávislý dohled. Státy zváží dopad těchto pravomocí na právo, odpovědnost a legitimní zájmy třetích stran s řádným výkonem spravedlnosti.

6.2.4.2 Uchovávání počítačových dat a následné zpřístupnění

Dalším pohledem na mezinárodní spolupráci v boji proti počítačové kriminalitě je uchovávání dat a jejich následné zpřístupnění příslušným orgánům v době, kdy je ohrožena jejich existence a kdy vzniká podezření, že tato data jsou ohrožena ztrátou nebo změněním. Musí se ale jednat o data, která byla uložena prostřednictvím počítačového systému a která mohou být použita v rámci vyšetřování. Nezbytná doba existence těchto dat čítá 90 dnů. Správci počítačového systému, v němž se nachází tato data, ukládá zákon povinnost udržovat tyto postupy v tajnosti po dobu, kterou stanoví vnitrostátní právní předpis. Během ukládání dat se musí provézt úkony, které zajistí, že na přenášená data nemá vliv více účastníků poskytující dané služby. Pro korektní zajištění dat a jejich následné zpřístupnění je určen státem zodpovědný orgán nebo osoba.

6.2.4.3 Odposlech dat

K závažným trestním činům musí být stanoveno opatření, které umožní legislativě shromažďovat záznam pomocí technických prostředků nebo spolupracovat s poskytovatelem služby, jenž by na základě svých stávajících technologií umožnil příslušným orgánům

shromažďovat a zaznamenávat obsažená data v reálném čase, v elektronických komunikacích a na území daného státu, pokud jsou data přenášena pomocí počítačového systému.

V rámci mezinárodní spolupráce Úmluva umožňuje přijmout legislativní a jiná právní opatření, která jsou nezbytná ke shromažďování a záznamu dat v počítačové síti nebo telekomunikaci. To vše pomocí speciálních technických prostředků. Právní úprava musí také počítat se zajištěním důvěrnosti u poskytovatele služeb i jakékoli další informaci o něm.

6.3 Zajištění mezinárodní spolupráce

Po přijetí této Úmluvy budou státy vzájemně a podle ustanovení příslušných platných mezinárodních dokumentů o mezinárodní spolupráci v trestních věcech postupovat na základě dohodnutých právních předpisů a vnitrostátních zákonů pro účely vyšetřování trestných činů, které se vztahují na počítačovou kriminalitu a shromažďování důkazů o této činnosti.

Stát vytvoří vybavené kontaktní místo, které má být k dispozici 24 hodin denně po celý rok, se zaškoleným personálem. Toto kontaktní místo poskytuje okamžitou pomoc v otázkách počítačové kriminality, vyšetřování a řízení trestních činů a zajišťování elektronických forenzních důkazů. Dále má poskytovat:

- technické rady,
- uchovávání dat,
- právní informace a lokalizaci podezřelé osoby,
- kontaktování jiného kontaktního místa.

6.3.1 Zásady vzájemné pomoci

Státy, jež podepsaly Úmluvu, se zavazují ke vzájemné pomoci v co nejširším rozsahu pro účely vyšetřování trestných činů, které se týkají počítačové kriminality, nebo ke shromažďování důkazů o trestné činnosti v elektronické podobě.

Každá ze smluvních stran může žádat o pomoc nebo sdělení informací prostřednictvím rychlých komunikačních prostředků – elektronická pošta, a to v rozsahu, který odpovídá přijatelnosti bezpečnostních opatření (šifrování). Na žádost tyto informace druhé straně formálně potvrdí. Dožadovaná strana odpoví jakýmkoli rychlým komunikačním prostřed-

kem. Úmluva garantuje poskytnutí mezinárodní pomoci, pokud se trestná činnost týká počítačové kriminality. Stát má také právo uplatňovat své nároky na poskytnutí mezinárodní pomoci.

Strany si mohou bez předchozí žádosti mezi sebou předávat informace získané v rámci svého vlastního vyšetřování v případě, kdy věří, že sdělované informace pomohou přijímané straně při zahájení vyšetřování týkajícího se trestních činů, které byly stanoveny v souladu s Úmluvou. Pokud se některý ze států rozhodne, že takové informace poskytne, může požadovat jejich utajení nebo použití jen za určitých podmínek. Pokud se druhá strana rozhodne přijmout tyto informace, je potom vázána podmínkami, které uvedla poskytující strana.

6.3.1.1 Přeshraniční přístup k datům

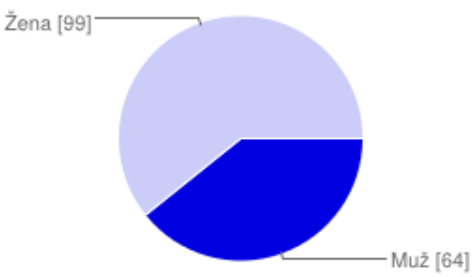
Každý účastník Úmluvy může požádat jinou stranu, aby data uložená prostřednictvím počítačového systému umístěného na jejich území podrobila prohlídce, umožnila prohlídku nebo poskytla přístup. K žádosti tohoto typu použije dotazovaná strana mezinárodních dokumentů a právních předpisů. Je zde i možnost urychleného vyřízení za předpokladu, že tato data jsou zvláště ohrožena ztrátou.

Data, která nepotřebují povolení jiné ze stran, se dají získat z veřejně dostupných zdrojů bez ohledu na geografické umístění nebo s pomocí počítačového systému, který je umístěn na území státu, jenž požaduje tyto informace. Další z možností je získat dobrovolný souhlas osoby, která má zákonnou pravomoc zpřístupňovat tato data druhým stranám srze počítačový systém umístěný v zemi této osoby. Smluvní strany si mohou taktéž pomáhat v poskytování obsahu odposlouchávaných dat (při shromažďování nebo zaznamenávání v reálném čase) přenášených počítačovým systémem v rozsahu, jakém to stanovují příslušné normy a vnitrostátní právní úprava. [1,9,14,15,26,27]

7 ZPRACOVÁNÍ DOTAZNÍKU

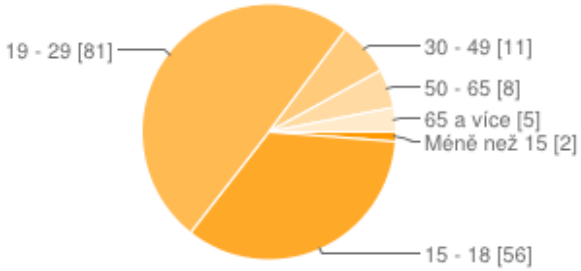
Tento anonymní dotazník byl vytvořen pomocí internetové služby drive.google.com na základě elektronického formuláře, který se skládá ze čtyř částí. Úvod slouží ke zjištění základních informací o respondentovi – jeho pohlaví, věk, dosažené vzdělání a národnost. Zbylé tři části (Používání internetu, Rizika internetu, Ochrana práv zákony ČR a mezinárodními smlouvami) se zaměřují na otázky informovanosti o rizicích internetu a některých oblastech počítačové kriminality. Výzkumu se zúčastnilo 163 osob.

7.1 Informace o respondentech



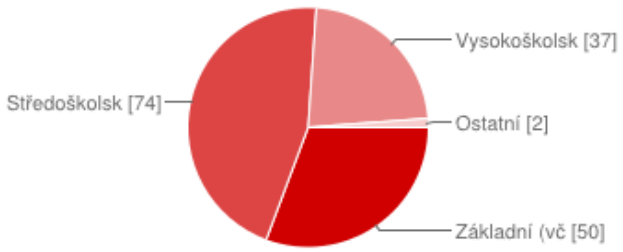
Muž	64	39 %
Žena	99	61 %

Obr. 9 – Pohlaví respondentů



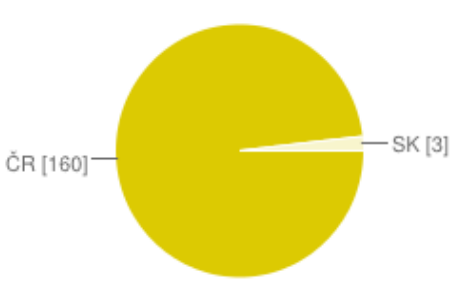
Méně než 15	2	1 %
15 - 18	56	34 %
19 - 29	81	50 %
30 - 49	11	7 %
50 - 65	8	5 %
65 a více	5	3 %

Obr. 10 – Věk respondentů



Základní (včetně žáků ZŠ)	50	31 %
Středoškolské	74	45 %
Vysokoškolské	37	23 %
Ostatní	2	1 %

Obr. 11 – Nejvyšší dosažené vzdělání respondentů

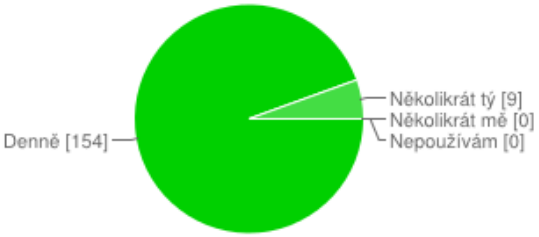


ČR	**160**	98 %
SK	**3**	2 %

Obr. 12 – Státní občanství

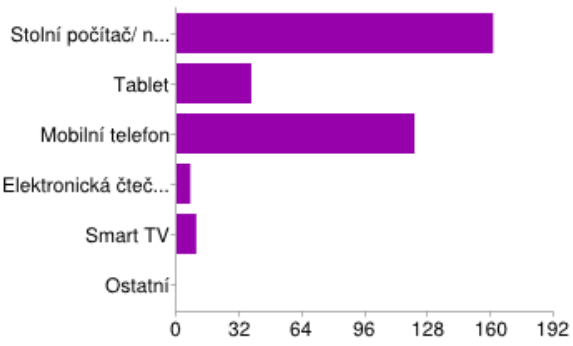
7.2 Využívání internetu

Téměř všichni respondenti využívají internet denně a připojují se přes stolní počítač nebo notebook, případně mobilní telefon. Vzhledem k začínajícímu trendu rozšiřování Smart TV se poměrně velká část respondentů připojuje i pomocí tohoto zařízení. Můžeme tedy konstatovat, že internet se stal každodenní součástí života moderního člověka.



Denně	**154**	94 %
Několikrát týdně	**9**	6 %
Několikrát měsíčně	**0**	0 %
Nepoužívám	**0**	0 %

Obr. 13 – Využívání internetu

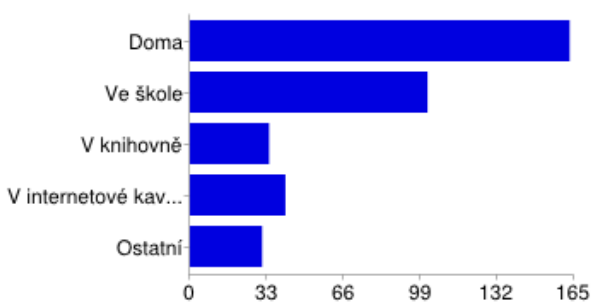


Stolní počítač/ notebook	**161**	48 %
Tablet	**38**	11 %
Mobilní telefon	**121**	36 %
Elektronická čtečka knih	**7**	2 %
Smart TV	**10**	3 %
Ostatní	**0**	0 %

Obr. 14 – Využití internetu na různých zařízení

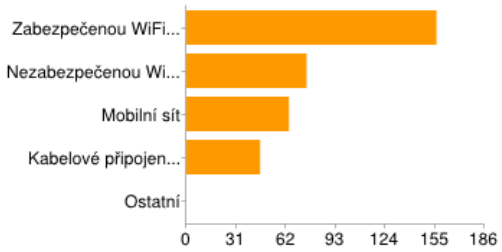
K připojování na internet dochází u dotazovaných osob téměř vždy doma pomocí zabezpečené sítě WiFi – k tomuto druhu připojení se váže vyšší zabezpečení sítě. Při připojování na internet skrze nezabezpečenou síť se uživatel vystavuje nebezpečí, které může mít

za následek odcizení osobních nebo jinak citlivých údajů. Z naměřených dat také vyplývá, že se stává připojení k internetu pomocí WiFi rozšířenější než kabelové připojení xDSL.



Doma	**163**	44 %
Ve škole	**102**	27 %
V knihovně	**34**	9 %
V internetové kavárně	**41**	11 %
Ostatní	**31**	8 %

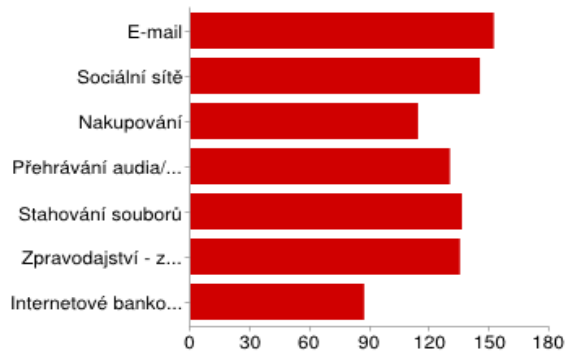
Obr. 15 – Místo využívání internetu



Zabezpečenou WiFi síť	**156**	46 %
Nezabezpečenou WiFi síť - veřejné přístupové body	**75**	22 %
Mobilní sít	**64**	19 %
Kabelové připojení (xDSL)	**46**	13 %
Ostatní	**0**	0 %

Obr. 16 – Druh připojení k internetu

Co se týká využívání poskytovaných služeb na internetu, lidé ve věkovém rozmezí 19 – 29 let nejčastěji používají internetové bankovnictví, email a nakupování, lidé do 18 let nejvíce navštěvují stránky věnované sociálním sítím (např. Facebook.com, Twitter.com).

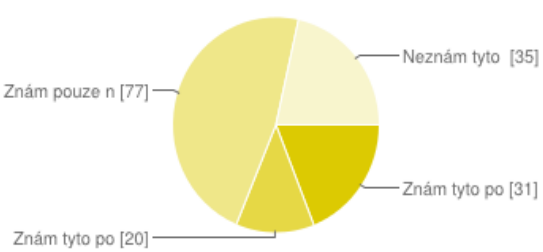


E-mail	**152**	17 %
Sociální sítě	**145**	16 %
Nakupování	**114**	13 %
Přehrávání audia/ videa	**130**	14 %
Stahování souborů	**136**	15 %
Zpravodajství - zprávy, počasí, atd...	**135**	15 %
Internetové bankovnictví	**87**	10 %

Obr. 17 – Využívání služeb na internetu

7.3 Pojmy počítačové kriminality

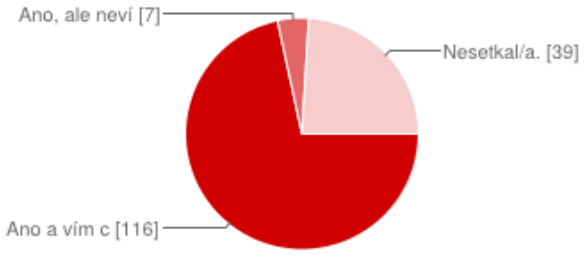
V této části jsme se zaměřili na znalost respondentů v pojmech počítačové kriminality. Z diagramu na obrázku č. 18 lze vyčíst znalost následujících pojmů: phishing, pharming, sociální inženýrství[1] a krádež identity[2]. Většina dotazovaných uvedla, že nezná alespoň některé z těchto výrazů. Poměrně malé procento je obeznámeno s těmito pojmy včetně znalosti jejich významu.



Znám tyto pojmy a vím co znamenají.	31	19 %
Znám tyto pojmy, ale nevím co znamenají.	20	12 %
Znám pouze některé z pojmů.	77	47 %
Neznám tyto pojmy.	35	21 %

Obr. 18 – Znalost základních pojmů počítačové kriminality

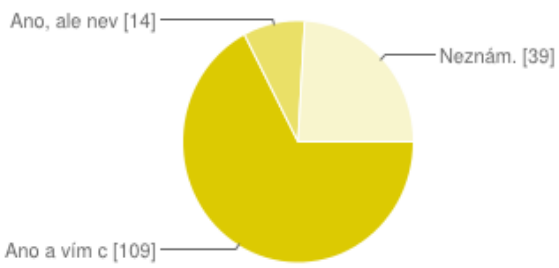
V rámci novějších druhů počítačové kriminality nás zajímalo, zda se dotazovaní setkali s pojmy kyberšikana[3], stalking[4] a kyberstalking[5]. Z následujících diagramů vyplývá, že společnost je vesměs obeznámena se zmíněnými pojmy. Stále však zůstává nemalé procento těch, kteří tato rizika internetu a moderních technologií neznají.



Ano a vím co znamená.	116	72 %
Ano, ale nevím co znamená.	7	4 %
Nesetkal/a.	39	24 %

Obr. 19 – Znalost pojmu kyberšikana

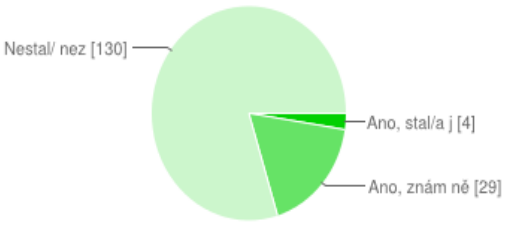
[1] Sociální inženýrství označuje vydávání se za jinou fyzickou či právnickou osobu se záměrem získat od této osoby informace k páchání počítačové kriminality.
[2] Krádež identity znamená odcizení osobních údajů k páchání trestné činnosti.
[3] Kyberšikana je šikana v kyberprostoru, tedy napadání jiné osoby pomocí internetu či jiných informačních a komunikačních technologií.
[4] Stalking značí opakované stupňované obtěžování.
[5] Kyberstalking je stalking v kyberprostoru – s využitím internetu, mobilních telefonů či jiných technologií.



Ano a vím co znamená.	**109**	67 %
Ano, ale nevím co znamená.	**14**	9 %
Neznám.	**39**	24 %

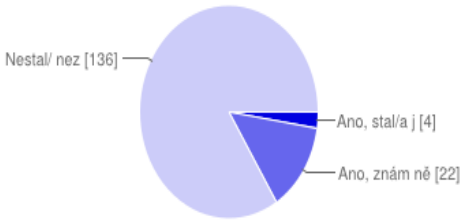
Obr. 20 – Znalost pojmu stalking a kyberstalking

Je pozitivní, že většina respondentů se zatím nikdy nestala cílem útoků těchto druhů počítačové kriminality. V následujících diagramech však vidíme, že někteří se bohužel obětí kyberšikany či kyberstalkingu stali nebo někoho takového znají.



Ano, stal/a jsem se obětí kyberšikany.	**4**	2 %
Ano, znám někoho, kdo se stal obětí kyberšikany.	**29**	18 %
Nestal/ neznám.	**130**	80 %

Obr. 21 – Oběti kyberšikany

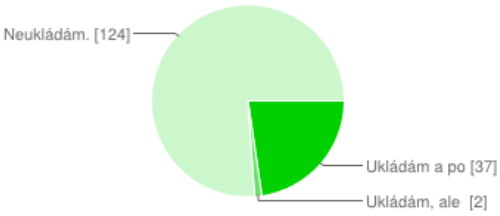


Ano, stal/a jsem se obětí stalkingu/ kyberstalkingu.	**4**	2 %
Ano, znám někoho, kdo se stal obětí stalkingu/ kyberstalkingu.	**22**	14 %
Nestal/ neznám.	**136**	84 %

Obr. 22 – Oběti stalkingu/ kyberstalkingu

7.4 Ochrana osobních údajů

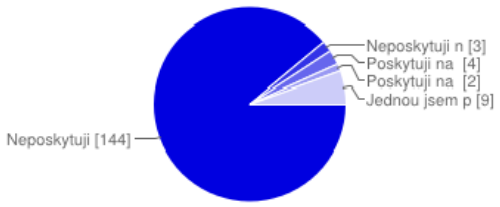
Vzhledem k tomu, že ochrana přihlašovacích údajů je jednou se základních a mezi veřejností nejrozšířenějších podmínek k ochraně osobních údajů, je překvapivé, že si nezanedbatelná část respondentů ukládá na svůj počítač přihlašovací údaje, a někteří dokonce ani nemají počítač chráněný.



Ukládám a počítač mám chráněný (heslo, antivirus).	37	23 %
Ukládám, ale počítač nemám chráněný.	2	1 %
Neukládám.	124	76 %

Obr. 23 – Ukládání přihlašovacích údajů (např. do internetového bankovnictví) na PC

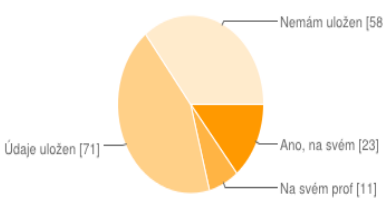
Osobní údaje si však téměř všichni respondenti chrání tím, že je přímo neposkytují. Vzhledem k vysokému počtu respondentů, kteří se takto vyjádřili, se ale domníváme, že si spousta z nich neuvědomuje, co poskytování údajů znamená. Jelikož dříve uváděli, že používají nakupování přes internet, zákonitě musí obchodníkovi obvykle v elektronickém formuláři své údaje poskytnout. V tomto případě si zákazník nemůže ověřit, ke komu se data dostanou, přestože by měla být chráněna zákonem. Očividně lidé nevidí riziko, které představuje např. výše popsaná metoda pharming.



Neposkytuji.	144	89 %
Neposkytuji na internetu, ale telefonicky ano.	3	2 %
Poskytuji na internetu, ale ne po telefonu.	4	2 %
Poskytuji na internetu i po telefonu.	2	1 %
Jednou jsem poskytl/a (nezáleží jakým způsobem).	9	6 %

Obr. 24 – Poskytování osobních údajů

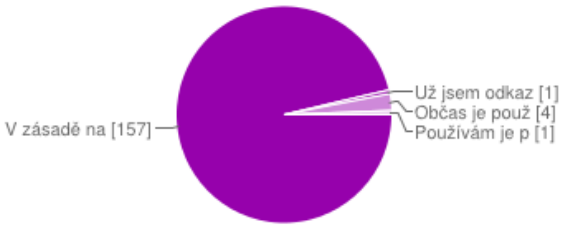
Obrovský rozmach sociálních sítí (především Facebook.com) způsobil, že uživatelé internetu dobrovolně poskytují osobní údaje na svých profilech, aniž by v tom viděli možná rizika, což vyplývá i z následujícího diagramu.



Ano, na svém profilu mám veřejně uvedeny osobní údaje.	23	14 %
Na svém profilu nemám uloženy své osobní údaje, ale pokud si je někdo vyžádá, údaje poskytnu.	11	7 %
Údaje uložené mám, ale neposkytuji je veřejnosti.	71	44 %
Nemám uložené své osobní údaje na sociálních sítích.	58	36 %

Obr. 25 – Osobní údaje na sociálních sítí

V souvislosti s rizikem spojeným se spamy, sociálním inženýrstvím a formou počítačové kriminality phishing jsme se ptali na používání odkazů na internetové stránky obsažené v nevyžádaných emailech. Z diagramu je zřejmé, že jsou lidé obeznámeni s problémem phishingu, přestože tento pojem mnohdy neznají. Pouze zanedbatelný počet respondentů si toto rizika neuvědomuje.

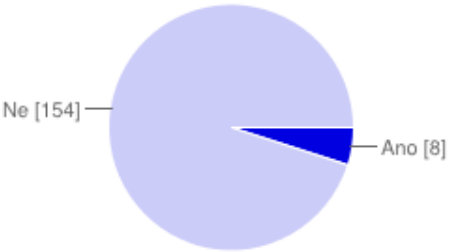


V zásadě na tyto e-maily nereaguji.	157	96 %
Už jsem odkazy někdy použil/a.	1	1 %
Občas je použiji.	4	2 %
Používám je pravidelně/ většinou.	1	1 %

Obr. 26 – Používání odkazů obsažených v nevyžádaných emailech

7.5 Obrana proti počítačové kriminalitě

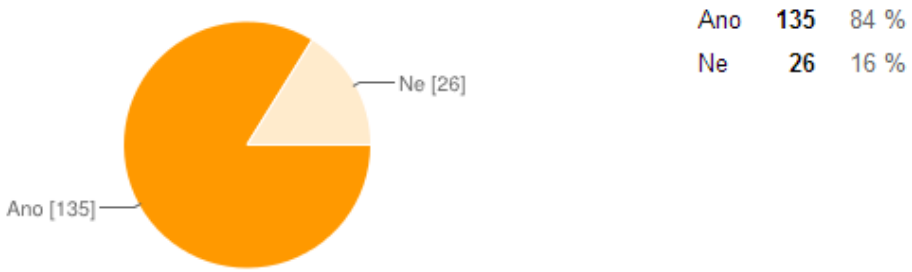
5 % dotázaných se přímo stalo obětí počítačové kriminality.



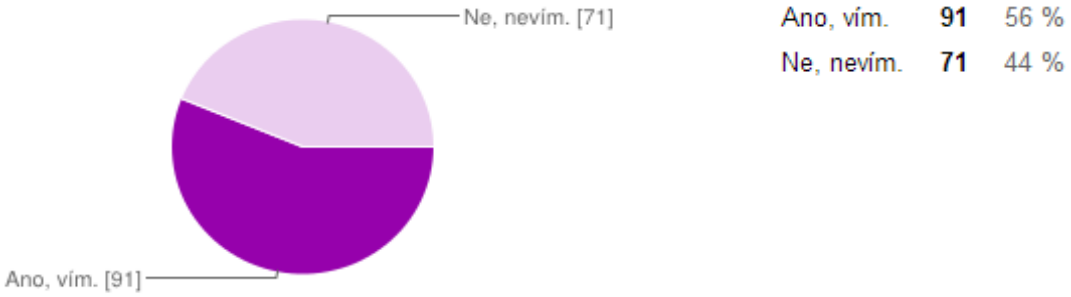
Ano	8	5 %
Ne	154	95 %

Obr. 27 – Oběti počítačové kriminality

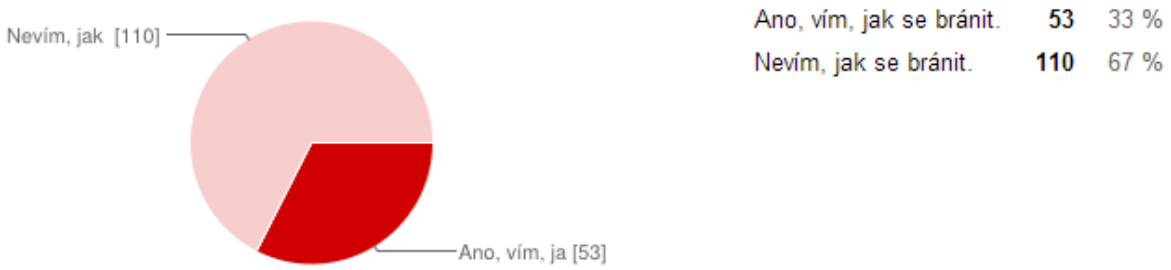
Přestože si většina respondentů myslí, že v ČR existují zákony proti počítačové kriminalitě, mnozí z nich nevědí, na koho se obrátit a jak se bránit v případě, že se stanou obětí nějakého kyberzločinu.



Obr. 28 – Existence zákonů proti počítačové kriminalitě v ČR



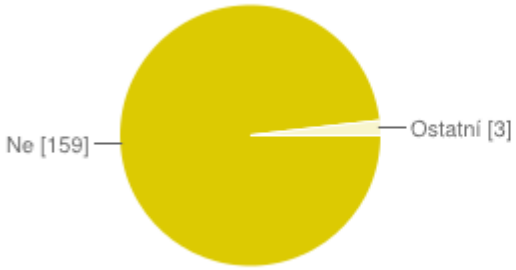
Obr. 29 – Povědomí o tom, na koho se obrátit v případě, že se člověk stane obětí počítačové kriminality



Obr. 30 – Znalost možností obrany proti počítačové kriminalitě v ČR a EU

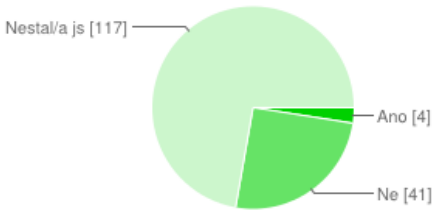
Drtivá většina dotázaných nikdy počítačovou kriminalitu nenahlašovala, což lze vyčíst z diagramu na obr. č. 31. Pole „ostatní“ představovalo odpověď „ano“ a bylo použito, aby respondenti mohli uvést konkrétní orgán, který kontaktovali. V tomto případě kontaktovali Policii ČR. Jednalo se o respondenty, kteří se sami stali obětí kyberzločinu. Někteří z nich také uvedli, že se bránili pomocí zákonů či mezinárodních smluv.

Je však také zřejmé, že přestože lidé znají možnosti obrany, sami se bojí či z jiných důvodů nechtějí kontaktovat příslušné státní orgány a mezinárodní instituce a situaci řešit.



Ne	**159**	98 %
Ostatní	**3**	2 %

Obr. 31 – Nahlášení počítačové kriminality



Ano	**4**	2 %
Ne	**41**	25 %
Nestal/a jsem se obětí počítačové kriminality.	**117**	72 %

Obr. 32 – Obrana pomocí zákonů či mezinárodních smluv

ZÁVĚR

Počítačová kriminalita je v současné době velmi diskutovaným problémem. Od zavedení nového trestního zákoníku v roce 2009, ve kterém je obsažena řada kriminalizovaných zločinů, se počítačová kriminalita dá trestat ve větší míře. Postihy za tuto trestnou činnost nejsou nijak zvláště vysoké, tomu je přisuzován stále zvyšující se počet případů počítačové kriminality.

Tato diplomová práce rozebrala základní projevy tohoto druhu kriminality a předkládá programy, agentury a organizace, které se touto problematikou zabývají především na mezinárodní úrovni. Důraz byl kladen na systematičnost a ucelenost, aby byla vystižena hlavní část trestné činnosti páchané skrze počítačové systémy. Taktéž byl proveden rozbor jednoho mezinárodního dokumentu, který přispěl k vytvoření několika paragrafů do našeho trestního zákoníku a na základě kterého začaly vznikat instituce a organizace pro boj proti počítačové kriminalitě.

Po analýze všech mezinárodních organizací, tedy těch, které pracují na nadnárodní úrovni a komunikují s celým světem, se dá říci, že tyto organizace vysoce přispívají svou činností ke snižování trestné činnosti a ke zdokonalení boje proti počítačové kriminalitě. Svou roli zde hraje také soukromý sektor, který svým vývojem a výzkumem nemálo přispívá právě k tomuto boji.

Údaje, které jsme shromáždili prostřednictvím dotazníku, vypovídají o tom, že lidé se sice běžně setkávají s počítačovou kriminalitou, ale nahlašování a řešení této činnosti nepřikládají příliš velký důraz. Taktéž se ve velké míře porušují základní otázky bezpečnosti, neboť si lidé správným způsobem nechrání svůj počítač a přihlašují se často do sítě internet přes nezabezpečený bod připojení.

Navrhovaným řešením, jak veřejnosti poskytovat důležité a aktuální informace o možnostech ochrany a jak zvýšit procento lidí, kteří by se proti těmto činům bránili, je větší propagace 1.) rizik internetu a moderních technologií obecně a 2.) obrany proti kyberzločinům. Tato propagace by mohla být uskutečňována nejlépe prostřednictvím médií. Jednalo by se např. o krátké spoty v televizním vysílání, vyobrazení kriminálních činů skrze webové stránky.

SEZNAM POUŽITÉ LITERATURY

[1] 11. Kongres OSN o prevenci kriminality a trestní justici. In: Základní dokumenty 11. kongresu předložené delegátům. 2006. Dostupné z: http://www.ok.cz/iksp/docs/322.pdf.

[2] ČERVEŇ, P. Cracking a jak se proti němu bránit, Brno: Computer Press, 2003.

[3] Česká republika. Zákon trestní zákoník. In: Sbírka zákonů. Tiskárna Ministerstva vnitra, p. o., 2009. Dostupné z: www.mvcr.cz/soubor/sb011-09-pdf.aspx.

[4] DOLEŽAL, M. Kyberútokům se musí umět bránit každá země, tvrdí šéf specialistů NATO. Datum vydání: 4. 1. 2012. Dostupný z WWW: <http://zpravy.idnes.cz/kyberutokum-se-musi-umet-branit-kazda-zeme-tvrdi-sef-specialistu-nato-1eh-/zpr_nato.aspx?c=A120104_130737_zpr_nato_inc.

[5] DOLEŽAL, Martin. NATO se snaží svázat kyber-prostor. In: NatoAktual.cz [online]. 2011 [cit. 2014-05-05]. Dostupné z: http://www.natoaktual.cz/nato-se-snazi-svazat-kyber-prostor-prvni-cast-f4j-/na_analyzy.aspx?c=A111205_164033_na_analyzy_m02.

[6] DOLEŽAL, Martin. NATO svazuje kyber-prostor. In: NatoAktual.cz [online]. 2011 [cit. 2014-05-05]. Dostupné z: http://www.natoaktual.cz/nato-svazuje-kyber-prostor-druha-cast-dxs-/na_analyzy.aspx?c=A111212_091109_na_analyzy_m02.

[7] FLÍDR, Tomáš. Mezinárodní právo kyberprostoru a Talinský manuál. [online]. [cit. 2014-05-20]. Dostupné z: http://www.kyberbezpecnost.cz/?p=198.

[8] INTERPOOL. Activitis [online]. 2014 [cit. 2014-05-10]. Dostupné z: http://www.interpol.int/Crime-areas/Cybercrime/Activities/Harmonization.

[9] JELÍNEK J. Trestní právo hmotné, Obecná část, Praha: Linde, 2004, 277s.

[10] KŘÍŽ, Zdeněk. 12. kongres OSN o prevenci kriminality a trestní justici: Salvador, Brazílie, 12.- 19. dubna 2010. Vyd. 1. Praha: Institut pro kriminologii a sociální prevenci, 2010, 185 s. Prameny (Institut pro kriminologii a sociální prevenci). ISBN 978-807-3381-028.

[11] KŘÍŽ, Zdeněk. Adaptace Severoatlantické aliance na nové mezinárodní bezpečnostní prostředí: aplikace přístupů konceptu kooperativní bezpečnosti. 1. vyd. Brno: Mezinárodní politologický ústav MU, 2006, 217 s. Vysokoškolské učebnice (Aleš Čeněk). ISBN 80-210-4218-4.

[12] MACHÁČEK, Miloslav. Počítačová kriminalita a bezpečnost. [online]. 2013 [cit. 2014-05-20]. Dostupné z: http://www.internetprovsechny.cz/pocitacova-kriminalita-a-bezpecnost/.

[13] MATĚJKA, M. Počítačová kriminalita, Praha: Computer Press, 2002, str. 42.

[14] Mezinárodní spolupráce v boji proti informační kriminalitě. Mezinárodní spolupráce v boji proti informační kriminalitě [online]. 2009 [cit. 2014-05-20]. Dostupné z: www.mvcr.cz/soubor/cyber-vyzkum-studie-mezinarodni-pdf.aspx.

[15] MUSIL, Stanislav. INSTITUT PRO KRIMINOLOGII A SOCIÁLNÍ PREVENCE. Počítačová kriminalita: Nástin problematiky, Kompendium názorů specialistů. Praha, 2000.

[16] NETOPILÍK, Petr. Realizace mezinárodní ochrany v ČR. Institut mezioborových studií, 2008. Bakalářská. UTB. Vedoucí práce Kejdová Miroslava.

[17] OBR ML., Jiří. Sniffing: Odposlech datové komunikace. [online]. [cit. 2014-04-20]. Dostupné z: http://www.itbiz.cz/sniffing-odposlech-datove-komunikace.

[18] ONDŘEJ, Jan. Mezinárodní právo veřejné, soukromé, obchodní. 4. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012, 476 s. Vysokoškolské učebnice (Aleš Čeněk). ISBN 978-807-3803-483.

[19] PIKNA, Bohumil. Evropský prostor svobody, bezpečnosti a práva (prizmatem Lisabonské smlouvy). 3. rozš. vyd. Praha: Linde, 2012, 435 s. ISBN 978-80-7201-889-5.

[20] Počítačová kriminalita. NewsLab [online]. 2014 [cit. 2014-04-21]. Dostupné z: http://www.newslab.cz/cyber-crime/.

[21] Počítačová kriminalita pod lupou: Celosvětový průzkum hospodářské kriminality - Česká republika. In: Pwc.cz [online]. PricewaterhouseCoopers, 2011 [cit. 2014-04-10]. Dostupné z: http://www.pwc.com/cz/en/hospodarska-kriminalita/assets/Crime_survey_CR_czech_ele.pdf.

[22] Právní předpisy a jiné akty. Interstitucionální spis: 2011/0166 (NLE), Brusel 12. září 2011, 12196/2/11 REV (cs).

[23] První phishing v Česku, terčem byla CitiBank. Finance.cz [online]. 2006 [cit. 2014-03-01]. Dostupné z: http://www.finance.cz/zpravy/finance/63677-prvni-phishing-v-cesku-tercem-byla-citibank/.

[24] TIKK, Eneken a Anna-Maria TALIHÄRM. International Cyber Security Legal & Policy Proceedings. USA: CCD COE Publications, 2010. ISBN 978-9949-9040-4-4. Dostupné z: http://www.ccdcoe.org/245.html.

[25] TOP 5 hrozeb a ohrožení zabezpečení firem v uplynulém roce. Systémonline.cz [online]. 2013 [cit. 2014-05-12]. Dostupné z: http://www.systemonline.cz/images_aqua/2013/listopad/EY_top5.jpg.

[26] Úmluva o počítačové kriminalitě. In: Sněmovní tisk 890/0, část č. 1/7. 2001. Dostupné z: http://www.psp.cz/sqw/text/tiskt.sqw?o=6&ct=890&ct1=0.

[27] WAISOVÁ, Šárka. Řešení konfliktů v mezinárodních vztazích: aplikace přístupů konceptu kooperativní bezpečnosti. 1. vyd. Plzeň: Aleš Čeněk, 2011, 250 s. Vysokoškolské učebnice (Aleš Čeněk). ISBN 978-807-3803-391.

[28] What is NATO. NATO.int [online]. 2014 [cit. 2014-05-18]. Dostupné z: http://www.nato.int/nato-welcome/index.html.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BBS	Bulletin Board Systém – systém elektronických nástěnek
CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
CI2RCO	Critical Information Infrastructure Research Co-ordination – Koordinace výzkumu v oblasti kritické informační infrastruktury
DOS	Disk Operating Systém – diskový operační systém
DNS	Domain Name System – hierarchický systém doménových jmen
ENISA	European Network and Information Security Agency – Evropská agentura pro síťovou a informační bezpečnost
EU	Evropská unie
ICT	Information and Communication Technologies – informační a komunikační technologie
IGCI	Středisko INTERPOOL Global Complex for Inovations
INHOPE	International Association of Internet Hotlines – Internetová asociace horkých linek
INTERPOOL	International Criminal Police Organization – Mezinárodní policejní organizace
IP	Internetový protokol
ISP	Internet Service Providers
IT	Informační technologie
MHD	Městská hromadná doprava
NATO	North Atlantic Treaty Organisation – Severoatlantická aliance
NC3B	NATO Consultation, Command and Control Board
NCIRC	National Criminal Intelligence Resource Center
p2p	Peer-to-peer – Rovný s rovným

PC	Personal computer – osobní počítač
PIN	Personal identification number – Osobní identifikační číslo
OBSE	Organizace pro bezpečnost v Evropě (OSCE)
OECD	Organisation for Economic Co-operation and Development – Organizace pro hospodářskou spolupráci a rozvoj
OSCE	Organization for Security and Cooperation in Europe – Organizace pro bezpečnost a spolupráci v Evropě (OBSE)
OSN	Organizace spojených národů
RFID	Radio Frequency Identification – Identifikace na rádiové frekvenci
TCP	Transmission Control Protocol – Primární přenosový protokol

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK MEZINÁRODNÍ SPOLUPRÁCE V BOJI PROTI POČÍTAČOVÉ KRIMINALITĚ

Dobrý den,

jmenuji se Vladimír Stojaspal a jsem studentem 2. ročníku navazujícího magisterského studia Univerzity Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, obor Bezpečnostní technologie, systémy a management.

Tento dotazník je součástí mé diplomové práce na téma Mezinárodní spolupráce při otírání počítačové kriminality. Dotazník je zcela anonymní a výsledky budou použity výhradně pro potřeby mé diplomové práce. Dotazník se zaměřuje na identifikaci počítačové kriminality, její formy a informovanost veřejnosti o tomto problému. Vyplnění dotazníku zabere cca 5 minut.

Děkuji Vám za spolupráci.

Bc. Vladimír Stojaspal
lada.stojaspal@gmail.com

Pohlaví: *

- ○ Muž
- ○ Žena

Věk: *

- ○ Méně než 15
- ○ 15 - 18
- ○ 19 - 29
- ○ 30 - 49
- ○ 50 - 65
- ○ 65 a více

Nejvyšší dosažené vzdělání: *

- ○ Základní (včetně žáků ZŠ)
- ○ Středoškolské
- ○ Vysokoškolské
- ○ Jiné:

Státní občanství: *

- ČR
- SK

Používání internetu

Jak často využíváte internet? *

- Denně
- Několikrát týdně
- Několikrát měsíčně
- Nepoužívám

Na jakých přístrojích používáte internet? *

Možnost více odpovědí.

- Stolní počítač/ notebook
- Tablet
- Mobilní telefon
- Elektronická čtečka knih
- Smart TV
- Jiné:

Kde se připojujete k internetu? *

Možnost více odpovědí.

- Doma
- Ve škole
- V knihovně
- V internetové kavárně
- Jiné:

Pro připojení na internet využíváte: *

Možnost více odpovědí.

- Zabezpečenou WiFi síť
- Nezabezpečenou WiFi síť - veřejné přístupové body
- Mobilní sít
- Kabelové připojení (xDSL)
- Jiné:

Co všechno využíváte na internetu? *

Možnost více odpovědí.

- [ ] E-mail
- [ ] Sociální sítě
- [ ] Nakupování
- [ ] Přehrávání audia/ videa
- [ ] Stahování souborů
- [ ] Zpravodajství - zprávy, počasí, atd...
- [ ] Internetové bankovnictví

Rizika internetu

Znáte následující pojmy: phishing, pharming, sociální inženýrství, krádež identity?

Vyberte jednu možnost.

- ( ) Znám tyto pojmy a vím co znamenají.
- ( ) Znám tyto pojmy, ale nevím co znamenají.
- ( ) Znám pouze některé z pojmů.
- ( ) Neznám tyto pojmy.

Ukládáte si své přihlašovací údaje (např. do internetového bankovnictví, číslo kreditní karty) ve svém počítači?

- ( ) Ukládám a počítač mám chráněný (heslo, antivirus).
- ( ) Ukládám, ale počítač nemám chráněný.
- ( ) Neukládám.

Používáte odkazy na internetové stránky, které jsou obsaženy v nevyžádaných e-mailech?

Např: "Půjčíme Vám až 1 000 000 Kč na cokoliv!", "Úspěšné hubnutí už za 5 týdnů!" apod.

- ( ) V zásadě na tyto e-maily nereaguji.
- ( ) Už jsem odkazy někdy použil/a.
- ( ) Občas je použiji.
- ( ) Používám je pravidelně/ většinou.

Poskytujete své osobní údaje bez toho, aniž byste si ověřili, s kým komunikujete?

Rodné číslo, adresa trvalého bydliště, číslo účtu/ karty...

- ( ) Neposkytuji.
- ( ) Neposkytuji na internetu, ale telefonicky ano.

- Poskytuji na internetu, ale ne po telefonu.
- Poskytuji na internetu i po telefonu.
- Jednou jsem poskytl/a (nezáleží jakým způsobem).

Poskytujete své osobní údaje na sociálních sítích?

Facebook, Twitter, Lidé.cz...

- Ano, na svém profilu mám veřejně uvedeny osobní údaje.
- Na svém profilu nemám uloženy své osobní údaje, ale pokud si je někdo vyžádá, údaje poskytnu.
- Údaje uložené mám, ale neposkytuji je veřejnosti.
- Nemám uložené své osobní údaje na sociálních sítích.

Setkali jste se s pojmem kyberšikana?

- Ano a vím co znamená.
- Ano, ale nevím co znamená.
- Nesetkal/a.

Znáte pojem stalking a kyberstalking?

- Ano a vím co znamená.
- Ano, ale nevím co znamená.
- Neznám.

Stali jste se Vy nebo někdo z vašich blízkých obětí kyberšikany?

Kyberšikana je šikanování jiné osoby s využitím internetu, mobilních telefonů či IT technologií.

- Ano, stal/a jsem se obětí kyberšikany.
- Ano, znám někoho, kdo se stal obětí kyberšikany.
- Nestal/ neznám.

Víte na koho se máte obrátit v případě, že jste se stali obětí počítačové kriminality?

- Ano, vím.
- Ne, nevím.

Stali jste se Vy nebo někdo z vašich blízkých obětí stalkingu/ kyberstalkingu?

Zneužívání internetu či IT technologií k opakovanému stupňujícímu obtěžování telefonáty, SMS zprávami, atd.

- Ano, stal/a jsem se obětí stalkingu/ kyberstalkingu.
- Ano, znám někoho, kdo se stal obětí stalkingu/ kyberstalkingu.

- Nestal/ neznám.

Ochrana práv zákony ČR a mezinárodními smlouvami

Myslíte si, že v ČR existují zákony související s počítačovou kriminalitou?

- Ano
- Ne

Víte, jak se můžete bránit proti počítačové kriminalitě v ČR a EU?

- Ano, vím, jak se bránit.
- Nevím, jak se bránit.

Kontaktovali jste někdy příslušný státní orgán, aby jste nahlásili počítačovou kriminalitu?

Pokud ano, do kolonky "jiné" napište, jaký státní orgán jste kontaktovali (Policii ČR, atd.).

- Ne
- Jiné:

Bránili jste se počítačové kriminalitě pomocí zákonů či mezinárodních smluv?

- Ano
- Ne
- Nestal/a jsem se obětí počítačové kriminality.

Znáte internetový portál E-bezpečí.cz?

- Ano
- Ne

Stali jste se někdy obětí počítačové kriminality?

- Ano
- Ne

Kontaktovali jste nějakou soukromou agenturu?

Vzhledem k řešené problematice. Pokud ano, do kolonky "jiné" napište jakou.

- Ne
- Jiné:

Dotazník v elektronické podobě naleznete na adrese:

http://goo.gl/hTLfmd