UNIVERZITA PALACKÉHO V OLOMOUCI

Právnická fakulta

Pavel Burian

Počítačová kriminalita a softwarové pirátství z pohledu kriminalistiky a trestního práva

Diplomová práce

Olomouc 2011

Prohlašuji, že jsem diplomovou práci na téma *Počítačová kriminalita a softwarové pirátství z pohledu kriminalistiky a trestního práva* vypracoval samostatně a citoval jsem všechny použité zdroje.

V Olomouci dne 25. 2. 2011 .....

OBSAH

Seznam použitých zkratek:

TrZ - Zákon č. 40/2009 Sb., trestní zákon, ve znění pozdějších předpisů

TrŘ - Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů

LZPS - Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů

BSA - Business Software Aliance

EU - Evropská unie

EFF - Electronic Frontier Foundation

ČVUT - České vysoké učení technické v Praze

PC - počítač

USA - Spojené státy americké

OSN - Organizace spojených národů

WIPO - Světová organizace duševního vlastnictví

IP - Internetový protokol

AutZ. - aktuální znění: zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů

MSN - Microsoft Network

ICQ - I Seek You

DoS - Denial of Service

CD - Compact Disk

Úvod

V úvodu své diplomové práce zabývající se *Počítačovou kriminalitou a softwarovým pirátstvím z pohledu kriminalistiky a trestního práva* bych chtěl nejprve provést stručný historický exkurz do oblasti počítačové kriminality v České republice a v zahraničí. Téma historie se ostatně v různých podobách a souvislostech objeví také v dalších kapitolách této práce. Mým primárním cílem je poukázat na hlavní a aktuální témata tohoto odvětví. Esenciálním bodem práce je vyšetřování počítačové kriminality, popis jednotlivých trestných činů z trestněprávního hlediska a v neposlední řadě fenomén softwarového pirátství a možnosti prevence tohoto druhu kriminality.

Mnoho autorů upozorňuje na rychlý vývoj nových technologií, nákladnost vyšetřování a vysoké požadavky na kvalifikaci vyšetřovatelů počítačové kriminality. Jedná se o nekonečný boj mezi počítačovými hackery, crackery na straně jedné a orgány činnými v trestním řízení na straně druhé. Pachatelé jsou většinou o krok napřed a vymýšlejí stále nové a sofistikovanější způsoby, jak zastřít svou činnost, ztížit odhalování stop a nalezení místa činu, odkud k útoku došlo. Informační technologie jsou již dlouhou dobu součástí každodenního života velké části společnosti, a přestože existuje mnoho pozitivních aspektů, které je provázejí, vzrůstají také možnosti potenciálních pachatelů této trestné činnosti. Z tohoto důvodu je dalším z mých cílů definovat ta nejdůležitější jednání pachatelů a případné způsoby zneužití těchto technologií.

Ať již v soukromém či veřejném životě, je obtížné nalézt oblast, kam by nezasahovaly informační technologie a kde by nebylo nutné užití stolního počítače popřípadě komunikace prostřednictvím sítě Internet. Obecně se diskutuje o době informační společnosti resp. o době post-informační.[1]

S vývojem nových a propracovaných technologií souvisí také potřeba stále aktuální a dokonalejší právní úpravy, která bude potenciální protiprávní jednání pachatelů s dostatečnou mírou postihovat. Současný zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen „TrZ“) obsahuje několik nových skutkových podstat, kterými se zákonodárce snažil reagovat na rychlý, řekl bych až bouřlivý, vývoj této oblasti kriminality. Tak je tomu nejen v České republice, ale také v zahraničí. Velkou roli na vývoj v této oblasti má hlavně fenomén sítě Internet a jeho globální charakter, demokratické až anarchistické základy. Jak uvádí Vladimír Smejkal, problém není v neexistenci právní úpravy, ale spíše

[1] SMEJKAL, Vladimír. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. *Trestněprávní revue*, 2003, č. 6, s. 161.

v aplikaci platného práva. V tak dynamicky se rozvíjející oblasti jako jsou počítačové technologie, Internet aj., je aplikace právních předpisů přinejmenším obtížná.[2]

Svá specifika má počítačová kriminalita také v oblasti procesní, tedy při dokazování, vyhledávání stop orgány činnými v trestním řízení a při dalších činnostech souvisejících s vyšetřováním. K metodice vyšetřování počítačových deliktů se vyjadřuje např. Václav Jirovský. Dle jeho názoru je při vyšetřování nutné zodpovědět pět stěžejních otázek: kdo, co, kde, kdy a proč.[3]

Další z kapitol této práce se zabývá problematikou porušování autorského práva v podobě softwarového pirátství, tedy neoprávněného užívání počítačových programů. Mou snahou je vystihnout a popsat ta nejdůležitější jednání, o kterých hovoříme v souvislosti s trestným činem porušení autorského práva dle ustanovení § 270 TrZ.

Věnovat se budu nejen platné právní úpravě na území České republiky, ale také legislativní činnosti na poli Evropské unie, zejména v rámci sekundární legislativy.

[2] SMEJKAL, Vladimír. Internet a §§§. 2. vydání. Praha: Grada Publishing, spol. s.r.o., 2001. s. 14
[3] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vydání. Praha: Grada Publishing, spol. s.r.o., 2007. s. 255

1 VYMEZENÍ ZÁKLADNÍCH POJMŮ[4]

Hacking

je úmyslné překonání bezpečnostního opatření, a tím neoprávněný průnik do informačního systému jiné osoby s postihem za neoprávněný přístup k počítačovému systému a nosiči informací dle ustanovení § 230 a 231 TrZ. Hacker je pachatel takového činu.

Cracking

je prolamování a obcházení technické ochrany zabudované v počítačových programech či jiných produktech včetně obcházení tzv. hardwarových klíčů, je postižitelný dle ustanovení § 270 TrZ jako porušování autorského práva, práv souvisejících a práva k databázi. Pachatel takového činu se nazývá Cracker.

Phishing

je podvodné získávání bezpečnostních hesel a kódů od uživatelů na Internetu či sítě mobilních telefonů, zejména rozesílání zpráv tvářících se jako originální, např. z bank, knihoven, od operátorů sítí elektronických komunikací aj.

Malware

je počítačový program, který poškozuje uživatele. Jedná se zejména o počítačové viry, červy, trojské koně. Postihováno dle ustanovení § 230, 232, popř. § 228 TrZ.

Warez

je internetové pirátství, šíření nelegálních počítačových programů či jiných produktů chráněných autorským právem sítěmi elektronických komunikací včetně nelegálního zpřístupňování nebo sdílení hudebních či audiovizuálních autorských děl a zvukových záznamů systémem peer-to-peer.

Peer-to-peer sítě

pojem vychází z angličtiny – „rovný s rovným“. V této síti spolu uživatelé komunikují přímo, bez zprostředkování komunikace pomocí specializovaných počítačů – serverů. Každý počítač připojený k této síti slouží zároveň jako klient i jako server. Všechny připojené počítače jsou si tedy podle jejího protokolu rovny.[5]

Pharming

je podvodné přesměrování zákazníka na falešné webové stránky internetového

[4] HENDRYCH, Dušan a kol. *Právnický slovník*. 3. vydání. Praha: C.H.BECK, 2009. 1488 s.
[5] MINÁRIK, Tomáš. Peer-to-peer sítě z hlediska trestního práva. In HORYNA, Mojmír (ed). *Český právní řád a ochrana kyberprostoru: (vybrané problémy)*. Praha: Karolinum, 2008, s. 66

bankovnictví, kde se požadují další údaje např. pro autorizační SMS zprávy zasílané na mobilní telefon uživatele aj. Jedná se o sofistikovanější formu jiného nelegálního činu – phishing.

Spyware

je počítačový program, který bez vědomí a svolení uživatele odesílá z jeho počítače data na určenou adresu, což umožňuje nejen monitorování práce uživatele, zjišťování internetových adres, které navštívil (a tím i jeho zájem), prohlížení datových souborů v jeho počítači atp., ale také zjišťování bezpečnostních kódů, čísel účtů, kreditních karet atp.

Počítačové viry

jsou počítačové programy, které ničí data v počítači. Do počítače pronikají z Internetu či CD a množí se v něm.

Sniffing

je neoprávněné monitorování cizí elektronické komunikace („internetové čmuchání“). Sniffer je počítačový program, který tuto nelegální činnost umožňuje. Postižitelné jako porušování tajemství přepravovaných zpráv dle ustanovení § 182 TrZ.

Trojské koně

jsou počítačové programy, které jsou zdánlivě neškodné (např. v podobě hry, obrázku či zprávy), ale jsou nosiči počítačových virů a červů, které proniknou do počítače a po spuštění počítače se v něm aktivují.

Electronic Frontier Foundation

Mezinárodní nezisková organizace se sídlem v USA (San Francisco). Hlavním bodem jejího zájmu je boj za svobodný Internet.[6]

[6] viz. http://www.eff.org/

2 CHARAKTERISTIKA A OBSAH POČÍTAČOVÉ KRIMINALITY

2.1 Pojem počítačová kriminalita

Počítačovou kriminalitu lze chápat jako označení určité specifické skupiny trestných činů. Tyto mají určité společné znaky, např. specifické rysy osoby pachatele. Možnosti využití počítačů se stále rozšiřují. Prvotními úkoly stolních počítačů byly jednoduché matematické operace a výpočty. Později spolu zařízení začala komunikovat prostřednictvím sítě. A tento okamžik bychom mohli považovat za období vzniku počítačové kriminality.[7]

Na samotný pojem „počítačová kriminalita" existují různé pohledy a názory. Pojetí tedy není jednotné a snadno definovatelné. Jak již bylo nastíněno, jedná se o jednu z nejrychleji se vyvíjejících oblastí v rámci kriminality obecně. Důležitým hlediskem je skutečnost, že počítačová kriminalita je činnost charakterizovaná tím, že ji lze spáchat pouze s využitím výpočetní techniky. Tato může být předmětem trestného činu (zde vyjma případů, kdy jsou předmětem trestné činnosti komponenty počítače jako věci movité), nebo pachatelovým nástrojem. Počítačová kriminalita se může týkat také obsahu počítače, tedy dat a příslušného softwaru, který může být upraven nebo pozměněn. Mnozí zastávají širší pojetí tohoto druhu kriminality. Například K. Novák hovoří o jakékoliv trestné nebo nekalé činnosti páchané pomocí počítačů.[8] Václav Jirkovský zastává názor, že označení počítačová kriminalita neboli „IT crime", „cybercrime", „kybernetická kriminalita" a v poslední době často používaný termín „informační a informatická kriminalita"[9] znamená jakýkoliv čin směřující k narušení nebo zneužití počítače nebo počítačového systému a informací v něm obsažených.[10]

2.1.1 Kybernetická kriminalita

Slovní spojení „kybernetická kriminalita" nevychází z pojmu kybernetika, jak by se mohlo na první pohled jevit, ale od pojmu „kybernetický prostor", který je označován jako: *„nervový systém" globální ekonomiky, který je tvořen stovkami a tisíci propojených počítačů,*

[7] SMEJKAL, Vladimír. *Internet a §§§*. 2. vydání. Praha: Grada Publishing, spol. s.r.o., 2001. s. 150
[8] NOVÁK, Karel. Počítačová kriminalita. Praha: Institut pro kriminologii a sociální prevenci, 1992.
[9] SMEJKAL, Vladimír. Počítačová a internetová kriminalita v České republice. Právní rozhledy, 1999, č. 12, příloha, s. 2
[10] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vydání. Praha: Grada Publishing, spol. s.r.o., 2007. s. 91

serverů, routerů, přepínačů, optických kabelů. Kybernetický prostor tak umožňuje této infrastruktuře její funkci, uvádí ji v život. Kyberprostor je sběrný, popisný termín pro všechno od Internetu a světové sítě až po imaginární a metaforický prostor, který v něm existuje. Kyberprostor je tam, kde jsou informace, je to skutečný a zároveň fiktivní prostor, prostor, kde probíhá e-mailová diskuse, prostor chat-roomů".[11]

Z hlediska teorie není vhodné pohlížet na pojem kybernetický prostor pouze jako na něco digitálního a informatického. Kybernetický prostor je nutné zkoumat a poznávat jej skrze připojení k osobnímu počítači.[12] Útoky v tomto prostoru učiněné se vyznačují vysokou mírou efektivity. Ve velmi krátkém čase lze z jednoho místa zasáhnout zájmy v mnoha jiných oblastech. Finanční náklady jsou přitom zanedbatelné nebo žádné, stejně tak možnost odhalení pachatele.[13] Kybernetický prostor se stále rozšiřuje, což mimo jiné dokládá překročení hranice jedné miliardy uživatelů v roce 2006 a dvou miliard v roce 2010.[14]

2.1.2 Informatické právo

Širším pojmem je tzv. informatické právo. To se skládá z řady specializací jako počítačové právo, telekomunikační právo, autorské právo, právo informačních systémů, právo ochrany osobních údajů atp.[15]

2.2 Internet

Pro počítačovou kriminalitu je typické, že může postihnout celou společnost. Zasahuje do různých oblastí života. Výpočetní technika je užívána jak ve veřejné správě, tak v armádě, ve zdravotnictví i dalších oblastech. Abychom blíže nahlédli do světa počítačové kriminality, musíme se také podívat na fenomén jménem Internet.

Jedná se o pojem, který není lehko uchopitelný. Nemá jednoho majitele a není ani subjektem práva. Sám o sobě nemůže nabývat práv a zavazovat se. Jedná se o informační

---

[11] POLČÁK, Radim. ŠKOP, Martin. MACEK, Jakub. *Normativní systémy v kyberprostoru (úvod do studia).*Brno, Masarykova univerzita, 2005. s. 10.
viz. také LESSING, L. The Zones of Cyberspace. *Standford Law review*, 1996, č. 48, s. 1403
[12] POLČÁK: *Normativní systémy v kyberprostoru...* s. 10.
[13] GŘIVNA, Tomáš. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. In HORYNA, Mojmír (ed). *Český právní řád a ochrana kyberprostoru: (vybrané problémy).* Praha: Karolinum, 2008, s. 21 – 34.
[14] POŠVIC, Kamil. *Počet uživatelů internetu v roce 2010 překročil 2 miliardy.* [online]. root.cz, 1.února 2011 [cit. 3. února 2011]. Dostupné na <http://www.root.cz/zpravicky/pocet-uzivatelu-internetu-v-roce-2010-prekrocil-2-miliardy/>
[15] SMEJKAL, Vladimír. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. *Trestněprávní revue*, 2003, č. 6, s. 2

systém skládající se z rozličných subjektů práva, ať již fyzických či právnických osob nebo majetku.[16] Nelze ho tedy pojmout jednoduše. V obecnější rovině si tento pojem můžeme představit jako médium. V rovině technické je Internet soustavou serverů, datových komunikací a počítačů, které jsou k nim připojeny.[17]

2.2.1 Komplexita Internetu

Rád bych upozornil na tzv. „komplexitu" Internetu. Jak uvádí Radim Polčák, Internet je složitý systém, na který je nutno nahlížet komplexně, tedy nikoliv pouze na jeho jednotlivé elementy. Představit si ho můžeme na příkladu mraveniště. Mravenec sám o sobě je schopen pracovat s omezeným počtem informací a jeho práce je značně neefektivní. Každý z nich má přiděleno určité kvantum úkolů, s nimiž pracuje, a podíváme-li se na každého jednotlivě, dojdeme k závěru, že to není nic výjimečného. Přestaneme-li však zkoumat jednotlivé elementy a přejdeme na hledisko komplexní, dojdeme k závěru, že dělba práce v samotném mraveništi, rozdělování zdrojů atp. je záležitostí téměř dokonalou, budící obdiv.[18] Z tohoto pohledu je také nutné nahlížet na pojem Internet jako na komplexní a složitý systém.

2.2.2 Legislativní regulace Internetu

Vhodné je položit si otázku, do jaké míry by takto složitý a potenciálně nebezpečný systém jako je Internet měl být regulován právně, tedy normami. Jedním z nejvýznamnějších hnutí zabývajících se již od roku 1990 bojem za svobodný Internet je hnutí „Electronic Frontier Foundation". Tato organizace odmítá vládní ingerence do oblasti Internetu a uvádí pro tento argument řadu důvodů, které jsou shrnuty v tzv. „Deklaraci nezávislosti kyberprostoru". V této deklaraci mimo jiné odmítají užití pojmu Internet v souvislosti s institutem vlastnictví. Argumentují skutečností, že Internet sám o sobě postrádá jakoukoliv hmotnou podstatu.

„Nemáme těla a na rozdíl od Vás se řád mezi námi nevytváří prostřednictvím násilí. Věříme v nastolení pořádku díky etice, osvícenému individualismu a smyslu pro všeobecné blaho. Můžeme se volně přemisťovat mezi Vašimi jurisdikcemi a tak jediné pravidlo, které skutečně ustavuje naše společenství, je zlaté pravidlo morálky. Na tomto základě chceme řešit

[16] SMEJKAL, Vladimír. Internet a §§§. 2. vydání. Praha: Grada Publishing, spol. s.r.o., 2001. s. 17
[17] SMEJKAL, Vladimír a kol. Právo informačních a telekomunikačních systémů. 2. vydání. Praha: C.H.Beck, 2004. s. 587
[18] POLČÁK, Radim. Právo a evropská informační společnost. 1. vydání. Brno: Masarykova univerzita, 2009. s. 29

všechny problémy a nepřijímáme způsoby, které se nám snažíte vnutit.“[19]

Hnutí upozorňuje na neexistenci společenské smlouvy, která by upravovala vztah mezi novým společenstvím, které Internet vytváří, a státem. Internet se má s problémy vypořádat prostřednictvím vlastních nástrojů a nikoliv zásahů zvnějšku. Trestní právo spočívá v individuálním postihu pachatele. Co se týče Internetu, jedná se vlastně o data, která přesahují jurisdikci států a která se mnohdy objevují na místech, kde žádná jurisdikce není, a tudíž není ani možný postih pachatele.[20] To je problematické a nahrává slovům EFF. Domnívám se, že prostředí Internetu si se samoregulací vztahů nevystačí. Ostatně podíváme-li se na případy pornografie, podvodů v elektronickém bankovnictví atp., dojdeme k závěru, že bez vnější autority by v prostředí Internetu panovala anarchie. Ač Internet jistě přesahuje jurisdikci nebo se objevuje v místech, kde žádná jurisdikce není, důsledky jednání s Internetem spojených se objevují v každodenním životě běžného člověka. Nelze přilnout k argumentu, že Internet nemůže mít žádného vlastníka (chybí hmotná podstata), vytváří vlastní společenství založené na etice, smyslu pro všeobecné blaho aj. Stále se jedná o lidský faktor, o člověka - uživatele, který Internetu dává tvář a určuje směr jeho vývoje. Otázkou pouze zůstává „do jaké míry“ a „jaké vztahy“ v oblasti počítačových sítí regulovat.

V některých případech se setkáváme s odmítnutím legislativní regulace prostředí Internetu a to nejen u hnutí EFF, ale také u orgánů činných v trestním řízení. Jeden z takovýchto případů se odehrál v České republice. Policie ČR odložila případ týkající se trestného činu pomluvy z toho důvodu, že k příslušnému protiprávnímu jednání došlo na internetovém fóru. K tomuto se později ve svém rozhodnutí vyjádřil Nejvyšší soud ČR, který v rozsudku poskytl jakýsi návod pro vyšetřovatele a popsal chyby, kterých se orgán činný v trestním řízení dopustil. V tomto případě došlo k pochybení z důvodu nepřibrání znalce z oboru výpočetní techniky, který by posoudil, zda-li je možné danou osobu identifikovat a vyhledat.[21]

To, že Internet a vztahy, které díky němu vznikají, hraje velkou roli i v každodenním životě člověka ilustruje případ, který se odehrál v Číně. Počítačový uživatel („hráč“) online počítačové hry usmrtil jiného, který bez jeho souhlasu prodal virtuální zbraň v internetové

---

[19] POLČÁK, Radim. Právo a evropská informační společnost. 1. vydání. Brno: Masarykova univerzita, 2009. s. 37
plné znění viz. https://projects.eff.org/~barlow/Declaration-Final.html
[20] POLČÁK: *Právo a evropská...*, s. 38.
[21] Rozsudek Nejvyššího soudu ze dne 16.1. 2001, sp. zn. 4 Tz 265/2000

aukci. Tomuto činu předcházelo odmítnutí čínské policie zabývat se tímto případem, jelikož virtuálním prodejem věcí se žádná právní norma nezabývá. [22]

[22] VYLEŤAL, Martin. *Online hry hýbou Internetem, psychikou a peněženkami hráčů*. [online]. lupa.cz, 12.srpna 2005 [cit. 20. listopadu 2010]. Dostupné na <http://www.lupa.cz/clanky/online-hry-hybou-internetem-psychikou-a-penezenkami-hracu/>

3 Historie počítačové kriminality

Již roku 1968 došlo k propojení prvních čtyř univerzitních počítačů. V té době ještě nikdo nepředpokládal tak bouřlivý vývoj informačních technologií v následujících desetiletích. *„Interaktivita, u knižních virtuálních postav dosud nedostupná, se stala podstatou počítačové komunikace, totální ztráta mimoverbálního vnímání, možnost vytváření nesmrtelných virtuálních jedinců, snadnost přechodu mezi komunitami a potlačená potřeba kompromisů vedly k vytvoření nového „kybernetického" světa, který se pro mnohé stal snesitelnější a příjemnější nežli svět reálný."* Takto popisuje „příchod" Internetu a nových informačních technologií Václav Jirovský, vedoucí Ústavu bezpečnostních technologií a inženýrství ČVUT.[23]

3.1 Členění počítačové kriminality z historického hlediska[24]

3.1.1 **Období pravěku** (do roku 1981, kdy byl na trh uveden první PC)

V této době hovoříme o prvním „počítačovém" zločinu. Poprvé se také objevuje dnes již známý termín „hacks"[25]. V počátcích měl však tento pojem význam spíše pozitivní. Aby si programátoři upravili software k obrazu svému, museli využít svých vlastních schopností a možností.[26]

3.1.2 **Období středověku** (do roku 1994)

Jedná se o období, kdy došlo k syntéze počítače a telefonní linky, řešila se otázka ochrany svobody projevu a občanských práv na síti a v této souvislosti vznikla také Nadace elektronického pohraničí – EFF. V této době si orgány činné v trestním řízení uvědomovaly vážnost a nebezpečí potenciálně možných jednání, která jsou s informačními technologiemi spojena, vyvrcholením této éry byl pak případ Sundevil. Pachateli se v tomto případě podařilo přesměrovat příchozí hovory floridského kurátora do vzdáleného města New York.[27]

3.1.3 **Období novověku** (od roku 1994 do současnosti)

Ve dvacátých letech dochází k masovému rozšíření technologie PC, operačního systému Microsoft Windows a sítě Internet. Tím se také rozšiřují možnosti potenciálních

[23] JIROVSKÝ: *Kybernetická kriminalita*, s. 16.
[24] MATĚJKA: *Počítačová kriminalita*, s. 17.
[25] doslova „záseky"
[26] MATĚJKA: *Počítačová kriminalita*, s. 18-20.
[27] Tamtéž, s. 23-25.

pachatelů a jejich zaměření, např. na šíření počítačových virů nebo tzv. DoS útoky.[28] S přibývajícím počtem komerčních softwarových produktů se také rozšiřuje fenomén známý pod termínem softwarové pirátství, v souvislosti s tím se začíná používat pojem warez. Softwarovému pirátství se tak dostalo jeho organizované a vysoce sofistikované podoby.[29]

3.2 První počítačový delikt v zahraničí

V zahraničí se první zločin z oblasti počítačové kriminality odehrál již v roce 1801 ve Francii. Tkadlec Jacquard sestrojil tkalcovský stav, který dokázal automatizovat určité druhy úkonů, tímto „ohrozil" stávající zaměstnance, kteří pod vidinou ztráty pracovních míst donutili Jacquarda upustit od dalšího vývoje stroje.[30]

Ve velké míře docházelo také k falšování údajů v papírových dokladech, prováděly se různorodé výpočty na počítači zaměstnavatele (jednalo se tedy o neoprávněné užívání cizí věci) a to za účelem vidiny snadného zisku. Pro počátky období počítačové kriminality je typická vysoká míra tzv. latence, tedy skrytosti počítačových deliktů. Ta se do značné míry promítá také do dnešní doby. Možnosti, jak odhalit pachatele trestného činu, byly minimální. Latenci počítačových deliktů nepřispěla mimo jiné skutečnost, že případy této kriminality byly řazeny do oblasti deliktů hospodářských.

3.3 Historie počítačové kriminality v České republice

Podíváme-li se do historie počítačové kriminality, zjistíme, že možnosti pachatele byly ponejvíce limitovány soudobým stavem techniky. První případ, který lze v České republice označit za počítačovou kriminalitu, se odehrál v sedmdesátých letech. Jednalo se o pracovníka úřadu důchodového zabezpečení, který za pomoci magnetu poškodil záznamy na magnetických páskách a který tímto jednáním naplnil skutkovou podstatu trestného činu sabotáže (později bylo dané jednání dvakrát překvalifikováno). Tímto činem způsobil pozastavení výplat důchodů v celé ČSSR.[31]

Během let 1990 až 1995 došlo v České republice k 150% nárůstu hospodářské trestné činnosti. Jednalo se hlavně o krádeže, podvody aj., tedy o typickou majetkovou kriminalitu.

Vladimír Smejkal datuje novou dobu počítačového zločinu dvěma fakty. Prvním z nich je nástup osobních počítačů, druhým vznik počítačových sítí a možnosti vzdáleného

[28] útok směřující k odstavení služby resp. odepření přístupu.
[29] MATĚJKA: *Počítačová kriminalita*, s. 32-41.
[30] Tamtéž, s. 18
[31] SMEJKAL: *Internet a §§§*, s. 154.

přístupu k počítačům. Tímto se počítač dostal k většímu množství uživatelů a rozšířily se také možnosti potenciálních pachatelů trestné činnosti.[32]

Z historického hlediska je důležitým bodem přelom roku 1991 a 92, kdy byly do tehdy platného a účinného trestního zákona zařazeny dvě nové skutkové podstaty související s počítačovou kriminalitou[33] (dále jen „starý trestní zákon"). Jednalo se o ustanovení § 257a, tedy trestný čin poškození a zneužití záznamu na nosiči informací, a dále ustanovení § 178, neoprávněné nakládání s osobními údaji. Vzhledem k dynamickému vývoji oblasti počítačové kriminality byl tento stav dlouhou dobu nedostačující a bylo zapotřebí přizpůsobit a aktualizovat příslušnou platnou právní úpravu.

[32] SMEJKAL: *Internet a §§§,* s. 157.
[33] Zákon č. 140/1961 Sb., trestní zákon, ve znění zákona č. 52/2009 Sb. účinného ke dni 1. 4. 2009

4 Počítačová kriminalita a její organizace v zahraničí

Otázka kybernetických hrozeb není předmětem diskuze jen na území České republiky. Inspiraci a zkušenosti bylo nejdříve nutno čerpat ze zahraničních zdrojů. Jednalo se především o země, kde mají s kybernetickými útoky zkušeností nejvíce, např. Korejskou republiku, Japonsko, USA a další země. Touto problematikou se zabývali především pracovníci odboru bezpečnostní politiky Ministerstva vnitra ČR Oldřich Krulík a Václav Hník.

4.1 Situace v USA

Jedním z důležitých faktů je finanční náročnost boje proti kybernetickým hrozbám v USA. Informační bezpečnosti je věnováno více než 14 % z rozpočtu Ministerstva obrany. Již v 90. letech došlo na půdě Carnegie Mellon University[34] k vytvoření určité struktury. Zjednodušeně řečeno týmu, který reagoval na možné počítačové ohrožení.[35] Od roku 1997 se problematice bezpečnostních hrozeb v této oblasti věnují vládní kruhy a vznikla celá řada organizací. V roce 2000 vznikl např. „Národní plán pro ochranu informačních systémů".[36] Po událostech z 11. 9. 2001 došlo k navýšení zájmu ohledně problematiky kybernetických hrozeb, útoků a možném spojení s terorismem. Vznikl tzv. „zákon o informační bezpečnosti".[37] Tomu také odpovídalo vyčlenění dalších finančních prostředků na tyto aktivity.

Problematice je tedy věnována značná pozornost, zabývají se jí tisíce specialistů a to zejména z již zmíněné Carnegie Mellon University. Tito odborníci spolupracují hlavně se zástupci a absolventy dané univerzity, přičemž ke spolupráci dochází také v rámci těch nejdůležitějších subjektů na poli počítačové kriminality, kterými jsou Ministerstvo vnitřní bezpečnosti a Ministerstvo obrany. Tyto subjekty si uvědomují, že k účinné obraně proti kybernetickým útokům je nutné spolupracovat nejen na úrovni národní, ale taktéž mezinárodní. Z důvodu účinnějšího boje proti počítačové kriminalitě by se příslušné orgány a úřady měly o své poznatky dělit dokonce se svými konkurenty. V celém systému spolupráce se projevuje jedno ze základních specifik počítačové kriminality jako takové a to je její „bezhraničnost". Počítačový útok může přijít odkudkoliv bez ohledu na hranice daného

[34] viz. http://www.cmu.edu/index.shtml
[35] Computer Emergency Response Team Coordination Center, CERT/CC.
[36] National Plan for Information Systems Protection
[37] Federal Information Security Management Act, FISMA

státu.[38]

V různých státech světa fungují ekvivalentní organizace a uskupení typu CSIRT.CZ[39] v České republice. U nás zahájila tato organizace činnost až v roce 2008. Z tohoto důvodu je vhodné inspirovat se novými zkušenostmi a poznatky ze zahraničí. V prvé řadě se jedná Spojené státy americké.

Jedním z důležitých poznatků je skutečnost, že na poli bezpečnostních hrozeb působí ve většině států akademická pracoviště. Tento sektor byl zapojen do procesu boje proti kybernetickým hrozbám ve většině zemí již od počátku. Určitým sjednocujícím bodem je fakt, že k navýšení financí a větší aktivitě v oblasti kybernetické kriminality napomohla mnohdy konkrétní událost, např. situace po 11. 9. 2001 v USA.

4.2 Situace v Polsku

V mnoha státech je tématu počítačové kriminality věnována stále velmi nízká pozornost. Podíváme-li se na sousední země, zjistíme, že v Polsku vznikla pracovní skupina zabývající se kybernetickou kriminalitou již v roce 2002. Jedním z cílů tohoto uskupení bylo například určit rozsah kritické infrastruktury a analyzovat situaci na poli této problematiky. Aktivní jsou zejména správci Vzdělávací a akademické počítačové sítě.[40] Během posledních let došlo k většímu rozvoji dvou projektů a to „Dohledového systému Arakis“ a technického a koordinačního centra v rámci kontrarozvědky.[41]

4.3 Situace v Německu

Ve Spolkové republice Německo dohlíží na bezpečnostní aktivity Spolkový úřad pro bezpečnost v informační technice.[42] Určité aktivity a odborné diskuze probíhají v Německu

[38] KRULÍK, Oldřich. HNÍK, Václav. *Zahraniční inspirace související s tématem kybernetických hrozeb*. [online]. mvcr.cz, srpen 2006 [cit. 16. prosince 2010]. Dostupné na <http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/zahranicni_inspirace.pdf>

[39] Modelový bezpečnostní tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích ČR. viz. https://www.csirt.cz/

[40] Naukowa i Akademiczna Siet Komputerowa, NASK

[41] KRULÍK: *Zahraniční inspirace…* Dostupné na <http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/zahranicni_inspirace.pdf>

[42] viz. http://www.bsi.de/ - Bundesamt für Sicherheit in der Informationstechnik,BSI

již od roku 1986. V té době fungovala na jeho území „Ústřední agentura pro šifrování“.[43] Roku 2005 činil rozpočet Spolkového úřadu již přes 52 milionů Eur.[44]

4.4 Situace na Slovensku

Na Slovensku zatím neexistuje organizace, která by se věnovala výhradně počítačovým hrozbám. I přesto, že v roce 2006 nastal vážný bezpečnostní incident u Národného bezpecnostného úradu Slovenska. Servery úřadu byly zablokovány opakovanými žádostmi o připojení a došlo také ke zkopírování desetitisíců emailových komunikací. Jedná se o mediálně známý incident.[45]

4.5 Situace v Rakousku

Každé Ministerstvo Rakouské republiky spolupracuje s několika bezpečnostními techniky z oblasti informačních technologií. Konkrétní případy incidentů ze světa počítačového pirátství jsou řešeny přímo odděleními kriminální policie.[46]

[43] Zentralstelle für das Chiffrierwesen, ZfCh.
[44] KRULÍK: *Zahraniční inspirace…* Dostupné na <http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/zahranicni_inspirace.pdf>
[45] Tamtéž
[46] Tamtéž

5 Trestněprávní úprava počítačové kriminality

5.1 Dělení trestných činů souvisejících s počítačovou kriminalitou

Trestné činy lze dělit dle různých kritérií[47]:

1. Trestné činy ve vztahu k počítači, jeho příslušenství a jiným předmětům jako věcem movitým. Hovoříme o majetkové kriminalitě v klasickém významu.
2. Trestné činy ve vztahu k softwaru, k datům. Zde je počítač předmětem trestného činu nebo cílem útoku. Jedná se o informační kriminalitu.
3. Trestné činy, kde počítač slouží jako prostředek. Do této kategorie řadíme hospodářskou kriminalitu.

Michal Matějka rozděluje protiprávní jednání proti počítači a protiprávní jednání, kde počítač vystupuje jako nástroj, tedy s využitím počítače. Dále člení protiprávní jednání na:[48]

1. Tradiční – do této skupiny bychom zařadili nejen klasickou trestnou činnost, tedy trestné činy loupeže, krádeže, zpronevěry, ale také průmyslovou špionáž, podvody, padělání, pomluvy, vydírání atp.
2. Nová – např. jednání jako je hacking, carding, zneužití osobních údajů, spamming, warez, phreaking, cracking, sniffing nebo tzv. doménové pirátství v podobě cybersquattingu.

5.2 Úprava počítačové kriminality v zákoně č. 140/1961 Sb.

Co se týče stávající právní úpravy, existuje zde několik specifik, která ji odlišují od té dřívější, tedy od zákona č. 140/1961 Sb., trestní zákon, ve znění zákona č. 52/2009 Sb. účinného ke dni 1. 4. 2009. Před nabytím účinnosti aktuálního znění trestního zákona[49] existovala pouze jediná explicitní norma týkající se počítačové kriminality. Jednalo se o ustanovení § 257a starého trestního zákona definující trestný čin poškození a zneužití záznamu na nosiči informací. Trestné bylo jednání spočívající v získání přístupu k nosiči informací s úmyslem způsobit jinému škodu nebo jinou újmu, nebo získat sobě nebo jinému neoprávněný prospěch. Dále neoprávněné užití takovýchto informací, zničení, poškození nebo

[47] SMEJKAL, Vladimír. *Internet a §§§*. 2. vydání. Praha: Grada Publishing, spol. s.r.o., 2001. s. 153
[48] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha: Computer Press, 2002. s. 49
[49] aktuální znění: zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

jednání spočívající v zásahu do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení.

Z výše uvedeného vyplývá, že čin bylo možné spáchat pouze úmyslně. Obecně bylo tímto ustanovením chráněno softwarové i hardwarové vybavení počítače. Nejasnosti byly ohledně výkladu termínu „nosič informací". V konečném důsledku bychom si pod tímto pojmem mohli představit i „chytrou" mikrovlnnou troubu. Přidáme-li k názvu trestného činu slovo „elektronických informací", je znění tohoto ustanovení o poznání jasnější. Komentář k aktuálnímu znění trestního zákona se snaží absenci vhodné definice nosiče informací napravit:

„Nosičem informací se rozumí jakýkoli nosič dat v informační technice, tedy materiál, do kterého nebo na který lze zaznamenávat („zapsat") data a z kterého lze data zpět získat („přečíst") – např. pevný disk (tzv. „HDD" nebo „hard disk"), operační paměť (tzv. RAM), disketa, CD-R, CD-RW, DVD-R, DVD+R, DVD-RW, DVD+RW, Blu-Ray, USB key, mobilní telefon."[50]

5.2.1 Příklady možných protiprávních jednání dle ustanovení § 257a zákona č. 140/1961

Důležité je upozornit na skutečnost, že nebyla popsána nedbalostní varianta tohoto trestného činu. Úmysl musela doprovázet pohnutka nebo snaha způsobit újmu. Tomáš Sokol a Vladimír Smejkal popisují některá konkrétní jednání, za které byl v minulosti pachatel již odsouzen. Jednalo se kupříkladu o počítačového uživatele, který umístil na nemovitosti zařízení technického charakteru, prostřednictvím kterého užíval neoprávněně IP adresu jednoho z klientů obchodní společnosti za účelem připojení k síti Internet. Dále se jednalo o případ zaměstnance, který bez vědomí zaměstnavatele užíval jeho počítač a také nainstalovaný software k tomu, aby vytvářel nabídkové rozpočty pro své vlastní zákazníky. Dále způsobil nefunkčnost celého softwaru tím, že vymazal údaje o stavebních akciích zaměstnavatele. Jednání naplňující tuto skutkovou podstatu byla tedy různorodá. Pod ustanovení § 257a starého TrZ by také spadala tzv. „průmyslová špionáž". V tomto případě mohlo dojít např. k průniku do systému konkurenčního podnikatele a zneužití jeho dat. [51]

[50] ŠÁMAL, Pavel a kol. *Trestní zákoník. Edice velké komentáře*. 1. vydání. Praha: C.H.Beck, 2009. s. 2089
[51] MATĚJKA: *Počítačová kriminalita*, s. 52

5.2.2 Statistika Ministerstva spravedlnosti ČR k ustanovení § 257a

Z oficiálních statistik, konkrétně ze statistické ročenky kriminality za rok 2009, kterou každoročně vydává Ministerstvo spravedlnosti ČR (odbor dohledu Ministerstva spravedlnosti ČR) plyne, že z trestného činu dle ustanovení § 257a bylo stíháno celkem 21 osob, z toho 16 osob bylo obžalováno a odsouzeny byly jen 4. Soud udělil 3 podmíněné tresty a jeden trest obecně prospěšných prací.[52]

Zásadní roli však v tomto ohledu hraje vysoká míra latence počítačové kriminality, kdy mnoho trestných činů zůstává stále neodhaleno, ať již z důvodu dokonalejší technické vybavenosti pachatelů, nebo jejich vyšší kvalifikace.

5.3 Úprava počítačové kriminality v zákoně č. 40/2009 Sb.

Současná právní úprava uvádí dvě nové skutkové podstaty namísto staršího ustanovení § 257a. Jedná se o § 230 a § 231 TrZ.

Toto ustanovení vychází z ideového základu Úmluvy o počítačové kriminalitě,[53] což zmiňuje např. důvodová zpráva k trestnímu zákonu.[54] U nového ustanovení postačí získat pouze neoprávněně přístup k počítačovému systému (překonáním určitého bezpečnostního opatření, např. hesla). Není tedy nutné, aby pachatel s počítačovým systémem manipuloval, postačí pouze překonání firewallu nebo vloupání se do kanceláře, kde je počítač uložen.

5.3.1 Trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací dle ustanovení § 230

5.3.1.1 Překonání bezpečnostního opatření

(Odst. 1) *„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.“*[55]

Odst. 1 postihuje typicky jednání hackera, který zkouší hesla do té doby než „natrefí“

---

[52] Odbor dohledu ministerstva spravedlnosti ČR. *Statistická ročenka kriminality: rok 2009*. [online]. portal.justice.cz, 2009 [cit. 22. prosince 2010]. Dostupné na <http://portal.justice.cz/Justice2/soubor.aspx?id=85103>

[53] plné znění úmluvy v anglickém znění viz. Council of Europe. Convention on Cybercrime. [online]. http://conventions.coe.int, 23. září 2001 [cit. 20. ledna 2011]. Dostupné na < http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm >

[54] Důvodová zpráva k zákonu č. 40/2009 Sb., trestní zákoník.

[55] aktuální znění: zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

na to správné. Setkáme se zde s často užívaným termínem „hacking“. Zpravidla půjde o jednání, která jsou přípravného charakteru a mohou mít vztah k jinému trestnému činu, především majetkové povahy, např. trestný čin krádeže dle ustanovení § 205 TrZ, ale také porušení autorského práva v souvislosti s ustanovením § 270 TrZ.[56] Primárně je tímto ustanovením chráněn počítačový systém před ohrožením jeho bezpečnosti. K odst. 1 není zapotřebí úmysl způsobit jinému škodu nebo jinou újmu, popřípadě získat sobě nebo jinému neoprávněný prospěch. Takové okolnosti jsou vyžadovány až v odst. 3 a 4 jako zvláště přitěžující.[57]

5.3.1.2 Získání přístupu k počítačovému systému

(Odst.2) *„Kdo získá přístup k počítačovému systému nebo k nosiči informací a*

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,
b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, bude potrestán....“[58]

Odst. 2 se týká osoby, která již přístup k počítačovému systému má, přičemž nezáleží na tom, zda tento přístup získala legálně či nelegálně, a dále jedná s daty v tomto systému způsobem v ustanovení popsaném. Pachatel může mít legální přístup k počítačovému systému např. na základě uzavřené pracovní smlouvy nebo z důvodu výkonu určité funkce. Jeho úmysl manipulovat s daty nemusí přijít ihned při získávání přístupu k tomuto systému nebo nosiči informací. Ten pojme pachatel povětšinou ve fázích pozdějších. Tento proces ulehčuje dokazování subjektivní stránky tohoto trestného činu.[59] Jednání popsané v odst. 2 pís. b) poskytuje ochranu před tzv. „počítačovou sabotáží“. Obecně zde primární ochrana připadá na integritu a dostupnost počítačových dat a systémů.

---

[56] KUCHTA, Josef. Úprava majetkových trestných činů v novém trestním zákoníku. *Právní rozhledy*, 2010, č. 1, s. 11
[57] ŠÁMAL: *Trestní zákoník*…, s. 2086
[58] aktuální znění: zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
[59] KUCHTA: *Úprava majetkových trestných činů…*, s. 11

Odst. 3 postihuje motiv pachatele tohoto trestného činu a odst. 4 je kvalifikovanou skutkovou podstatou ve vztahu k odst. 1 a 2. Přísněji bude potrestán např. ten, kdo způsobí vážnou poruchu v činnosti orgánů státní zprávy, územní samosprávy, soudu nebo jiného orgánu veřejné moci a v činnosti právnické nebo fyzické osoby, která je podnikatelem.[60] Zvýšenou pozornost je nutné požadovat při možné záměně tohoto ustanovení s trestným činem neoprávněné užívání cizí věci dle ustanovení § 207 TrZ. Pokud nedojde k naplnění některého z jednání uvedených v ustanovení § 230 TrZ a pachatel pouze užívá nosič nebo počítač, k němuž získal legálním způsobem přístup, pak se jedná o tzv. „krádež počítačového času", tedy neoprávněné užívání cizí věci.[61]

Důležité je stanovení určité hranice, která posoudí, zda-li je neoprávněný přístup jednáním nebezpečným pro společnost či nikoliv. Svou roli bude v tomto procesu hrát zabezpečení operačního systému potenciální oběti. Tedy zda-li používá aktuální a dostatečně bezpečný firewall, antivirový program a další softwarové produkty pro bezpečnou práci s PC.

5.3.1.3 Neoprávněný průnik

Nebezpečnějším bude pachatel, který softwarovou obranu uživatele dokáže překonat, než-li ten, kdo se pokusí např. uhodnout jednoduché heslo za účelem získání přístupu do systému (jméno oběti, název oblíbeného filmu atp.) a uspěje pouze v důsledku „počítačové negramotnosti" uživatele PC. Otázkou také je, zda-li by neměl být trestný pouze takový průnik, který umožní spáchání jiného trestného činu nebo je jeho součástí. Tento průnik je často zmiňován v souvislosti s narušením soukromí uživatele a přirovnáván k situaci, kdy pachatel neoprávněně vnikne do obydlí jiného. Tímto také naruší jeho soukromí a má možnost dostat se k osobním věcem.[62] Typickým neoprávněným průnikem je získání přístupového hesla prostřednictvím příslušného softwaru nebo náhodným uhodnutím.

5.3.2 Trestný čin opatření a přechovávání přístupového zařízení a hesla dle ustanovení § 231 TrZ.

Výše uvedený trestný čin chrání společnost před jednáním spočívajícím v opatření a přechovávání zařízení, nástrojů a prostředků, které by mohly sloužit ke spáchání trestných činů porušování tajemství dopravovaných zpráv dle ustanovení § 182 TrZ nebo

[60] SOKOL, Tomáš. SMEJKAL, Vladimír. *Postih počítačové kriminality podle nového trestního zákona*. [online]. pravniradce.ihned.cz, 22. července 2009 [cit. 25. prosince 2010]. Dostupné na <http://pravniradce.ihned.cz/c4-10077480-37865090-F00000_d-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>
[61] KUCHTA: *Úprava majetkových trestných činů…*, s. 11
[62] ŠÁMAL: *Trestní zákoník…*, s. 2086

neoprávněného přístupu k počítačovému systému a nosiči informací dle ustanovení § 230 TrZ.

(Odst. 1) *„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 nebo jakýkoli jiný*
a) prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo
b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup do počítačového systému nebo jeho části, bude potrestán...“[63]

5.3.2.1 Předčasné dokonání

Ve své podstatě se jedná o předčasně dokonaný trestný čin neboli speciální přípravu k dvěma výše uvedeným trestným činům. Samotná příprava daného jednání by nebyla trestná, nejedná se totiž o zvlášť závažný zločin dle ustanovení § 20 odst. 1 a § 14 odst. 3 TrZ, proto hovoříme o činu předčasně dokonaném. Důvodem je mimo jiné také obtížná možnost odhalení daného jednání. Jedná se o trestný čin úmyslný. K dokonání je potřeba nejen opatření a přechovávání přístupových zařízení, ale také úmysl spáchat výše uvedené trestné činy.[64] Tímto je vyloučeno stíhání soudního znalce popřípadě počítačového experta, který s danými údaji může pracovat. Pod pojmem „přístupové zařízení“ si můžeme představit např. čtečku bankovních karet.[65]

5.3.3 Trestný čin poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

Z důvodů vysoké nebezpečnosti jednání existuje také nedbalostní varianta daného trestného činu. Jedná se o ustanovení § 232 TrZ, tedy o trestný čin poškození záznamu v počítačovém systému a na nosiči informací a o zásah do vybavení počítače z nedbalosti.

K dokonání tohoto trestného činu se vyžaduje porušení povinnosti plynoucí ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté (typicky se bude jednat o zaměstnance, jenž mají určitou povinnost nakládat řádně

[63] aktuální znění: zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
[64] ŠÁMAL: *Trestní zákoník*…, s. 2097-8
[65] Tamtéž, s. 2100

s hardwarem a softwarem, se kterým pracují). Příkladem jednání, která bychom dle tohoto ustanovení mohli kvalifikovat jsou např. zavirování počítače a zničení dat na tomto zařízení, připojování se na nebezpečné internetové adresy, nedodržení bezpečnostních opatření tak, aby byl počítač dostatečně zabezpečen atp.[66]

Z hlediska subjektivní stránky postačí nedbalost a to v obou svých formách, tedy vědomá i nevědomá. Musí se však jednat o nedbalost hrubou, kterou definuje ustanovení § 16 odst. 2 TrZ.

Odst. 2: *„Trestný čin je spáchán z hrubé nedbalosti, jestliže přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem.“*[67]

Dalším důležitým znakem tohoto trestného činu je způsobení značné škody na cizím majetku, tedy alespoň 500 000 Kč. Není-li tato podmínka splněna, lze uvažovat o postihu dle jiných ustanovení trestního zákona (např. ohrožení utajované informace z nedbalosti dle ustanovení § 318 TrZ nebo maření úkolů úřední osoby z nedbalosti dle ustanovení § 330 TrZ)

Naplněním skutkové podstaty tohoto trestného činu může být ohrožen provoz významného a důležitého provozu jako je např. letiště popřípadě fungování důležitého orgánu státní správy. Z těchto důvodů je nutné zesílit veřejnoprávní ochranu informačních systémů, k čemuž má přispět aktuální právní úprava v trestním zákoně. Předchozí právní úprava postihu počítačové kriminality obsažena v ustanovení § 257a starého TrZ. byla již v rámci boje proti aktuálním hrozbám nedostačující.

5.4 Společný předmět ochrany

Společným znakem těchto 3 trestných činů je jejich objekt. Tím je zájem na ochraně dat uložených na nosiči informací proti jejich neoprávněnému použití, neoprávněným změnám, poškození, zničení, učinění neupotřebitelnými a ochrana počítače nebo jiného telekomunikačního zařízení nebo jiného nosiče informací před neoprávněnými zásahy. Nejsou to však jediné zájmy, které jsou chráněny. Nepřímo se jedná také o ochranu obchodního či bankovního tajemství, autorských děl, údajů o pacientech, údajů o zaknihovaných cenných papírech, utajované informace (pokud jsou obsaženy v nosiči). Předmětem útoku je právě nosič informací, jeho obsahové a technické vybavení.[68]

---

[66] KUCHTA: *Úprava majetkových trestných činů…*, s. 12
[67] aktuální znění: zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
[68] JELÍNEK: *Trestní právo…*, s. 620

6 Úmluva o počítačové kriminalitě a závazky plynoucí z evropského a mezinárodního práva obecně.

Stávající právní úprava nevychází pouze z „domácí“ legislativy, ale orientuje se také na úpravu přeshraniční. Do trestního zákona byla zapracována Úmluva o počítačové kriminalitě,[69] která byla schválena 8. 11. 2001 Výborem ministrů Rady Evropy a v platnost vstoupila 1. 7. 2004.[70] Tento dokument obsahuje závazky jak procesněprávního, tak hmotněprávního charakteru. Popsaná jednání jsou rozdělena do 4 základních kapitol. Jedná se o činy proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů, zločiny se vztahem k počítači, zločiny se vztahem k obsahu počítače (ty mají postihovat především dětskou pornografii) a zločiny se vztahem k autorským nebo obdobným právním úpravám.[71]

6.1 Trestné činy obsažené v Úmluvě o počítačové kriminalitě

1. Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
   - Neoprávněný přístup (čl. 2)
   - Neoprávněné zachycení informací (čl. 3)
   - Zásah do dat (čl. 4)
   - Zásah do systému (čl. 5)
   - Zneužití zařízení (čl. 6)
2. Trestné činy související s počítači
   - Falšování údajů souvisejících s počítači (čl. 7)
   - Podvod související s počítači (čl. 8)
3. Trestné činy související s obsahem
   - Trestné činy související s dětskou pornografií (čl. 9)
4. Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu (čl. 10)[72]

---

[69] plný text úmluvy v anglickém znění viz. Council of Europe. Convention on Cybercrime. [online]. http://conventions.coe.int, 23. září 2001 [cit. 20. ledna 2011]. Dostupné na <http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>

[70] SOKOL, Tomáš. SMEJKAL, Vladimír. Postih počítačové kriminality podle nového trestního zákona. [online]. pravniradce.ihned.cz, 22. července 2009 [cit. 25. prosince 2010]. Dostupné na <http://pravniradce.ihned.cz/c4-10077480-37865090-F00000_d-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>

[71] JELÍNEK: *Trestní právo…*, s. 86

[72] ŠÁMAL: *Trestní zákoník…*, s. 2089

Jedná se o demonstrativní výčet, tedy nikoli ohraničenou definici všech potenciálně možných protiprávních jednání. To je mimo jiné dáno skutečností, jak rychle a bouřlivě se rozvíjí tato oblast kriminality. Právní úprava ve stávajícím trestním zákoně tomuto odpovídá. Podíváme-li se podrobněji na trestné činy související s důvěryhodností, integritou a dostupností počítačových dat a systémů a to z pohledu platné právní úpravy, jedná se zejména o:

1. Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TrZ)
2. Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TrZ)
3. Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TrZ)
4. Porušení tajemství dopravovaných zpráv (§ 182 TrZ)[73]

Úmluva sama o sobě stále přímo nedefinuje termín počítačová kriminalita, ale obsahuje určitá vodítka a znaky určitých jednání, která by měla být postihována ve všech členských státech. Je nutné dodat, že každý stát může uplatnit výhradu, a tak nestíhat určité typy jednání. Ve své podstatě tento dokument obsahuje 2 základní závazky. Jedním z nich je závazek zavést do národní trestní legislativy příslušné skutkové podstaty trestných činů, druhý závazek obsahuje uzákonění odpovídajících procesních pravomocí orgánů činných v trestním řízení.

Úmluva vede také k usnadnění vyšetřování trestných činů a shromažďování důkazů. Měla by napomoci spolupráci, která usnadní vydávání pachatelů kybernetických zločinů. Pro účinnější charakter úmluvy je nutné, aby byla ratifikována všemi členskými státy. Zatím se tak nestalo ve všech případech. Ovšem významným faktorem je, že došlo k ratifikaci úmluvy ze strany „počítačových velmocí" Spojených států amerických a Japonska.[74]

V rámci přípravy úmluvy se diskutovalo mimo jiné o problematice uložení povinnosti poskytovatelům služeb shromažďovat a uchovávat elektronická data. Příslušné ustanovení nebylo nakonec do úmluvy zakomponováno, ale i přesto se dokument zmiňuje o elektronických datech a jejich rozdělení dle jejich obsahu na data provozní, data obsahová a data o odběratelích. Toto rozlišení je významné z hlediska určení míry zásahu do soukromí

[73] ŠÁMAL: *Trestní zákoník...*, s. 2084
[74] POLČÁK, Radim. Právo na internetu: Spam a odpovědnost ISP. 1. vydání. Brno: Computer Press, 2007. s. 14-16

osob.[75]

Úmluva o počítačové kriminalitě je významným krokem k harmonizaci skutkových podstat jednotlivých trestných činů, stejně tak procesních postupů.[76]

6.2 Vybrané závazky plynoucí z evropského a mezinárodního práva

Mezinárodní právní nástroje jsou vždy výsledkem konsenzu několika států s rozdílnými národními právními úpravami, a proto se jedná spíše o minimum, na kterém se shodla většina států.

Určitou míru iniciativy v oblasti počítačové kriminality vyvíjí např. Organizace spojených národů (OSN).[77] Jedná se např. o Rezoluci Hospodářské a sociální Rady OSN, přijatou dne 26. 7. 2007, která se týká mezinárodní spolupráce při vyšetřování, stíhání a trestání hospodářských podvodů a trestných činů souvisejících s identitou osob a která se dále zabývá také obecnými možnostmi prevence.

Dalším iniciátorem aktivit v boji nejen proti počítačové kriminalitě je Organizace pro hospodářskou spolupráci a rozvoj (OECD).[78] Její snahou je v současné době bojovat proti fenoménu jménem spam, krádeži identity nebo šíření malwaru.[79]

6.2.1 Regulace na půdě Evropské unie

V rámci EU se jedná především o úpravu v podobě směrnic a rámcových dokumentů. Z těch nejdůležitějších lze zmínit:

1. Rámcové rozhodnutí Rady 2005/222/SV ze dne 24. 2. 2005 o útocích proti informačním systémům.

Dokument vychází z faktu, že útoky proti informačním systémům jsou mnohdy přeshraničního rázu. Regulace se v tomto ohledu zdá být nezbytnou. Trestně stíhána by měla být jednání spočívající v protiprávním přístupu k informačním systémům, protiprávním zásahům do systému a protiprávním zásahům do dat. Postižena by měla být zejména jednání menšího rozsahu.

---

[75] GŘIVNA, Tomáš. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. In HORYNA, Mojmír (ed). *Český právní řád a ochrana kyberprostoru: (vybrané problémy)*. Praha: Karolinum, 2008, s. 25
[76] Tamtéž, s. 26
[77] Tamtéž, s. 23
[78] viz. http://www.oecd.org/home/0,3675,en_2649_201185_1_1_1_1_1,00.html
[79] GŘIVNA: Závazky k ochraně..., s. 27

2) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. 7. 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

Tato směrnice upravuje především pravidla zpracování provozních a lokalizačních údajů. Ve chvíli, kdy již nejsou tyto údaje potřebné pro přenos sdělení, musí být vymazány nebo anonymizovány. Pokud je tak nezbytné např. z důvodu národní bezpečnosti, obrany nebo pro odhalování a stíhání trestných činů, mohou jednotlivé státy omezit rozsah těchto práv a povinností.

7 Vyšetřování počítačové kriminality

Vyšetřování počítačové kriminality má svá vlastní specifika a liší se od běžně známých vyšetřovacích postupů. Na některá základní specifika upozorňuje V. Jirovský[80].

1. Velký objem a rozptýlení digitálních stop
2. Problém při zajištění příslušného hardwaru
3. Náročná vyčíslitelnost způsobených škod
4. Finanční náročnost vyšetřování – např. nákladný software
5. Průtahy při zajišťování digitálních stop
6. Legislativní nedostatky
7. Obtížnost dokazování

7.1 Finanční náročnost vyšetřovacích postupů

Práce vyšetřovatele klade důraz na vysokou kvalifikaci v dané problematice, avšak i vysoce kvalifikovaný odborník nemusí včas rozpoznat příslušnou hrozbu a digitální stopy mohou zmizet během několika málo minut. Také z tohoto důvodu je v oblasti počítačové kriminality velmi důležitá prevence. Pokud bychom kladli větší důraz na preventivní činnost, je pravděpodobné, že křivka nákladů by se rapidně snížila. Nejedná se pouze o software nutný k účinnému vyšetření konkrétního deliktu, ale také platy vysoce kvalifikovaných odborníků, složité znalecké posudky aj.

Pro většinu vyšetřovacích úkonů je nutná přítomnost kvalifikovaného odborníka, znalce a tito pracují s těmi nejmodernějšími technickými prostředky. Konkrétně se může jednat o potřebu zkopírovat určité paměťové médium, vyhnout se nástrahám, které pachatel připravil, koupi sledovacího zařízení, paměťových jednotek, obalových materiálů, hardwarového a softwarového vybavení obecně atp.[81] Má-li pevný disk kapacitu v řádech terabitů,[82] bude velmi nákladné vytvoření jeho identické kopie a bude nutné užití hned několika pevných disků popřípadě jiných paměťových zařízení.

[80] JIROVSKÝ: *Kybernetická kriminalita…*, s. 251
[81] PORADA, Viktor. Metody vyšetřování počítačové kriminality. 1. vydání. Praha: Policejní akademie České republiky. 1998. s. 28
[82] 1 terabit = 1000 gigabitů, tedy 10^{12} bitů.

7.2 Typické podněty k vyšetřování

V mnoha případech je pachatel odhalen spíše náhodně, například při svém vlastním pochybení. Vhodná je v tomto ohledu systematičtější práce vyšetřovatelů.[83] Typickým podnětem k vyšetřování počítačových deliktů jsou např. oznámení občanů, samotné výsledky operativně pátrací činnosti Policie ČR, popřípadě oznámení různých institucí. Občana může k oznámení vést „altruistická snaha" o přispění společnosti. V jiném případě se může jednat přímo o poškozeného, který má zájem na tom, aby došlo k náhradě veškeré škody. Zvláštní formou podnětů jsou anonymní oznámení nebo iniciativy soukromých detektivních subjektů.[84] Anonym může skýtat určitá rizika spojená s nevraživostí podatele, mstou, popřípadě potřebou zničit konkurenta, obchodního partnera atp.

7.3 Metodika vyšetřování počítačové kriminality

Metodik vyšetřování existuje celá řada. Obecně vzato se jedná o určitý proces vyšetřování, který se liší v závislosti na konkrétní situaci a osobě pachatele. Nelze tedy stanovit obecný vyšetřovací postup pro všechny situace zároveň.

„Pod odhalovací činností orgánů činných v trestním řízení se rozumí systém operativně pátracích a jiných opatření orgánů činných v trestním řízení za účelem získávání prvotních poznatků (signálů) o latentní trestné činnosti, zjištění existence faktu spáchání trestného činu a jeho dokumentace pro potřeby budoucího trestního stíhání."[85]

Důležité je zjistit, jakým způsobem pachatel pronikl k počítačovým datům, a zkusit tento postup rekonstruovat. Další 2 kroky jsou z hlediska dopadení pachatele nejdůležitější. Jedná se o stanovení okamžiku, kdy bude zahájeno trestní stíhání, a nastavení případné pasti na pachatele. V tuto chvíli je vhodné sbírat všechny potřebné důkazy a důležité informace. Jedním z posledních kroků je zjištění výše škody, která byla pachatelem způsobena. To je mnohdy obtížné, ne-li nemožné. Situaci neulehčuje ani skutečnost, že data, která jsou uložena na potenciálním důkazním materiálu, bývají často chráněna státem uznaným tajemstvím, ať již státním, bankovním atp. Situace tedy vyžaduje požádání příslušného orgánu o povolení

---

[83] LÁTAL, Ivo. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista*, 1998, č. 3, příloha.
Dostupné na <http://aplikace.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html>

[84] PORADA: *Metody vyšetřování počítačové…*, s. 24-25

[85] POŽÁR, Josef. Odhalování a vyšetřování kybernetické kriminality. In JIROVSKÝ, Václav (ed). *Sborník přednášek konference CYTER 2009*. Praha: České vysoké učení technické v Praze, Fakulta dopravní, Ústav informatiky a telekomunikací. 2009. s. 31

nebo souhlas, a tedy i o více času.[86] V oblasti počítačových deliktů se při vyšetřování rozhoduje v rámci minut nebo dokonce sekund. V opačném případě se důkazní materiály mohou stát nepoužitelnými, popřípadě jsou zničeny. Počítačová kriminalita je ze své podstaty skrytá činnost, jejíž následky nemusejí být zjevné hned od počátku. Jedná se spíše o trvající nebo pokračující delikty.[87]

7.3.1 Trasování pachatele

Pachatel svou činnost mnohdy účinně maskuje a úspěšně zahlazuje stopy, které by vyšetřovatele dovedly k jeho osobě. Často také nepoužije vlastního počítače, ale využije možnosti internetových kaváren nebo jiných veřejných míst, kde snáze dosáhne svého cíle. Situace je složitější v okamžiku, kdy k útoku dochází z vnějšího prostředí, což bude pravděpodobně pravidlem. To mimo jiné znamená, že k trasování[88] je potřeba využít sítě Internet. Trasování je závislé na záznamech, které mohou být pachatelem pozměněny. V této souvislosti hovoříme o tzv. logu.[89] Pokud tento záznam existuje, je pravděpodobné, že některé důležité údaje uvnitř budou pozměněny nebo budou z jiného důvodu nepoužitelné. Riziko spočívá ve skutečnosti, že log může být změněn samotným vyšetřovatelem při jeho neodborném zásahu nebo neúmyslným pochybením. [90]

7.4 Vyšetřovací situace

V rámci vyšetřování lze rozlišit určité vyšetřovací situace. Ty se liší zejména podle toho, zda-li je možné vyslovit závěr o totožnosti pachatele či nikoliv, popřípadě způsobu spáchaní trestného činu. Z pohledu kriminalisty je nejjednodušší situace, kdy je známa totožnost pachatele, a tak si může vytvořit vhodné vyšetřovací verze a sdělit obvinění konkrétní osobě.

Složitější situace nastane ve chvíli, kdy totožnost pachatele je sice známa, ale není jasné, jakým způsobem tento čin spáchal. Zde je vhodné předložit znalcům protokol o výslechu obviněného, aby orgány činné v trestním řízení mohly učinit vlastní závěry o její věrohodnosti a zkoumat technické detaily výpovědi.

Není-li známa ani totožnost pachatele, je situace z pohledu vyšetřování nejsložitější.

---

[86] PORADA: *Metody vyšetřování počítačové…*, s. 26
[87] PORADA, Viktor. *Kriminalistická metodika vyšetřování*. 1. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. 2007. s. 190
[88] specializovaný zápis informací o aktuálně spuštěném programu
[89] tzv. záznam o provozu systému
[90] JIROVSKÝ: *Kybernetická kriminalita…*, s. 256

Jedním z možných důvodů je fakt, že pokud po sobě pachatel nezanechá žádné stopy, může být jeho odhalení velmi obtížné až nemožné. Vyšetřovatel se musí zaměřit na získání možných zdrojů, ze kterých by plynuly informace o pachateli. Tyto mohou při absenci stop chybět. Nutná je hlavně analýza způsobu spáchaní trestného činu za pomoci soudního znalce.[91] Určení konkrétního způsobu spáchání trestného činu může vyloučit z vyšetřování konkrétní osoby, které:[92]

- nejsou zaměstnány v určité instituci
- nemají možnost provádět dané operace
- neznají přesně posloupnost potřebných operací
- neznají detailně funkce používaného programu
- nemají přístup k programovému vybavení pracoviště nebo speciálním souborům
- nevykonávají činnost, která předpokládá kumulaci konkrétních funkcí atp.

Počítačový expert vyšetřující tuto trestnou činnost musí rozpoznat rozdíl mezi bezcenným materiálem a potenciálním důkazem. Ne všechny posbírané stopy mohou v pozdějších fázích řízení sloužit jako důkaz, dokonce mohou být důkazem nezákonným. Dvě stopy se mohou navzájem vylučovat a být tak v přímém rozporu. Vhodné je doporučit jejich zálohu a pracovat pouze s kopií systému, přičemž originál si ponechat pro případ potřeby.[93] Hovoříme-li o konkrétních postupech, je vhodné dále doporučit zkoumání systému z hlediska specifických klíčových slov, zjištění stavu systémových souborů a obecně tyto soubory analyzovat. Je také vhodné zkoumat datum změny nebo vytvoření jednotlivých souborů aj.[94]

7.5 Přibrání znalce k vyšetřování počítačových deliktů a činnost počítačových expertů

Kriminalisté se mnohdy k vyšetřování počítačového deliktu nedostanou, a to z důvodu jeho neoznámení. Společnosti se snaží řešit si tyto problémy samy, protože často nedisponují potřebnými odborníky a kapacitami, které by příslušnou problematiku úspěšně vyřešily. Otázkou je také rozsah kompetencí soukromých subjektů. Orgány činné v trestním řízení mají mnohem více možností zasáhnout a učinit příslušné opatření. V tomto ohledu je vhodné

[91] PORADA: *Kriminalistická metodika...*, s. 187-189
[92] PORADA: *Metody vyšetřování počítačové...*, s. 17
[93] JIROVSKÝ: *Kybernetická kriminalita...*, s. 257
[94] Tamtéž, s. 258

zmínit možnost tvorby vyšetřovacího týmu, skládajícího se z odborníků, konzultantů popřípadě soudních znalců. V oblasti počítačové kriminality se můžeme setkat s termínem, který původně označuje americké speciální jednotky, tedy „SWAT“[95] nebo „CSIRT“, tedy Computer Security Incident Response Team.[96]

Dle ustanovení § 105 odst. 1 trestního řádu: *„Je-li k objasnění skutečnosti důležité pro trestní řízení třeba odborných znalostí, vyžádá orgán činný v trestním řízení odborné vyjádření. Jestliže pro složitost posuzované otázky takový postup není postačující, přibere orgán činný v trestním řízení znalce. V přípravném řízení přibírá znalce ten orgán činný v trestním řízení, jež považuje znalecký posudek za nezbytný pro rozhodnutí…“*[97]

Příklad, kdy je nanejvýš vhodné soudního znalce přibrat, uvádí Ivo Látal. Je-li při nalezení zemřelého, popřípadě u domovní prohlídky, nalezen elektronický diář, který by mohl objasnit základní informace o daném skutku a který by mohl být stěžejním důkazem v případu, je zapotřebí přibrat soudního znalce a to z toho důvodu, aby účinně zajistil tento důkazní materiál, nevybily se baterie nebo se diář jinak neznehodnotil. Otázkou pro znalce by mohla být např. skutečnost, zda-li je možné příslušné informace z elektronického diáře obnovit, popřípadě přenést na jiný přístroj, určit značku, výrobní číslo diáře a další.[98] Znalci nepřísluší zkoumat právní stránku věci, např. hodnotit, zda-li daná informace souvisí či nesouvisí s příslušnou trestnou činností.

Otázka, jaké experty si společnost „najme“, závisí na její velikosti a finančních možnostech. Menší si vystačí s počítačových technikem, který zajistí běžný chod, aktualizaci softwaru, jako je antivirový program, a kontrolu legálního softwaru. Problémem této trestné činnosti je právě požadavek na odbornost při úkonech s výpočetní technikou. Větší společnosti mají možnost pracovat se specialisty z útvaru informatiky, kteří provádějí revize logů, předávají zprávy o neobvyklém chování systému a kteří v neposlední řadě spolupracují při určování výše škod.

Počítačový expert vstupující na místo, na kterém se nachází příslušná výpočetní technika, musí postupovat velmi obezřetně a celý proces řádně dokumentovat. V případě, že v operačním systému „běží“ určité procesy, odborník tyto procesy po bližším zkoumání ukončuje a sleduje síťové aktivity. V případě, že objeví nežádoucí aktivitu, která by mohla vést ke zničení či poškození dat, ukončí činnost počítače násilným způsobem, tedy vypojením

---

[95] anglická zkratka pro „Special Weapon and Tactics“
[96] JIROVSKÝ: *Kybernetická kriminalita…* , s. 260
[97] aktuální znění: zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů
[98] LÁTAL, Ivo. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista*, 1998, č. 3, příloha.
Dostupné na <http://aplikace.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html>

ze zdroje. Tento postup však může být zrádný. Může dojít, a velmi pravděpodobně dojde, k poškození otevřených souborů a běžících procesů, které nebyly řádně ukončeny.

Pachatel je často vysoce kvalifikovaný a stopy mohou zmizet během několika málo okamžiků. Řadový policista nemá mnohdy dostatek odborných znalostí k posouzení situace a k okamžitému zásahu do hardwaru nebo softwaru počítače, jenž by odvrátil zničení nebo poškození dat, které by později mohly sloužit jako vhodná stopa. Viktor Porada uvádí vhodnost použití tzv. momentu překvapení.[99]

K úkonu, který je často na začátku vyšetřování zapotřebí nařídit, patří domovní prohlídka, která umožňuje vyhledat relevantní média jako jsou CD-ROMy, Flash paměti a další. Tyto mohou přispět k objasnění činu, protože pachatel si s velkou pravděpodobností informace a postupy, kterými svého jednání dosáhl, nebude uchovávat na hlavním paměťovém médiu.[100]

Způsoby, jakými lze páchat počítačové delikty jsou různorodé. Může dojít ke změně uložených dat, většinou zaměstnancem společnosti, popřípadě k neoprávněnému proniknutí do počítače, počítačového systému a jeho databáze. Zde existují 2 základní varianty možného jednání pachatele. Získá-li přístup do příslušné databáze, systému atp., postačí mu pocit určitého uspokojení z toho, že něco dokázal, překonal ochranu uživatele. V druhém případě informace, které neoprávněně získal, užije pro účely obchodní nebo obdobné. Získané informace může také zničit.[101] K závažným následkům může dojít také při neoprávněných pokynech k počítačovým operacím. Příkladem může být nákup losů loterie nebo podobné hry, kdy pachatel vlastním programem ovlivní generování náhodných čísel tím způsobem, že budou vygenerována ta čísla, která sám zakoupil.[102]

Pro pochopení problematiky vyšetřování počítačové kriminality je vhodné definovat pojem „bezpečnostní incident“. Dle V. Jirovského je to: *„Jakákoliv událost, která způsobila, že došlo k narušení činnosti počítačového systému, sítě nebo jejich součástí, či byl umožněn neautorizovaný přístup k datům, která následovně byla zmanipulována, vymazána, učiněna nepřístupnými nebo naopak zpřístupněna neoprávněným subjektům.“*[103]

---

[99] PORADA: *Kriminalistická metodika…*, s. 191
[100] PORADA: *Metody vyšetřování počítačové…*, s. 29-30
[101] PORADA: *Kriminalistická metodika…*, s. 184-185
[102] PORADA: *Metody vyšetřování počítačové…*, s. 11
[103] JIROVSKÝ: *Kybernetická kriminalita…*, s. 266

7.6 Počítačové stopy

Při vyšetřování hrají jedny z nejdůležitějších rolí ty stopy, které po pachateli zůstanou a které tak mohou napomoci k jeho dopadení. Hovoříme o tzv. „počítačových stopách". Ty nejtypičtější se nacházejí na pevném disku v podobě určitých dokumentů, popřípadě jiných typů souborů, na vyměnitelných paměťových médiích (např. Flash-disku nebo CD-ROMu). Významnou stopou může být také hardware počítače. I v případě počítačové kriminality se můžeme setkat se stopami typickými pro tzv. „klasickou" trestnou činnost. Kupříkladu stopy daktyloskopické, které lze nalézt uvnitř demontovaného počítače, dále ruční písmo nalezené na papírových poznámkách, stopy fonoskopické, mechanoskopické a další. Časté jsou také tzv. stopy účetní, tedy různé doklady, bilance a uzávěrky. Stejně jako při vyšetřování jiných trestných činů i zde se mohou objevit stopy paměťové. Jedná se o informace, které je určitá osoba schopna reprodukovat svými smysly a kterých konkrétní osoba nabyla v souvislosti s vyšetřovaným trestným činem, např. o přípravě činu, o průběhu událostí atp.[104]

V souvislosti s počítačovou kriminalitou hovoříme také o tzv. digitálních důkazech. Existuje více definic pojmu digitální důkaz. Obecně lze říci, že se jedná o: *„jakoukoli informaci s průkazní hodnotou ve vztahu k dané události, která je uložená nebo přenášená v digitální podobě."*[105] Při práci s těmito specifickými důkazy je nutné mít alespoň základní povědomí o skutečnostech, které digitální důkazy odlišují od těch „klasických".

Příklad, kdy se digitální důkaz ukázal jako stěžejní k vyšetření celého případu, uvádí Liljana Selinšek. Ve Velké Británii byl uškrcen muž vracející se ze svého oblíbeného podniku. Vzhledem k silnému dešti nebylo možné použít vzorek DNA nalezený na krku zemřelého a srovnat ho se vzorkem příbuzných. Hlavním podezřelým v případu byl švagr zemřelého, který odmítal spolupracovat. Vyšetřovatelé zabavili jeho osobní počítač a odborník na počítačovou forenzní analýzu zjistil, že den před vraždou si dotyčný zadal do internetového vyhledávače větu „jak zabít člověka". Toto zjištění hrálo velkou roli v další fázi případu.[106]

---

[104] PORADA: *Metody vyšetřování počítačové…*, s. 14-15
[105] SELINŠEK, Liljana. Některé právní aspekty forenzní analýzy digitálních dat. In HORYNA, Mojmír (ed). *Český právní řád a ochrana kyberprostoru: (vybrané problémy).* Praha: Karolinum, 2008, s. 133
[106] Tamtéž, s. 137

7.7 Nakládání s důkazy

Pokud příslušný bezpečnostní incident neskončí ve fázi administrativní, tedy tzv. „uvnitř“ podniku, je pravděpodobné, že se případem bude zabývat soud. V tuto chvíli je jednou ze zásadních otázek sběr důkazních materiálů, správná manipulace s nimi a jejich správné uchování.

7.7.1 Problémy při manipulaci s důkazy[107]

1. Prvním subjektem, který se o bezpečnostním incidentu dozví, je většinou IT oddělení nebo jemu podobný útvar, které se může snažit incident tzv. „zamést pod koberec“ a neposkytnout tak správné informace managementu, který by včasným rozhodnutím mohl reagovat.
2. Přístup zaměstnanců k citlivým údajům společnosti.
3. Podcenění rozsahu a významu incidentu.
4. Neexistující plán reakce na incident – v případě, kdy tento plán není připraven ve chvíli, kdy k incidentu dojde, může dojít k řadě pochybení v zákoně, popřípadě časovým ztrátám.

7.7.2 Evidence důkazního materiálu

Důležité je také všechny důkazy správně zaevidovat a uchovat. Vhodné je mít tzv. „evidenční list“, ve kterém bude uvedeno, kolik osob se s daným důkazem mohlo seznámit a přijít s ním do kontaktu, dále také odkud byly důkazy obdrženy, odkud kam byly přemisťovány a kam byly uloženy. Při práci s důkazním materiálem je nutné brát v potaz, že celý proces vyšetřování, sběru důkazů atp. se jednou někdo bude snažit zpochybnit a napadnout. Proto je evidence tak podstatnou součástí vyšetřování.[108]

Dle Zdeňka Blažka se důkazy nejčastěji nacházejí na firewallech, routrech a uživatelských PC. Při získání takového důkazu je obecným problémem jeho užití jako důkazu přímého. To lze pouze v případě, je-li možné spojit ho s konkrétní osobou, a to jednoznačně.[109]

---

[107] PROISE, Chris. MANDIA, Kevin. *Počítačový útok : detekce, obrana a okamžitá náprava*. 1. vydání. Praha : Computer Press. 2002. s. 77
[108] Tamtéž, s. 78-79
[109] KRČMÁŘ, Petr. *Jaké aktuální hrozby číhají na uživatele internetu?* [online]. root.cz, 27. února 2009 [cit. 4 ledna 2011]. Dostupné na <http://www.root.cz/clanky/jake-aktualni-hrozby-cihaji-na-uzivatele-internetu/>

7.8 Shrnutí kapitoly

Z výše podaného výkladu je zřejmé, že odhalování počítačové kriminality je záležitostí obnášející řadu specifických postupů a řešení. Dynamický vývoj tohoto druhu kriminality a vysoce kvalifikovaný pachatel znesnadňují shromažďování důkazů a možnost jeho usvědčení z trestné činnosti. Orgány činné v trestním řízení musejí být zásobeny aktuálními informacemi. Mezi rozhodné informace, které mohou napomoci k dopadení pachatele, patří určení konkrétního motivu, zodpovězení otázky, zda došlo ke vzniku škody, a určení její výše. V neposlední řadě také informace o tom, do jaké míry pachatel disponoval kvalifikovanými informacemi, tedy jeho znalosti výpočetní techniky, rozsah oprávnění pachatele atp. Důležité je také zjištění, zda byl překročen rozsah daných kompetencí nebo zda se jednalo o zásah v jejich mezích.[110]

Pro počítačovou kriminalitu je také typická spolupráce v mezinárodním měřítku. Jedná se o trestnou činnost, která není vázána na konkrétní místo. Pachatel může „útočit" na počítač prostřednictvím jiného stroje, který patří nic netušícímu uživateli. Vyšetřování na území jednoho státu by tedy pravděpodobně nevedlo k úspěchu a mezinárodní spolupráce je v těchto případech bezpodmínečná. V úvahu připadá využití mezinárodních policejních institucí jako Europol nebo Interpol.

[110] PORADA: *Kriminalistická metodika...*, s. 190

8 Osoba pachatele

Pachatelem počítačové kriminality se často stává zaměstnanec určité společnosti, který má jednoduchý přístup k zásadním přístupovým údajům a zjednodušenou pozici pro přípravu své trestné činnosti. Již z podstaty této trestné činnosti, tedy především technické a personální náročnosti při odhalování, je zřejmé, že se jedná o pachatele vzdělaného, vysoce kvalifikovaného a specializovaného v oblasti výpočetních technologií. Ve většině případů se jedná o vzdělání vysokoškolské, které souvisí zejména s technickými obory. Důležitým prvkem osobnosti pachatele je jeho pocit, že se nedopouští ničeho závažného, vymykajícího se všedním činnostem. Sedě v přítmí svého pokoje při práci s klávesnicí stolního počítače, nedokáže mnohdy domyslet důsledky, které z takového jednání mohou vyplynout. To je způsobeno také jistým specifikem počítačové kriminality a to tím, že zde absentuje prvek násilí.[111]

Pachatelé počítačových deliktů mají většinou problémy v sociální oblasti, mají problémy s navazováním vztahů, a proto se uchylují ke kontaktu „elektronickému" prostřednictvím sítě Internet. Připojují se do různých komunit a v rámci své protiprávní činnosti spolupracují. Pro stanovení okruhu pachatelů je důležité určit konkrétní motiv, který pachatele k trestnému činu vedl.

8.3 Motiv

Těmi nejdůležitějšími motivy jsou:[112]

1. zištné motivy (možnost rychle docílit velkého finančního obnosu)
2. motivy vyplývající z konfliktů v mezilidských vztazích
3. touha po moci (např. likvidace konkurentů)
4. touha dokázat svoji intelektuální převahu (např. nad vlastním zaměstnavatelem)
5. touha překonat určitý pocit nedocenění (ze strany přátel, rodiny atp.)
6. krycí motiv k utajení jiné trestné činnosti
7. snaha o vyniknutí v obchodní činnosti
8. politické motivy (likvidace politických protivníků)

---

[111] LÁTAL, Ivo. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista*, 1998, č. 3, příloha.
Dostupné na <http://aplikace.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html>
[112] PORADA: *Metody vyšetřování počítačové…*, s. 13

Z hlediska policejní praxe je důležité, že se tyto motivy nevyskytují samostatně ale častěji v kombinaci s několika dalšími.

Pachatele můžeme zjednodušeně rozdělit na tzv. amatéry a profesionály.

8.2 Pachatel amatér

Typicky se jedná o tzv. hackery. V jejich zájmu nemusí být primárně finanční zisk či potřeba získat určité informace popřípadě narušit systém. Projevuje se zde především snaha získat uznání. Jde spíše o určitý požitek, „sportovní“ zábavu. V těchto případech mu postačí, když se o daném činu začne hovořit. Dále se může jednat o pachatele, kteří se mstí nebo o tzv. crackery, tedy osoby, kterým jde spíše o destrukci systému, která jim přináší potěšení. I v případě pachatelů amatérů se jedná o osoby velmi vzdělané, flexibilní, přístupné učení se novým poznatkům a otevřené novým informacím.

8.3 Pachatel profesionál

Pachatel profesionál představuje vysokou hrozbu, protože při své činnosti využívá informace pocházející z jeho zaměstnání a mnohdy vyvíjí protiprávní činnost právě pro svého zaměstnavatele. Řadíme sem také počítačové piráty, jejichž cílem je zisk z jejich protiprávní činnosti, tedy prodeje nelegálního softwaru.[113]

[113] LÁTAL, Ivo. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista*, 1998, č. 3, příloha.
Dostupné na <http://aplikace.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html>

9 Softwarové pirátství

9.1 Business software aliance – BSA

Celosvětově působí na poli počítačového pirátství BSA. Svou činnost vyvíjí ve více než 80-ti zemích světa a hájí zájmy komerčního softwaru. Jedním z hlavních bodů její činnosti je ochrana duševního vlastnictví. Působí mimo jiné v Číně, Rusku, Indii a spolupracuje s celou řadou dalších organizací. Tvář BSA udávají její členové, mezi nimiž nechybí ti největší distributoři softwaru na světě jako jsou Microsoft, Apple, IBM, Dell, Adobe a další.[114] Dle této mezinárodní protipirátské organizace se na území České republiky používá přibližně 38 % softwarových produktů nelegálně. Situace v ČR spíše stagnuje a během posledních let se pohybuje stále na stejných hodnotách. Polsko a Slovensko jsou v rámci hodnocení užívání nelegálního softwaru statisticky v horším postavení. Opačná situace panuje v Rakousku a Německu. Ty patří k zemím s nejnižší mírou počítačového pirátství na světě.[115]

V případě snížení míry softwarového pirátství by z tohoto faktu těžila hlavně ekonomika. Stát by tak získal více nejen na daních, ale vznikla by také řada nových pracovních míst. Jak dodává Jan Hlaváč, tiskový mluvčí BSA: *„Pirátství jednoznačně škrtí ekonomický rozvoj…“*[116]

Diskuzi v laické i odborné veřejnosti vyvolala situace ohledně spolupráce BSA a Ministerstva financí ČR. Tito společně vydali tiskovou zprávu obsahující informace o tom, že počítačové pirátství bude častěji postihováno jako tzv. daňový únik. Meritum věci spočívá v tom, že pokud si podnikatel nebo společnost odepíše z daní příslušný druh hardwaru, automaticky lze předpokládat, že musí odepsat taktéž příslušný software. Neučiní-li tak, dostává se do hledáčku podezřelých. Taková skutečnost přehlíží software přístupný bezplatně, tedy např. tzv. open-source. Tisková zpráva, která byla později Ministerstvem financí pozměněna, se o bezplatném softwaru zpočátku nezmiňovala.[117]

---

[114] viz. http://www.bsa.org/country/BSA%20and%20Members/Our%20Members.aspx

[115] HLAVÁČ, Jan. *SOFTWAROVÉ PIRÁTSTVÍ KLESLO: V ČESKU SE UŽÍVÁ 38 % SOFTWARU NELEGÁLNĚ* [online]. portal.bsa.org, 12. května 2009 [cit. 20. prosince 2010]. Dostupné na <http://portal.bsa.org/globalpiracy2008/pr/pr_czechrep.pdf>

[116] HLAVÁČ, Jan. *SNÍŽENÍ MÍRY SOFTWAROVÉHO PIRÁTSTVÍ PŘINESE ČESKU MILIARDY KORUN, STUDIE POUKAZUJE NA EKONOMICKÉ PŘÍNOSY SNÍŽENÍ MÍRY SOFTWAROVÉHO PIRÁTSTVÍ* [online]. portal.bsa.org, 15. září 2010 [cit. 21. prosince 2010]. Dostupné na <http://portal.bsa.org/piracyimpact2010/pr/pr_czechrepublic_czech.pdf>

[117] KLIMÁNEK, Oldřich. *Spolupráce BSA a Ministerstva financí: „Hardware bez softwaru není uznatelný daňový náklad“ aneb Bezplatný software je automaticky pirátský?* [online]. dsl.cz, 28. května 2010 [cit. 22.

9.2 Software a duševní vlastnictví

Software je jako duševní vlastnictví uznáván již od roku 1980. Před tímto datem neexistovala platná legislativa, která by bránila jeho zcizení nebo kopírování. Teprve od okamžiku, kdy byl software definován jako literární dílo a kdy vydal na konci devadesátých let patentový úřad Spojených států amerických první patenty softwarovým vývojářům, rozvinulo se autorské právo a ochrana duševního vlastnictví obecně.[118]

První aplikace vznikaly v jakýchsi počítačových kroužcích, ve kterých se počítačoví příznivci scházeli a vyměňovali si své zkušenosti se softwarovými produkty. Začali si vytvářet vlastní aplikace a experimentovat. Určitým mezníkem byl vznik počítačových sdružení, tzv. Bulletin Board Systems (BBS). Pro komunikaci a výměnu zkušeností s ostatními se stačilo připojit k jedinému zařízení a to za pomoci modemu.[119] Proti rozvoji počítačového pirátství brojilo mnoho organizací. Prvními z nich byly např. „Sdružení vydavatelů softwaru“[120], „Kanadská aliance proti softwarové krádeži“[121] a „Aliance obchodního softwaru“[122]. Tyto organizace mnohdy nabízely za důležité informace vedoucí k dopadení „počítačových pirátů“ finanční odměnu.[123] Prvotním účelem počítačových pirátů bylo za pomoci ostatních uživatelů získat bezplatně komerční softwarové produkty. Postupem času se tento účel měnil a rozšiřoval. Již nebyl zájem na tom, zda-li někdo pirátský software používá, ale šlo o určitou zálibu v této činnosti. Jednalo se vlastně o určitou soutěž s ostatními piráty.[124]

V mnoha zemích se procento užívání nelegálního softwaru pohybuje pravidelně ve vysokých hodnotách. V počátcích softwarového pirátství se setkáváme hlavně s nízkou úrovní právního vědomí uživatelů a to nejen při instalaci aplikací na osobních počítačích, ale také ve velkých podnicích a v důležitých institucích.

9.3 Prameny softwarového pirátství

Nejdůležitější vnitrostátní právní normou týkající se softwarového pirátství je u nás již dlouhou dobu zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem

---

prosince 2010]. Dostupné na <http://www.dsl.cz/clanek/1795-spoluprace-bsa-a-ministerstva-financi-8222-hardware-bez-softwaru-neni-uznatelny-da-ovy-naklad-8220-aneb-bezplatny-software-je-automaticky-piratsky>

[118] CRAIG, Paul. HONICK, Ron. *Softwarové pirátství bez záhad*. 1. vydání. Praha: Grada. 2008. s. 27-28

[119] Tamtéž, s. 29

[120] Software Publisher´s Association, SPA

[121] Canadian Aliance Againts Software Theft, CAAST

[122] Business Software Aliance, BSA

[123] CRAIG: *Softwarové pirátství...* , s. 31

[124] Tamtéž, s. 32

autorským a o změně některých zákonů. Z mezinárodního hlediska hrají významnou roli také normy jako Bernská úmluva o ochraně literárních a uměleckých děl z roku 1986, Všeobecná úmluva o autorském právu z roku 1952, ale také úmluva o zřízení Světové organizace duševního vlastnictví (WIPO) z roku 1967.

Při hledání důvodů, proč se softwarové produkty nelegálně „kopírují" popřípadě proč dochází k prolamování ochran aplikací, mnohdy dojdeme k závěru, že největší vliv má samotná výsledná cena produktů.[125] Dle WIPO jsou duševním vlastnictvím: *„Práva k literárním, uměleckým a vědeckým účelům, k výkonu výkonných umělců, zvukových záznamů a rozhlasovému vysílání, k vynálezům ze všech oblastí lidské činnosti, k vědeckým objevům, k průmyslovým vzorům a modelům, k továrním, obchodním známkám a známkám služeb, jako i k obchodním jménům, práva na ochranu proti nekalé soutěži a všechna ostatní práva vztahující se k duševní činnosti v oblasti průmyslové, vědecké, literární a umělecké"*[126]

9.4 Případ Napster

Program Napster s sebou přinesl novou řadu problémů, do té doby neznámých. Jednalo se o program pro sdílení hudby v digitálním formátu mp3.[127] Docházelo ke sdílení zvukových souborů, které tak byly šířeny bez jakéhokoliv poplatku a které byly přitom pod ochranou autorského práva. Soudní spor, na základě žaloby americké organizace nahrávacích společností RIAA, Napster prohrál. Stěžejní problém spočíval v centrální databázi s indexem nahrávek uživatelů. V současné době jsou obdobné programy prakticky nepostižitelné, jelikož problém s indexováním vyřešily.[128] Příkladem je v současnosti oblíbená aplikace pro sdílení souborů DC++.[129]

V případě médií jako jsou filmy, hudební soubory atp., není z hlediska legislativy problém, pokud je uživatel „drží" na svém počítači a užívá pro vlastní potřebu. Komplikace nastávají až v okamžiku, kdy by takový materiál sdílel v síti s jinými uživateli. U nelegálního softwaru je situace odlišná. Trestně postižitelné je i samotné „držení" takového softwaru. V praxi se jedná o případy, kdy má uživatel nainstalován daný program přímo na svém počítači.

Hodnota současného softwaru se pohybuje i v rámci desítek tisíc korun, a tudíž

[125] PORADA, Viktor. KONRÁD, Zdeněk. *Metodika vyšetřování softwarového pirátství*. 1. vydání. Praha: Policejní akademie České republiky. 1999. s. 6-7
[126] Vyhláška ministra zahraničních věcí č.69/1975 Sb. O Úmluvě o zřízení Světové organizace duševního vlastnictví podepsané ve Stockholmu dne 14. července 1967, ve znění vyhlášky č. 80/1985 Sb.
[127] Jeden z formátů zvukových souborů, založený na kompresním algoritmu MPEG.
[128] MATĚJKA: *Počítačová kriminalita*, s. 36-37
[129] klient, který slouží k peer-to-peer sdílení souborů na síti

z pouhé neznalosti počítačových uživatelů může být lehce způsobena značná škoda. Karel Kuchařík, vedoucí skupiny pro odhalování informační kriminality při Úřadu služby kriminální policie a vyšetřování Policejního prezidia ČR, jako příklad uvádí program AutoCad,[130] popřípadě grafické studio.[131]

9.5 Zjištění údajů o uskutečněném telekomunikačním provozu

Jednou z účinných cest, jak efektivně oslovit poskytovatele internetového připojení, aby vykázal např. detailní informace o datovém toku nebo přidělených IP adresách, je prostřednictvím ustanovení § 88a TrŘ:

(Odst. 1) *„Je-li k objasnění skutečností důležitých pro trestní řízení třeba zjistit údaje o uskutečněném telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, nařídí předseda senátu a v přípravném řízení soudce, aby je právnické nebo fyzické osoby, které vykonávají telekomunikační činnost, sdělily jemu a v přípravném řízení buď státnímu zástupci nebo policejnímu orgánu. Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn.“* [132]

Z tohoto písemného příkazu by mělo být patrné, že povede k objasnění skutečností důležitých pro trestní řízení. Takového příkazu není třeba v případě dobrovolného souhlasu poskytovatele telekomunikačního zařízení. Pozor je však nutné dát zejména na čl. 13 LZPS, který hovoří o porušení listovního tajemství, zprávách podávaných telefonem atp.[133]

9.6 Nařízení domovní prohlídky

Další účinnou možností je nařízení domovní prohlídky, pro kterou trestní řád určuje taktéž přísné podmínky. V bytě nebo domě se může nacházet technika, prostřednictvím které se pachatel trestného činu dopustil. Ponejvíce se bude jednat o samotný počítač, DVD přehrávač, flash paměti aj. Konkrétní podmínky jsou uvedeny v ustanovení § 82 TrŘ:

(Odst. 1) *„Domovní prohlídku lze vykonat, je-li důvodné podezření, že v bytě nebo jiné prostoře sloužící k bydlení nebo v prostorách k nim náležejících (obydlí) je věc nebo osoba důležitá pro trestní řízení.*

---

[130] software pro navrhování ve 2D & 3D
[131] POTŮČEK, Jan. *Karel Kuchařík: dostaneme se i do uzavřených sítí* [online]. lupa.cz, 13.února 2007 [cit. 23. prosince 2010]. Dostupné na <http://www.lupa.cz/clanky/karel-kucharik-dostaneme-se-i-do-uzavrenych-siti/>
[132] aktuální znění: zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů
[133] aktuální znění: Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů

(Odst. 2) *Z důvodů uvedených v odstavci 1 lze vykonat i prohlídku prostor nesloužících k bydlení (jiných prostor) a pozemků, pokud nejsou veřejně přístupné.*

(Odst. 3) *Osobní prohlídku lze vykonat, je-li důvodné podezření, že někdo má u sebe věc důležitou pro trestní řízení…* "[134]

Tento příkaz musí být doručen do 24 hodin od chvíle, kdy odpadla překážka, která doručení bránila (podezřelý je např. na útěku).

V praxi budou orgány činné v trestním řízení uvažovat, zda-li je vhodnější odebrat celý osobní počítač nebo samostatný pevný disk, popřípadě jiné médium, na kterém může být nelegální software nainstalován či uložen. Taková věc může být podezřelé osobě také odňata.[135] Poté co odmítne dobrovolné vydání věci důležité pro trestní řízení, může dle ustanovení § 79 TrŘ. dojít k jejímu odnětí. Tak tomu bude v mnoha případech v souvislosti s domovní prohlídkou.

Soud může také rozhodnout o trestu propadnutí věci nebo jiné majetkové hodnoty a to za splnění podmínek uvedených v ustanovení § 55 TrZ zejména užil-li pachatel ke spáchaní trestného činu DVD, CD nebo jiného média. Musí se však jednat o věc nebo jinou majetkovou hodnotu náležící pachateli.

9.7 Vyšetřování softwarového pirátství

V případech softwarového pirátství je odhalení pachatele taktéž velmi obtížné. Prozradit se může sám např. inzercí o prodeji nelegálně „pálených" DVD disků v internetových anoncích nebo vystavením se nastrčené policejní volavce při předávání peněz. Možná je také situace, kdy bývalý zaměstnanec společnosti zatouží po odplatě zaměstnavateli, na kterého podá trestní oznámení. Iniciativa tedy vzejde ze strany občana.

Účinným způsobem, jak odhalit nelegální software uvnitř uživatelova počítače, je softwarový audit, který je schopen rozpoznat veškerý software u uživatele a který tak vyšetřovatelům ulehčí práci. Stejně tak je za určitých okolností možné odhalit již odinstalované aplikace popřípadě smazané soubory.[136]

---

[134] aktuální znění: zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů

[135] KRUTINA, Miroslav. MÚKA, Ondřej. *Odnětí a vydání věci doličné při podezření z porušení autorského práva* [online]. lupa.cz, 2. února 2007 [cit. 26. prosince 2010]. Dostupné na <http://www.lupa.cz/clanky/odneti-a-vydani-veci-dolicne-pri-podezreni-z-poruseni-autorskeho-prava/>

[136] MATĚJKA: *Počítačová kriminalita*, s. 85-86

Existují specifické stopy a soudní důkazy typické pouze pro softwarové pirátství. Jedná se hlavně o:[137]

1. neoprávněně zhotovené rozmnoženiny a plagiáty děl (literárních, uměleckých, vědeckých) a počítačových programů
2. nelegálně zhotovené obrazové a zvukové záznamy
3. nabývací doklady k podezřelým produktům
4. technické dokumentace (výrobní, projektová)
5. listinné důkazy (např. živnostenský list, smlouvy)
6. stopy ve vědomí ostatních osob

K těm nejzásadnějším otázkám, se kterými se vyšetřovatel při své činnosti setká, patří otázka, jedná-li se o dílo či produkt spadající pod ochranu duševního vlastnictví. Je-li tomu tak, zaměří se orgány činné v trestním řízení na samotného nositele práv vyplývajících z duševního vlastnictví.[138]

V pozdějších fázích vyšetřování dochází k podrobnému zkoumání pachatelových aktivit v síti Internet jako je účast v diskuzích, kde poptává aktuální nelegální software, nebo jeho inzeráty a emailová komunikace.[139]

9.7.1 Doložení legality softwarových produktů

V souvislosti s dokládáním legality nabytého softwaru je podstatné uchování dokladu o nabytí takového softwaru. Ani v tomto případě však nemáme absolutní jistotu ochrany a beztrestnosti. Podnikatelům tuto povinnost ukládá ustanovení § 31 a 32 zákona o účetnictví.[140] V případě běžného uživatele PC však takováto povinnost stanovena není a je otázkou, zda je uschování všech dokladů o nabytí v trestním právu bezvýhradně nutné.

V případě trestního řízení je třeba, aby spáchání trestného činu bylo pachateli prokázáno. On sám nemá povinnost obrany, uvádění důkazů popřípadě dalších okolností, které by mu v řízení mohly přispět k obraně. Samotným nabytím vlastnického práva k věci (prostřednictvím níž je dílo vyjádřeno) nenabývá uživatel softwaru právo díla užít, což je další

[137] MUSIL, Jan. KONRÁD, Zdeněk. SUCHÁNEK, Jaroslav. *Kriminalistika.* 2. vydání. Praha: C.H. Beck. 2004. s. 240
[138] Tamtéž, s. 241
[139] MATĚJKA: *Počítačová kriminalita*, s. 85-86
[140] aktuální znění: zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů

argument vymezující se proti diskuzím na veřejnosti obhajující bezpodmínečné uschovávání všech dokladů o nabytí vlastnictví.[141]

9.7.2 Warez

V úzkém spojení s nelegálním softwarem je jeho výroba a rozšiřování, tedy warez. Tato aktivita se nejvíce rozmohla společně s vývojem sítě Internet. V případě médií jako jsou CD, DVD by šíření nebylo tak masivní jako za pomoci Internetu. Jedná se o velkou síť uživatelů, typicky velmi organizovanou a dodržující pevná pravidla. Každý ve warez skupině má určitou funkci a jejím hlavním účelem je vydávání a rozšiřování toho, co není zatím volně a bezplatně k dispozici. Jednu z nejdůležitějších funkcí zastává cracker, tedy typicky zkušený a vzdělaný programátor, který dokáže obejít ochranu určitého produktu. Velké množství nelegálních dat se šíří např. skrze peer-to-peer[142] technologii.[143]

Odhalení pachatele, např. „crackera", může být velmi složité vzhledem k latenci této trestné činnosti. K odhalení může dojít na základě vlastních poznatků orgánů činných v trestním řízení nebo z podnětu České protipirátské unie popřípadě Ochranného svazu autorského.[144]

9.8 Trestný čin porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle ustanovení § 270 TrZ.

(Odst. 1) *„Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty..."*[145]

Trestněprávní postih porušení autorského práva je zakotven v ustanovení, které má tzv. „blanketní dispozici".[146] Odkazuje tedy na úpravu jinou, konkrétně na zákon upravující právo autorské, práva související s právem autorským a práva k databázi.[147] Objektem tohoto

---

[141] SMEJKAL: *Internet a §§§*, s. 71-72
[142] architektura počítačových sítí, ve kterých spolu komunikují přímo uživatelé
[143] JIROVSKÝ: *Kybernetická kriminalita*, s. 68-69
[144] MINÁRIK, Tomáš. Peer-to-peer sítě z hlediska trestního práva. In HORYNA, Mojmír (ed). Český právní řád a ochrana kyberprostoru: (vybrané problémy). Praha: Karolinum, 2008, s. 74
[145] aktuální znění: zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
[146] blanketní dispozice odkazuje obecně na normu nebo na více norem stejného druhu viz. např. JELÍNEK: *Trestní právo*..., s. 47
[147] aktuální znění: zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů

trestného činu je zájem na ochraně autorského práva a práv souvisejících. Obecným právním základem autorského práva je čl. 34 LZPS, který uvádí: *„Práva k výsledkům tvůrčí duševní činnosti jsou chráněna zákonem.“*[148]

Pokud jde o pojem „autorské dílo“, zahrnujeme sem také počítačový program a to na základě ustanovení § 2 odst. 2 AutZ. Ustanovení požaduje pouze jediné kritérium. Program musí být původní a to v tom smyslu, že je autorovým vlastním duševním výtvorem. Tento požadavek splňuje většina počítačových programů.[149] Z hlediska ochrany řadí autorský zákon počítačový program pod díla literární dle ustanovení § 65 odst. 1 AutZ.

9.8.1 Nikoliv nepatrný zásah do zákonem chráněných práv

Při hodnocení „nikoliv nepatrného“ zásahu je třeba zkoumat hlavně okolnosti daného případu a to zejména intenzitu takového zásahu, způsob provedení činu, jeho následky a závažnost, s jakou byla zasažena osobní a majetková práva autorů. V některých případech postačí, bude-li skutek hodnocen jako přestupek nebo jiný správní delikt, jindy bude třeba přistoupit k tvrdšímu postihu pachatele. Za nepatrný zásah budeme považovat např. situaci, kdy dojde k prodeji jednoho CD disku kamarádovi. O opačný případ se bude jednat, prodá-li někdo CD prostřednictvím inzerce, jedná-li se o činnost dlouhodobějšího charakteru nebo dopustí-li se pachatel daného jednání opakovaně.[150]

Z hlediska subjektivní stránky si pachatel musí být alespoň v hrubých rysech vědom skutečnosti, že nakládá s dílem, které je chráněno autorským právem. Nemusí tedy znát detailní rozsah oprávnění autora, postačí hrubé povědomí o těchto právech.[151]

Trestný čin dle ustanovení § 270 TrZ může být v jednočinném souběhu zejména s činem neoprávněného podnikání dle § 251 TrZ, porušení předpisů o oběhu zboží ve styku s cizinou dle § 261 TrZ a trestným činem porušení předpisů o pravidlech hospodářské soutěže dle § 248 odst. 1 TrZ.

9.8.2 Jednání s charakterem obchodní činnosti nebo jiného podnikání

Přísněji bude potrestán pachatel, jehož jednání bude mít charakter obchodní činnosti nebo jiného podnikání. Za jednání mající znaky obchodní činnosti nebo jiného podnikání lze považovat např. výrobu, rozmnožování nebo skladování zboží za účelem jeho prodeje.

---

[148] Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů
[149] ŠÁMAL: *Trestní zákoník...*, s. 2496
[150] Tamtéž, s. 2512
[151] Tamtéž, s. 2513

Nepostačí činnost pachatele „při podnikání“ nebo „v souvislosti s podnikáním“. V takovém případě by k přísnějšímu trestnímu postihu postačil jednorázový zásah např. v podobě protiprávního využití počítačového programu při zpracování daňového přiznání podnikatele.[152]

9.8.3 Spáchání činu ve značném rozsahu

Přísněji bude potrestán také pachatel, který činem pro sebe nebo pro jiného získá značný prospěch nebo který způsobí jinému značnou škodu. Dále, kdo se takového činu dopustí ve značném rozsahu.[153] Výkladové pravidlo pro stanovení výše škody uvedené v ustanovení § 138 odst. 1 TrZ nelze pro výklad tohoto spojení použít. Je nutné přihlédnout ke všem okolnostem případu. Rozhodující bude závažnost a intenzita zásahu do zákonem chráněného práva. Důležitým vodítkem je také délka porušování konkrétního práva popřípadě opakování zásahů.[154]

Nejpřísněji bude potrestán pachatel, který svým jednáním získá pro sebe nebo pro jiného prospěch velkého rozsahu.

9.8.4 Statistika Ministerstva spravedlnosti ČR k ustanovení § 270 TrZ.

Oficiální statistiky Ministerstva spravedlnosti ČR ve výroční zprávě o kriminalitě za rok 2009 hovoří o trestném činu uvedeném v ustanovení § 152 starého TrZ, tedy porušování autorského práva, práv souvisejících s právem autorským a práv k databázi. I přesto, že se jedná o již neúčinnou právní úpravu, je vhodné uvést několik faktů.

Za rok 2009 bylo celkem projednáváno 261 trestných činů, stíháno 220 osob, z toho 166 bylo obžalováno a 110 osob nakonec odsouzeno. Zajímavým faktem je, že soud neuložil žádný nepodmíněný trest odnětí svobody, v naprosté většině se jedná o tresty podmíněné.[155]

Je obtížné určit skutečný stav tohoto druhu kriminality a to vzhledem k vysoké míře latence v této oblasti. Mnoho trestných činů zůstane neodhaleno.

---

[152] Důvodová zpráva k zákonu č. 40/2009 Sb., trestní zákoník.
[153] JELÍNEK: *Trestní právo…*, s. 670
[154] ŠÁMAL: *Trestní zákoník…*, s. 2514
[155] Odbor dohledu ministerstva spravedlnosti ČR. *Statistická ročenka kriminality: rok 2009.* [online]. portal.justice.cz, 2009 [cit. 22. prosince 2010]. Dostupné na <http://portal.justice.cz/Justice2/soubor.aspx?id=85103>

10 Škodlivý software

10.1 Počítačové viry

Jedná se o počítačové programy, které se dokáží šířit samy bez vědomí uživatele. Podstatou viru je jeho reprodukce. K množení viru dochází napadáním dalších souborů a dokumentů. Dříve byl termín vir spojen hlavně se souborem končícím příponou „.exe“. Od roku 1996 je tento škodlivý software možné nalézt také v textovém souboru, jedná se o tzv. „macro viry“.[156]

Aspektem, který vyšetřovatelům počítačových deliktů činí největší problémy, je zjištění původce virového programu. Specifikem viru je skutečnost, že se aktivuje s určitým zpožděním, tedy např. v okamžiku, kdy si dotyčný uživatel nainstaluje příslušný software. V tu dobu bývá nalezení pachatele mnohdy nemožné.

Za obecně nebezpečnější typy virů jsou považovány ty, které působí pomalu, po dlouhou dobu, přičemž vykonávají svou destruktivní činnost. Vážné následky může počítačový vir způsobit i na samotném hardwaru počítače, dojít tak může i k „vypálení“ monitoru.[157]

10.2 Počítačoví červi

Na rozdíl od počítačového viru, červ se dokáže šířit automaticky. Sám rozesílá svou kopii na další počítače v síti. Může mít i další cíle, přičemž reprodukce bude jen jedním z nich.[158] Obecně se tito červi mohou šířit např. elektronickou poštou. Existují však i jiné způsoby. V USA, ve státě Louisiane se odehrál případ, při němž zákazníkům služby WebTV neznámý hacker zaslal počítačového červa. Tato služba nabízela internetové připojení skrze televizní spojení. Zákazníci v domnění, že email obsahuje pouze neškodný program pokoušející se změnit zobrazení nebo přednastavení barev, tuto aplikaci spustili. Počítačový červ však přednastavil číslo k internetovému připojení na 911, tedy na linku nouzového volání. Pachatel tak způsobil velké množství planých poplachů v několika státech USA.[159]

---

[156] ŠÁMAL: *Trestní zákoník...*, s. 2090
[157] ENDORF, Carl. SCHULTZ, Eugene. MELLANDER, Jim. *Detekce a prevence počítačového útoku*. 1. vydání. Praha: Grada, 2005. s. 109
[158] ŠÁMAL: *Trestní zákoník...*, s. 2091
[159] HARRIS, Shon. Hacking : manuál hackera. 1. vydání. Praha: Grada. 2008. s. 47

10.3 Trojský kůň

Trojský kůň na rozdíl od výše uvedeného softwaru nedokáže kopírovat sám sebe. Jedná se o skrytou část programu, která funguje jinak, než očekává uživatel, a to skrytě. Trojský kůň může být součástí volně stažitelného softwaru, přičemž mnohdy se jedná pouze o malý program. Vhodným příkladem je trojský kůň „Whack-a-mole". Jedná se o počítačovou hru obsahující program na odstranění škodlivého programu BackOrifice. Ve skutečnosti však instaluje tuto aplikaci do počítače nic netušícího uživatele.[160]

Funkce trojského koně může spočívat také ve vytvoření tzv. spam-serveru. V tomto případě se z napadeného počítače stane zdroj rozesílání nevyžádané pošty, tedy spamu.[161]

10.4 Backdoors

Jedná se o kód, který po své instalaci umožňuje vzdálené řízení počítače. Jde o typický nástroj hackera, který takto využívá a vzdáleně řídí hned několik počítačů, skrze které může anonymně útočit na další počítačové stroje. Moderní backdoors programy ke své činnosti používají oblíbené komunikační nástroje jako jsou ICQ nebo MSN messenger.[162]

Jedním z nejznámějších backdoors programů je „Back orifice", který útočníkovi umožní přístup k počítači, který byl tímto škodlivým softwarem infikován. Zvláštností tohoto programu je možnost téměř absolutní kontroly nad počítačem uživatele. Jedná se o možnost restartovat počítačový systém, mazat soubory, prohlížet přístupová hesla uživatele aj. Samotný program může být nenápadně nainstalován prostřednictvím otevření přílohy emailu. Následujícím krokem je nastavení spouštění daného programu po každém startu počítače a rozšíření položek registrů.[163]

10.5 Spyware

Podstatou spywaru je sběr a přenos informací. Jedná se o škodlivý software, který shromažďuje informace o chování internetového uživatele. Riziko spočívá v tom, že se může jednat o data velmi osobní jako jsou emailové adresy, přístupová hesla, ale i čísla kreditních

[160] JIROVSKÝ: *Kybernetická kriminalita*, s. 67
[161] ŠÁMAL: *Trestní zákoník...*, s. 2091
[162] JIROVSKÝ: *Kybernetická Kriminalita*, s. 63
[163] Tamtéž, s. 64

karet. Stejně jako v případě virů, tak i u spywaru je vhodné chránit počítač vhodným a aktualizovaným softwarem.[164]

10.6 Malware

Malware je pojem, který shrnuje různé internetové škůdce. Vychází z anglického „malicious software", tedy škodlivý software. Riziko nakažení systému tímto škodlivým softwarem (tedy virem, červem, trojským koněm atp.) je vyšší v případě, nemáme-li počítač zabezpečen nejnovějšími verzemi bezpečnostního softwaru.[165]

10.7 Právní kvalifikace dle ustanovení § 230 TrZ.

V případě Malwaru lze protiprávní jednání kvalifikovat dle ustanovení § 230, 232 popřípadě 228 TrZ.

Příslušné jednání může spočívat v tzv. zásahu do dat, tedy získání přístupu k počítačovému systému nebo nosiči informací a neoprávněném vymazání nebo jiném zničení (také poškození, změně, potlačení nebo snížení jejich kvality, v učinění neupotřebitelným) dat uložených v počítačovém systému nebo na nosiči informací dle ustanovení § 230 odst. 2 pís. b TrZ. Dále se může jednat o vložení dat do počítačového systému nebo zásah do programového vybavení počítače dle ustanovení § 230 odst. 2 pís. d TrZ. Tímto jednáním hrozí pachateli trest odnětí svobody až na dvě léta, zákaz činnosti, propadnutí věci nebo jiné majetkové hodnoty.[166]

V úvahu připadá také kvalifikace jednání dle ustanovení § 232 TrZ, požadující splnění podmínky hrubé nedbalosti a porušení povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté.

Možné je také naplnění skutkové podstaty trestného činu poškození cizí věci dle ustanovení § 228 TrZ.

---

[164] JIROVSKÝ: *Kybernetická Kriminalita*, s. 183
[165] ENDORF: *Detekce a prevence...*, s. 182
[166] ŠÁMAL: *Trestní zákoník...*, s. 2091

11 Prevence počítačové kriminality a softwarového pirátství

11.1 prevence počítačové kriminality

Vysokým nákladům na vyšetřování i samotnému deliktu lze účinně předejít správnou prevencí. Obecně je nutné:[167]

1. přijmout taková opatření, která omezí možnosti pachatele zaútočit na počítačový systém
2. testování přijatých opatření a technologií
3. detekce průniku a vyšetření průniku, včetně shromaždování důkazů a odstraňování vzniklých škod

Průniku do počítačového systému je třeba účinně zabránit, jeho vyšetření je až posledním krokem. Předně je nutné chránit počítačový systém a stanovit vhodnou zabezpečovací politiku. Jejím významným prvkem je užití nejnovějšího softwarového vybavení a nástrojů. Pomoci mohou také pravidelné preventivní kontroly. Jedním z druhů preventivní činnosti je simulace různých typů útoků. Tímto lze upozornit na slabá místa v systému a věnovat se poté přímo jim. Na tato slabá místa se poté lze zaměřit a nasměrovat tak příslušný bezpečnostní software. Ten je většinou spuštěn v pozadí systému, zjišťuje aktuální útoky a snaží se jim zabránit. Důležitou funkcí takového softwaru je také zaznamenání veškerých úkonů v počítačovém systému. Zaznamenání úkonů je důležité z hlediska nutnosti shromáždit všechny důležité důkazy, zjistit posloupnost, množství a intenzitu vedených útoků.

Funkce vedených záznamů je dvojí:[168]

1. Statistická (v důsledku zjištěných skutečností může dojít ke změně primární bezpečnostní politiky)
2. Podklad pro vyšetřování (v případě, dojde-li již k průniku do systému)

V oblasti počítačové kriminality se pravděpodobně ještě více než v jiných oblastech uplatní prevence před represí. *„V obecné rovině musí prevence počítačové kriminality především působit výchovně, ovlivňovat vztahy mezi lidmi a touto technikou, napomáhat*

[167] JIROVSKÝ: *Kybernetická kriminalita...*, s. 253
[168] Tamtéž, s. 253-254

formování počítačové kultury a kulturnosti..."[169]

Důležitým faktorem ovlivňujícím celou oblast počítačové kriminality je nedostatečná gramotnost, znalost možných i nemožných důsledků. Sdílet škodlivý software, popřípadě „nasadit" kolegovi v práci do počítačového systému trojského koně, nevyvolá jistě takový pocit viny, jako při situaci, kdy se někdo dopustí trestného činu krádeže v obchodním domě nebo překročí maximální povolenou rychlost na veřejné komunikaci. Význam zde má informování těch, kteří s výpočetní technikou přichází do styku. Jelikož k počítačovým útokům dochází často latentně a odhalení je mnohdy skoro nemožné, musí se na prevenci klást velký důraz. Již od útlého věku bychom měli mít jasnou představu o tom, k jakým důsledkům může běžným užíváním počítače dojít, jaká může být výše škod a jaké jsou alespoň přibližné trestněprávní důsledky.

Často spoléháme na technické prostředky, které mají zabránit útokům a ochránit nás před různými typy crackerů, hackerů atp. Avšak jako v jiných oblastech trestního práva i zde platí, že se jedná o určitý technologický souboj mezi potenciálními pachateli, „útočníky" a kriminalisty. Preventivní opatření budou účinná jen tehdy, bude-li mít trestní právo a vyšetřovatelé před pachateli „náskok". Tyto normy nemusejí vždy aktuálně pokrýt veškeré potenciální hrozby počítačové kriminality. Může se tedy jednat sice o jednání společensky nebezpečné, nikoliv však v trestním zákoně popsané.

11.1.1 Opatření v rámci prevence počítačové kriminality

V rámci prevence je vhodné zejména:[170]

1. Prověřování osob, které mají přístup k počítačům, programům a datům (např. zavedení nějakého přihlašovacího, evidenčního systému)
2. Vhodně rozdělit pravomoc subjektů, které mají určité oprávnění v systému (jde vlastně o to, aby „zaměstnanec" neměl více oprávnění než musí, přidělen by mu měl být přístup k té části systému a k těm souborům, které ke své práci nezbytně potřebuje)
3. Jasné rozvrstvení povinností pracovníků (např. stanovit vnitřními předpisy organizace)
4. Pravidelné interní a externí kontroly (zde je vhodné využít momentu překvapení)

[169] VLČEK, Martin. *Počítače a kriminalita : (Trestněprávní a kriminologické aspekty)*. 1. vydání. Praha, 1989. s. 52

[170] Tamtéž, s. 54-55

5. Ochrana technického charakteru (např. zajištění dostatečného záložního prostoru, sekundárního zdroje energie v případě, selže-li primární, ochrana proti požárům apod.)

Všechny druhy prevence by se měly prolínat, měly by být uplatňovány společně a hlavně by s nimi měli být obeznámeni všichni ti, kterých se přímo dotýkají. Společně se zdokonalováním informačních technologií se také rozšiřují možnosti pachatelů, kteří mohou mít určitý „technologický náskok" před vyšetřovateli. [171]

11.1.2 Psychologická prevence

Do této oblasti bychom zařadili povědomí občanů o tom, jaká jednání související s počítačovou kriminalitou jsou společensky nepřijatelná. Jedná se o jakousi osvětu realizovanou zejména různými kampaněmi skrze BSA nebo ministerstva.

11.1.3 Technická prevence[172]

Z technického hlediska se jedná o typicky „nekonečný" souboj mezi crackery, hackery a orgány činnými v trestním řízení, dále boj mezi tvůrci ochran, antivirových, firewallových programů a těmi, kteří se takovou ochranu snaží prolomit.

Snaha filmových společností o ochranu médií, na kterých si film lze přehrát, je patrná, avšak zatím neúspěšná. Situace se měla rapidně změnit s příchodem Blu-ray disků, které obsahovaly silnou ochranu zvanou BD+. Avšak i tuto se podařilo prolomit, blu-ray disk celý zálohovat do počítače a dále s ním pracovat. Podařilo se to společnosti Slysoft.[173]

Dle Daniela Dočekala je vhodné klást důraz zejména na vzdělání. Jak se bezpečně chovat v prostředí Internetu, by mělo být žákům vysvětlováno již na základních školách. Současné tendence Evropské unie vedou spíše k politice zakazování, což je do budoucna zapotřebí změnit. Právě internetoví uživatelé a jejich gramotnost, tedy tzv. lidský faktor, je hlavní příčinou průniků do zabezpečení systému počítače.

Problémem je také fakt, že údaje, které orgány činné v trestním řízení potřebují

---

[171] VLČEK: *Počítače a kriminalita...*, s. 57
[172] MATĚJKA: *Počítačová kriminalita...*, s. 78-80
[173] RUTZENSTORFER, Petr. *Poslední bariéra ochrany Blu-ray disků prolomena* [online]. 11. listopadu 2007 [cit. 28. prosince 2010]. Dostupné na <http://blu-ray.cz/2007/11/posledni-bariera-ochrany-blu-ray-disku-prolomena/>

k vyšetřování, jsou většinou předmětem telekomunikačního tajemství nebo se na ně vztahuje ochrana osobních a zprostředkovacích dat.[174]

11.2 Prevence softwarového pirátství

Mnozí uživatelé se stávají softwarovými piráty nevědomě, neuvědomují si hrozbu možné represe nebo se nechají unést „masovostí" počítačového pirátství. Problémem je také lehká a rychlá dostupnost softwaru skrze Internet. Postačí, objeví-li se jeden profesionální, programování a crackování znalý uživatel. Na něm je poté ta nejtěžší práce s prolamováním ochrany příslušného softwaru. Do těchto ochran investují softwarové firmy mnohdy nemalé finanční prostředky.[175] V případě, že se prolomení ochrany podaří, následuje fáze zprostředkování. Počítačový pirát se chce se svým úspěchem pochlubit na veřejnosti. Může to být pouze pocit uspokojení z „dobře odvedené práce" a pocit respektu ve světě počítačů. Ke „zcizování duševního vlastnictví" pak dochází přímo z domova pachatele.

Jedním z hlavních důvodů, proč se lidé obrací ke koupi originálního softwaru zády, je jeho výsledná cena. Ta se zdá být stále příliš vysoká. Velké společnosti jako Microsoft se snaží vycházet uživatelům vstříc a poskytují na českém trhu lokalizované verze svých produktů. To je sice uživatelsky přívětivější, stále to však nezabrání nelegálnímu šíření jejich produktů na trhu.

11.2.1 Hlavní příčiny softwarového pirátství

K hlavním příčinám softwarového pirátství můžeme řadit:[176]

1. Příliš vysokou cenu produktů (často v řádech desítek tisíc korun)
2. Potřeba zhodnotit software, touha vyzkoušet si zda-li splní má očekávání (poté si mnoho uživatelů uvědomí hodnotu a kvalitu daného produktu a samy si ho po tomto „nelegálním vyzkoušení" zakoupí)
3. Potřeba aktualizace starých verzí softwaru
4. Jistá forma zábavy a soutěže pro „crackery"

[174] KRUTINA, Miroslav. MÚKA, Ondřej. *Poskytnutí údajů o telekomunikačním provozu a domovní prohlídka* [online]. lupa.cz, 1. února 2007 [cit. 28. prosince 2010]. Dostupné na <http://www.lupa.cz/clanky/poskytnuti-udaju-o-telekomunikacnim-provozu-a-domovni-prohlidka/>
[175] CRAIG: *Softwarové pirátství…*, s. 164
[176] Tamtéž, s. 165-169

5. Nedůvěra v kompatibilitu zakoupeného produktu. Zde je vhodné upozorňovat přímo na webových stránkách výrobce na problémy s kompatibilitou příslušného systému a jeho další úskalí

Z technického pohledu lze hovořit o několika typech ochran softwarových produktů. Jsou to např. černé listiny, které obsahují heslo nebo sériové číslo, umožní spuštění a používání příslušného softwarového produktu a které již byly rozšířeny mezi uživateli na Internetu.[177] Dalším často používaným druhem ochrany je tzv. „online ověřování". V případě, je-li příslušná aplikace spuštěna, připojí se k domácímu serveru výrobce. Ten má tak možnost ověřit, zda-li je produkt zakoupen legálně, a vyřadit ho z provozu resp. omezit jeho použitelnost. Tento způsob ochrany je však lehké obejít prostřednictvím firewallu a blokací přístupu k domácímu serveru.[178]

Prevenci také nepřispívá malé zapojení občanů s prácí policie ČR a orgánů činných v trestním řízení obecně. Tzv. malá „kriminální citlivost" vůči trestným činům souvisejících s duševním vlastnictvím je způsobena pravděpodobně všeobecným povědomím o příliš vysokých cenách softwarových produktů. Při prevenci před páchaním této trestné činnosti se však může uplatnit činnost různých ochranných organizací autorů a softwarových firem.[179]

11.2.2 Účastníci prevence softwarového pirátství

Preventivní činnosti se účastní:[180]

1. Státní orgány – Česká obchodní inspekce, celní úřady, Policie ČR a další.
2. Nestátní subjekty – Ochranný svaz autorský pro práva k hudebním dílům, Nezávislá společnost výkonných umělců a výrobců zvukových a zvukově obrazových záznamů INTEGRAM, Česká protipirátská unie aj.
3. Policie ČR – např. prostřednictvím různých veletrhů a výstav (INVEX a další)

11.2.3 Systém „třikrát a dost"

Specifickým způsobem se porušování autorského práva snažila řešit francouzská vláda. Ta chtěla uplatnit systém „třikrát a dost", tedy v případě prvního porušení autorských práv (např. sdílením nelegálního softwaru) by došlo pouze k napomenutí, stejně tak v druhém

[177] CRAIG: *Softwarové pirátství…*, s. 196
[178] Tamtéž, s. 203
[179] MUSIL: *Kriminalistika*, s. 251
[180] Tamtéž, s. 251

případě. Při třetím provinění by byl uživatel odpojen od sítě Internet a to až na dobu jednoho roku. Francouzský zákon měl být zřízen úřadem HADOPI,[181] tedy Vysokým úřadem pro šíření děl a ochrany práv na Internetu. Jednalo se o administrativní orgán, který měl disponovat pravomocí odpojovat uživatele od sítě. To ovšem dle francouzského ústavního soudu kolidovalo se zásadou presumpce neviny uvedenou např. v Deklaraci práv člověka a občana. Dále se zásadou, že o vině a trestu může rozhodovat pouze soud, stejně tak ukládat tresty. Později bylo rozhodování o odpojení ze sítě svěřeno do rukou řádného soudce a problematika upravena speciálním zrychleným řízením.[182]

Možností odpojit od sítě Internetu se zabývala také samotná Evropská unie, jednalo se o stejný systém, tedy „třikrát a dost". Unie zpočátku narážela na skutečnost, že připojení k Internetu je součást základního práva na informace. Podmínkou přípustnosti takového systému je nutnost respektování základních práv a svobod fyzických osob a základních principů unijního práva. Je nutné respektovat nejen zásadu presumpce neviny, ale zachován musí být také princip účelnosti, přiměřenosti a nezbytnosti, bez kterých by řádná demokratická společnost nemohla existovat.[183]

11.3 Represe

V rámci represivní činnosti působí především orgány činné v trestním řízení, tedy Policie ČR, soudy, státní zástupce. Problémem zůstává nízká míra oznamování trestné činnosti ze strany společnosti. Může se jednat o ztrátu prestiže nebo pověsti orgánů. Dalším problémovým faktorem je nedostatečné vybavení struktur Policie ČR působících na poli počítačové kriminality, nutnost vysoké kvalifikace vyšetřovatelů a chyby při manipulaci s důkazním materiálem – typicky vypnutí počítače, kdy dojde ke ztrátě nejdůležitějších dat, které by v pozdějších fázích řízení mohly sloužit jako usvědčující důkaz pachatele.[184]

[181] Haute autorité pour la diffusion des èuvres et la protection des droits sur Internet
[182] HERCZEG, Jiří. GŘIVNA, Tomáš. Právo na přístup k Internetu, blokace stránek a digitální gilotina. *Trestněprávní revue*, 2010, č. 5, s. 4-5
[183] Tamtéž, s. 7-8
[184] MATĚJKA: *Počítačová kriminalita…*, s. 81

Závěr a budoucí vývoj počítačové kriminality

Vývoj kriminality bude v budoucnu ovlivňovat mnoho faktorů, přičemž mezi ty nejdůležitější patří:[185]

1. terorismus
2. organizovaný zločin
3. ekonomická kriminalita
4. zvyšování rozdílu mezi vyspělými a zaostalými zeměmi
5. institucionální a osobní vazby na země střední a východní Evropy
6. aktivity mezinárodních společenství: OSN, Rada Evropy, Evropská unie, NATO

Orgány Evropské unie a další subjekty zabývající se bojem proti počítačové kriminalitě si uvědomují, že nelze upřednostnit žádnou efektivní represi před funkční prevencí. Tento názor vyslovila např. Komise Evropského Parlamentu ve svém Sdělení Komise Evropského Parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů k obecné politice v boji proti počítačové kriminalitě ze dne 22. 5. 2007 (KOM (2007) 267). Je nutné vytvořit obecnou politiku boje proti počítačové kriminalitě a soustředit snahu na harmonizaci jednotlivých národních právních úprav. Zvyšující se počet trestných činů, větší důmyslnost pachatelů, nízká odborná příprava a technická vybavenost orgánů činných v trestním řízení a vyšetřovatelů jsou obecným a stále trvajícím problémem. Nutné je také zvýšit všeobecné povědomí o hrozbách spojených s počítačovou kriminalitou a zefektivnit právní a institucionální rámec nejen v rámci Evropské unie.[186]

V budoucnu se budeme pravděpodobně potýkat s problémem, jak zapracovat rychlý vývoj nových inovativních technologií do stávajících právních norem. Problémem také zůstává boj obchodníků/prodejců/umělců s uživateli, kteří nelegálně stahují a sdílejí hudební soubory ve vysoké kvalitě na sítích jako je peer-to-peer. Stejně tak je neutěšená situace ohledně crackerů, hackerů a dalších pachatelů, jejichž odhalení je velmi náročné a to nejen po stránce finanční, ale také personální a odborné.

Je vysoce pravděpodobné, že s příchodem nových, dosud neznámých, technologií dojde k vytvoření prostoru pro nová potenciálně nebezpečná jednání z oblasti počítačové

[185] CEJP, Martin. Pokusy o předvídání možného vývoje kriminality. *Trestněprávní revue*, 2010, č. 4, s. 111
[186] GŘIVNA, Tomáš. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. In HORYNA, Mojmír (ed). *Český právní řád a ochrana kyberprostoru: (vybrané problémy)*. Praha: Karolinum, 2008, s. 31-33

kriminality. Také z tohoto důvodu je vhodné pokračovat v procesu harmonizace nejen na poli Evropské unie, ale i Rady Evropy a dalších organizací.

LITERATURA

Právní předpisy:

Důvodová zpráva k zákonu č. 40/2009 Sb., trestní zákoník.

Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů

aktuální znění: zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

aktuální znění: zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů

aktuální znění: zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů

aktuální znění: zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů

Zákon č. 140/1961 Sb., trestní zákon, ve znění zákona č. 52/2009 Sb. účinného ke dni 1. 4. 2009

Vyhláška ministra zahraničních věcí č. 69/1975 Sb. O Úmluvě o zřízení Světové organizace duševního vlastnictví podepsané ve Stockholmu dne 14. července 1967, ve znění vyhlášky č. 80/1985 Sb.

Publikace:

CRAIG, Paul. HONICK, Ron. *Softwarové pirátství bez záhad*. 1. vydání. Praha: Grada. 2008. 212 s.

ENDORF, Carl. SCHULTZ, Eugene. MELLANDER, Jim. *Detekce a prevence počítačového útoku*. 1. vydání. Praha: Grada, 2005. 355 s.

GŘIVNA, Tomáš. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. In HORYNA, Mojmír (ed). Český právní řád a ochrana kyberprostoru: (vybrané problémy). Praha: Karolinum, 2008, 140 s.

HARRIS, Shon. *Hacking : manuál hackera*. 1. vydání. Praha: Grada. 2008. 399 s

HENDRYCH, Dušan a kol. *Právnický slovník*. 3. vydání. Praha: C.H.BECK, 2009. 1488 s.

JELÍNEK, Jiří a kol. *Trestní právo hmotné*. 1. vydání. Praha: Leges, 2009. 896 s.

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vydání. Praha: Grada Publishing, spol. s.r.o., 2007. 284 s.

MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha: Computer Press, 2002. 106 s.

MINÁRIK, Tomáš. Peer-to-peer sítě z hlediska trestního práva. In HORYNA, Mojmír (ed). *Český právní řád a ochrana kyberprostoru: (vybrané problémy).* Praha: Karolinum, 2008, 140 s.

MUSIL, Jan. KONRÁD, Zdeněk. SUCHÁNEK, Jaroslav. *Kriminalistika*. 2. vydání. Praha: C.H. Beck. 2004. 583 s.

NOVÁK, Karel. *Počítačová kriminalita.* Praha: Institut pro kriminologii a sociální prevenci, 1992.

POLČÁK, Radim. *Právo na internetu: Spam a odpovědnost ISP*. 1. vydání. Brno: Computer Press, 2007. 150 s.

POLČÁK, Radim. *Právo a evropská informační společnost*. 1. vydání. Brno: Masarykova univerzita, 2009. 202 s.

POLČÁK, Radim. ŠKOP, Martin. MACEK, Jakub. *Normativní systémy v kyberprostoru (úvod do studia).* 1. vydání. Brno: Masarykova univerzita, 2005. 102 s.

PORADA, Viktor a kol. *Kriminalistická metodika vyšetřování.* 1. vydání. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk. 2007. 231 s.

PORADA, Viktor. KONRÁD, Zdeněk. *Metodika vyšetřování softwarového pirátství.* 1. vydání. Praha: Policejní akademie České republiky. 1999. 54 s.

PORADA, Viktor. *Metody vyšetřování počítačové kriminality*. 1. vydání. Praha: Policejní akademie České republiky. 1998. 54 s.

POŽÁR, Josef. Odhalování a vyšetřování kybernetické kriminality. In JIROVSKÝ, Václav (ed). *Sborník přednášek konference CYTER 2009*. Praha : České vysoké učení technické v Praze, Fakulta dopravní, Ústav informatiky a telekomunikací. 2009. 90 s.

PROISE, Chris. MANDIA, Kevin. *Počítačový útok : detekce, obrana a okamžitá náprava*. 1. vydání. Praha : Computer Press. 2002. 410 s.

SELINŠEK, Liljana. Některé právní aspekty forenzní analýzy digitálních dat. In HORYNA, Mojmír (ed). Český právní řád a ochrana kyberprostoru: (vybrané problémy). Praha: Karolinum, 2008, 140 s.

SMEJKAL, Vladimír. *Internet a §§§*. 2. vydání. Praha: Grada Publishing, spol. s.r.o., 2001. 284 s.

SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů*. 2. vydání. Praha: C.H.Beck, 2004. 770 s.

ŠÁMAL, Pavel a kol. *Trestní zákoník. Edice velké komentáře*. 1. vydání. Praha: C.H.Beck, 2009. 3285 s.

VLČEK, Martin. *Počítače a kriminalita : (Trestněprávní a kriminologické aspekty)*. 1. vydání. Praha, 1989. 96 s.

Časopisy:

CEJP, Martin. Pokusy o předvídání možného vývoje kriminality. *Trestněprávní revue*, 2010, roč.X, č. 4, 111 s.

HERCZEG, Jiří. GŘIVNA, Tomáš. Právo na přístup k Internetu, blokace stránek a digitální gilotina. *Trestněprávní revue*, 2010, č. 5, 141 s.

KUCHTA, Josef. Úprava majetkových trestných činů v novém trestním zákoníku. *Právní rozhledy*, 2010, č. 1, s. 11

LÁTAL, Ivo. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista*, 1998, č. 3, příloha
Dostupné na <http://aplikace.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html>

SMEJKAL, Vladimír. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. *Trestněprávní revue*, 2003, č. 6, s. 161.

SMEJKAL, Vladimír. Počítačová a internetová kriminalita v České republice. *Právní rozhledy*, 1999, č. 12, příloha, s. 2

Elektronické zdroje:

Council of Europe. Convention on Cybercrime. [online]. http://conventions.coe.int, 23. září 2001 [cit. 20. ledna 2011]. Dostupné na <http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>

CZ.NIC, z.s.p.o. CZ.NIC od začátku roku zablokoval 150 škodlivých domén [online]. nic.cz, 25. února 2010 [cit. 5.ledna 2011]. Dostupné na <http://www.nic.cz/page/733/cz.nic-od-zacatku-roku-zablokoval-150-skodlivych-domen/>

DOČEKAL, Daniel. *CSIRT.cz přichází. Kyberzločincům navzdory* [online]. lupa.cz, 4. dubna 2008 [cit. 5. ledna 2011]. Dostupné na <http://www.lupa.cz/clanky/csirt-cz-prichazi-kyberzlocincum-navzdory/>

HLAVÁČ, Jan. *SOFTWAROVÉ PIRÁTSTVÍ KLESLO: V ČESKU SE UŽÍVÁ 38 % SOFTWARU NELEGÁLNĚ* [online]. portal.bsa.org, 12. května 2009 [cit. 20. prosince 2010]. Dostupné na <http://portal.bsa.org/globalpiracy2008/pr/pr_czechrep.pdf>

HLAVÁČ, Jan. *SNÍŽENÍ MÍRY SOFTWAROVÉHO PIRÁTSTVÍ PŘINESE ČESKU MILIARDY KORUN, STUDIE POUKAZUJE NA EKONOMICKÉ PŘÍNOSY SNÍŽENÍ MÍRY SOFTWAROVÉHO PIRÁTSTVÍ* [online]. portal.bsa.org, 15. září 2010 [cit. 21. prosince 2010]. Dostupné na <http://portal.bsa.org/piracyimpact2010/pr/pr_czechrepublic_czech.pdf>

KLIMÁNEK, Oldřich. *Spolupráce BSA a Ministerstva financí: „Hardware bez softwaru není uznatelný daňový náklad" aneb Bezplatný software je automaticky pirátský?* [online]. dsl.cz, 28. května 2010 [cit. 22. prosince 2010]. Dostupné na <http://www.dsl.cz/clanek/1795-spoluprace-bsa-a-ministerstva-financi-8222-hardware-bez-softwaru-neni-uznatelny-da-ovy-naklad-8220-aneb-bezplatny-software-je-automaticky-piratsky>

KRČMÁŘ, Petr. *Jaké aktuální hrozby číhají na uživatele internetu?* [online]. root.cz, 27. února 2009 [cit. 4 ledna 2011]. Dostupné na <http://www.root.cz/clanky/jake-aktualni-hrozby-cihaji-na-uzivatele-internetu/>

KRULÍK, Oldřich. HNÍK, Václav. *Zahraniční inspirace související s tématem kybernetických hrozeb*. [online]. mvcr.cz, srpen 2006 [cit. 16. prosince 2010]. Dostupné na <http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/zahranicni_inspirace.pdf>

KRUTINA, Miroslav. MÚKA, Ondřej. *Odnětí a vydání věci doličné při podezření z porušení autorského práva* [online]. lupa.cz, 2. února 2007 [cit. 26. prosince 2010]. Dostupné na <http://www.lupa.cz/clanky/odneti-a-vydani-veci-dolicne-pri-podezreni-z-poruseni-autorskeho-prava/>

KRUTINA, Miroslav. MÚKA, Ondřej. *Poskytnutí údajů o telekomunikačním provozu a domovní prohlídka* [online]. lupa.cz, 1. února 2007 [cit. 28. prosince 2010]. Dostupné na <http://www.lupa.cz/clanky/poskytnuti-udaju-o-telekomunikacnim-provozu-a-domovni-prohlidka/>

RUTZENSTORFER, Petr. Poslední bariéra ochrany Blu-ray disků prolomena [online]. 11. listopadu 2007 [cit. 28. prosince 2010]. Dostupné na <http://blu-ray.cz/2007/11/posledni-bariera-ochrany-blu-ray-disku-prolomena/>

POŠVIC, Kamil. *Počet uživatelů internetu v roce 2010 překročil 2 miliardy*. [online]. root.cz, 1.února 2011 [cit. 3. února 2011]. Dostupné na <http://www.root.cz/zpravicky/pocet-uzivatelu-internetu-v-roce-2010-prekrocil-2-miliardy/>

POTŮČEK, Jan. *Karel Kuchařík: dostaneme se i do uzavřených sítí* [online]. lupa.cz, 13.února 2007 [cit. 23. prosince 2010]. Dostupné na <http://www.lupa.cz/clanky/karel-kucharik-dostaneme-se-i-do-uzavrenych-siti/>

Odbor dohledu Ministerstva spravedlnosti ČR. *Statistická ročenka kriminality: rok 2009*. [online]. portal.justice.cz, 2009 [cit. 22. prosince 2010]. Dostupné na <http://portal.justice.cz/Justice2/soubor.aspx?id=85103>

SOKOL, Tomáš. SMEJKAL, Vladimír. *Postih počítačové kriminality podle nového trestního zákona.* [online]. pravniradce.ihned.cz, 22. července 2009 [cit. 25. prosince 2010]. Dostupné

na <http://pravniradce.ihned.cz/c4-10077480-37865090-F00000_d-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>

Tisková zpráva. *Pracovní skupina CSIRT.CZ o vládním bezpečnostním pracovišti CSIRT* [online]. cesnet.cz, 30. března 2010 [cit. 6. ledna 2011]. Dostupné na <http://www.cesnet.cz/doc/tisk/2010/tz100330.html>

VYLEŤAL, Martin. *Online hry hýbou Internetem, psychikou a peněženkami hráčů.* [online]. lupa.cz, 12.srpna 2005 [cit. 20. listopadu 2010]. Dostupné na <http://www.lupa.cz/clanky/online-hry-hybou-internetem-psychikou-a-penezenkami-hracu/>

Soudní rozhodnutí:

Rozsudek Nejvyššího soudu ze dne 16.1. 2001, sp. zn. 4 Tz 265/2000

SHRNUTÍ

Tato diplomová práce blíže pojednává o tématu počítačové kriminality a softwarového pirátství z pohledu kriminalistiky a trestního práva. Upozorňuje na stěžejní pojmy dané problematiky a pokouší se je jednoznačně vysvětlit. V menším měřítku se věnuje historickým okolnostem a vývoji této oblasti kriminality v České republice i zahraničí. Ve větším rozsahu zpracovává a popisuje jednotlivé skutkové podstaty trestných činů, které s tématem souvisejí, a věnuje se též srovnání starší právní úpravy s úpravou aktuální, tedy zákonem č. 40/2009 Sb. ve znění pozdějších předpisů. Stručněji se v práci zmiňuji také o zahraničních inspiracích a zdrojích, situaci v jednotlivých zemích a to především z hlediska organizačního. Za nejdůležitější zdroj z „evropského" prostředí zde považuji Úmluvu o počítačové kriminalitě. Také z tohoto důvodu je část práce věnována tomuto dokumentu.

Jedním z hlavních bodů této práce je vyšetřování počítačové kriminality a softwarového pirátství, postupy související s odhalováním a prokazováním trestné činnosti a problematika související včetně možností předcházení dané trestné činnosti.

RESUMÉ

The thesis deals with cyber crime and software piracy from the point of view of criminology and criminal Law. The purpose of the study is to highlights keywords of the theme and to clearly explain them. This thesis also considers historical circumstances and development of cybernetic criminality in the Czech Republic and abroad. The goal of the thesis is explanation of the various elements of criminal acts which are associated with the topic, and to compare previous legislation with the current one, regulated by law no. 40/2009. Moreover, there is also a survey of foreign inspirational sources and of a situation in foreign countries. The most important legal act in "European" area is the Convention on Cybercrime, therefore the significant part of my thesis is dedicated to this legal document.

The aim of the thesis is to explicate an investigation of computer crime and software piracy, procedures related to a detection and a proof of crimes and related issues, which includes a presentation of different ways of preventing the crime.

Klíčová slova / Key words

Počítačová kriminalita / Computer criminality

Úmluva o počítačové kriminalitě / Convention on Cybercrime

Vyšetřování počítačové kriminality / Investigation of Computer Crime

Kybernetická kriminalita / Cyber crime

Trestný čin / Crime

Softwarové pirátství / Software Piracy

Počítačové stopy / Computer tracks

Porušení autorského práva / Infringement of copyright

Škodlivý software / Malicious software

Osoba pachatele / Person of the offender

Přístup k počítačovému systému / Access to a computer system

Případ Napster / The case of Napster

Prevence / Prevention

Internet / Internet