Univerzita Pardubice

Fakulta ekonomicko-správní

Kybernetická trestná činnost a její ekonomické aspekty

Bc. Jaroslav Sochor

Diplomová práce

2015

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2014/2015

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jaroslav Sochor**
Osobní číslo:	**E13951**
Studijní program:	**N6202 Hospodářská politika a správa**
Studijní obor:	**Ekonomika veřejného sektoru**
Název tématu:	**Kybernetická trestná činnost a její ekonomické aspekty**
Zadávající katedra:	**Ústav ekonomických věd**

Zásady pro vypracování:

Cílem práce je vymezit kybernetickou trestnou činnost podle platného (a účinného) znění zákona a její vliv na ekonomiku. Součástí práce budou konkrétní případové studie, jejich deskripce, analýza a komparace s podobnými případy kybernetické trestné činnosti a jejich vlivem na ekonomiku.

Osnova:
- Teoretická východiska a použité metody.
- Historie a současnost zkoumaného problému.
- Právní rámec kybernetické trestné činnosti a jeho vývoj.
- Ekonomické aspekty kybernetické trestné činnosti.
- Případová studie v oblasti dané problematiky.

Rozsah grafických prací: -

Rozsah pracovní zprávy: **cca 50 stran**

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

Seznam odborné literatury:

CRAIG, P. P., HONICK, R. Softwarové pirátství bez záhad. 1. vydání. Překlad Tomáš Hlaváč. Praha: Grada, 2008, 212 s. ISBN 978-80-247-1765-4.
GŘIVNA, T. et al. Český právní řád a ochrana kyberprostoru: vybrané problémy. Praha: Karolinium, 2008. 140 s. ISBN 978-80-246-1703-9.
GŘIVNA, T., POLČÁK, R. Kybernetika a právo. 1. vydání Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.
JIROVSKÝ, V. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1.vydání Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.
MCQUADE, S. C. Encyclopedia of cyber crime. Westport, Conn.: Greenwood Press, 2009, xxiii, 210 p. ISBN 03-133-3974-0.
POLČÁK, R. Právo na internetu: spam a odpovědnost ISP. 1. vydání Brno: Computer Press, 2007. 150 s. ISBN 978-80-251-1777-4.
Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

Vedoucí diplomové práce: **Ing. Zdeněk Řízek, Ph.D.**
Ústav ekonomických věd

Datum zadání diplomové práce: **29. září 2014**
Termín odevzdání diplomové práce: **30. dubna 2015**

doc. Ing. Renáta Myšková, Ph.D.
děkanka

L.S.

doc. Ing. Jolana Volejníková, Ph.D.
vedoucí ústavu

V Pardubicích dne 29. září 2014

Prohlašuji

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury. Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 23. 7. 2015

Jaroslav Sochor

Rád bych poděkoval vedoucímu práce panu Ing. Bc. Zdeňkovi Řízkovi, Ph. D. za ochotný přístup a cenné rady při zpracování diplomové práce, dále Bc. Martině Machové za poskytnutí informací v oblasti právní úpravy kybernetické trestné činnosti.

ANOTACE

Kybernetická trestná činnost se stále vyvíjí a zdokonaluje úměrně k tomu, jak se vyvíjí informační technologie. V dnešní době není počítačová kriminalita pouze záležitostí jednotlivých států, protože pro tuto trestnou činnost neexistují hranice. Na to se snaží reagovat mezinárodní legislativa. Způsobené škody a ekonomické dopady se dají pouze odhadovat. V České republice nejvíce škod způsobují kybernetické podvody. Důležité je, aby se o tomto problému zvyšovalo povědomí a nebyl podceňován.

KLÍČOVÁ SLOVA

Kybernetická kriminalita, trestná činnost, útok, hacker, trestní zákoník, náklady

TITLE

Cybercrime and its economic aspects

ANNOTATION

Cybercrime is still being developed and perfected in proportion to how information technology develops. Nowadays cybercrime is not merely a matter for individual states because there are no boundaries for this crime. It seeks to reacts international legislation. Damages and economic impacts can only be estimated. In the Czech Republic the most damage are caused by cyber frauds. It is important that the increased awareness of the problem and not underestimated.

KEY WORDS

Cybercrime, criminal activity, attack, hacker, costs

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

BBS	Bulletin board system
COE	Comitte of Europe
CSIS	Center for Strategic and International Studies
ČR	Česká republika
ČPU	Česká protipirátská unie
ČSÚ	Český statistický úřad
DOS	Denial of Service
EU	Evropská unie
HDP	Hrubý domácí produkt
ICT	Informační a komunikační technologie
IT	Informační technologie
NATO	North Atlantic Treaty Organization
MV ČR	Ministerstvo vnitra České republiky
OECD	Organisation for Economic Co-operation and Development
OSN	Organizace spojených národů
P2P	Peer to peer
PC	Personal computer
TZ	Trestní zákoník
TPB	The Pirate Bay
UN	United Nations
WWW	World Wide Web

Úvod

Vzhledem ke skutečnosti, že se stále více lidských aktivit přesouvá z fyzického prostředí do prostředí kybernetického a s ohledem na rychlost vývoje v oblasti informačních a komunikačních technologií, který mnohdy předbíhá vývoj právní úpravy, je důležité věnovat tématu kybernetické trestné činnosti zvýšenou pozornost.

V úvodu diplomové práce jsou popsány základní pojmy tak, jak je definuje současná legislativa a mnozí autoři zabývající se problematikou kybernetické trestné činnosti. Následně navazuje popis příčin vzniku počítačové kriminality a krátký exkurz do historie počítačové kriminality ve světě a v České republice. Vyzdviženy jsou osobnosti, které udaly trend a směr, jakým se v budoucnu začala ubírat trestná činnost v oblasti informačních technologií.

Třetí kapitola je věnována právní úpravě jednotlivých typů kybernetických útoků v České republice. Pro konkrétní představu jsou zde uvedeny i jednotlivé případy kybernetické trestné činnosti ze současnosti. Zvláštní podkapitola je věnována organizované „pirátské“ skupině The Pirate Bay, která představuje (v současné době existující a fungující) subjekt trestné činnosti využívající nejmodernější technologie, na které nestačí legislativa adekvátně reagovat, a která se stala mimo jiné inspirací pro vznik Pirátských politických stran v Evropě.

Mezinárodní právní úprava kybernetické trestné činnosti, kterou se řídí jednotlivé členské státy mezinárodních organizací, je uvedena v kapitole čtvrté. Je zde podrobněji popsán jeden z nejvýznamnějších dokumentů Rady Evropy v oblasti počítačové kriminality Convention of Cybercrime, jehož ratifikací se členské státy zavazují k přijmutí legislativních opatření, která kriminalizují kybernetické trestné činy.

Pátá kapitola nabízí globální pohled ekonomických aspektů kybernetické trestné činnosti, podrobně se zabývá náklady korporací na konkrétní typy kybernetických útoků a součástí jsou také náklady na kybernetickou trestnou činnost ve vybraných zemích.

V závěru práce je provedena analýza kybernetické trestné činnosti v České republice. Jsou zde uvedeny počty trestných činů a jejich výše škod. Na základě dostupných dat jsou popsány vývojové trendy pro tuto oblast, komparovány jednotlivé typy kybernetických útoků a je zde poskytnut přehled typů pachatelů.

1 Teoretická východiska kybernetické trestné činnosti

Cílem kapitoly je definovat kybernetickou trestnou činnost. Definice vycházejí jak ze současné legislativy, tak i od autorů zabývající se touto problematikou. Součástí kapitoly je definice kyberprostoru, kybernetických útoků a útočníků. Poslední část je věnována současným problémům v této oblasti.

1.1 Kyberprostor

Pojem kyberprostor poprvé použil William Gibson v roce 1982 v povídce „Burning Chrome“. Do širšího povědomí se ovšem dostal prostřednictvím jeho románu „Neuromancer“. Kyberprostor je zde popsán takto: *„Kyberprostor. Sdílená halucinace každý den pociťovaná miliardami oprávněných operátorů všech národů, dětmi, které se učí základům matematiky…Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města, ustupující…“*[1]. Takto zní tedy úplně první definice kyberprostoru. Ovšem pro definici trestné činnosti v tomto prostoru není postačující, proto je zde uvedeno několik následujících.

Pokud bychom chtěli popsat kyberprostor dle aktuálního znění zákona o kybernetické bezpečnosti, pak bychom ho definovali jako: *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“*[2].

Docent Tomáš Gřivna uvádí, že *„kybernetický prostor nemá hmotnou podstatu, je imaginární. Jeho vznik a další existence je však závislá na světě reálném. Vznik kyberprostoru byl esenciálně spjat s určitou úrovní technologické vyspělosti společnosti, s rozvojem informačních a telekomunikačních technologií. Připojením na komunikační a informační služby vytváří jednotliví uživatelé určitý druh společného prostoru, který lze nazvat kyberprostorem.“*[3]

---

[1] GIBSON, William. *Neuromancer*. Unabridged ed. Westminster, Md: Books on Tape, 2011. ISBN 978-030-7969-958. s. 64 – 65.

[2] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti ve znění pozdějších předpisů.

[3] GŘIVNA, Tomáš, et al. Český právní řád a ochrana kyberprostoru: vybrané problémy. Praha: Karolinium, 2008. 140 s. ISBN 978-80-246-1703-9 . s . 21.

Kyberprostor můžeme tedy chápat jako nehmotný svět vytvářený moderními technologiemi existující vedle světa reálného. Je to prostor kde vyhledáváme a získáváme informace, vzděláváme se, podnikáme, obchodujeme, komunikujeme, jak mezi sebou tak i s institucemi a orgány státní správy, a v neposlední řadě se bavíme. Právě v tomto prostředí, pokud je vytvářena činnost, kterou je porušován zákon nebo je v rozporu s morálními pravidly společnosti lze mluvit o kybernetické trestné činnosti.

Specifikem kyberprostoru je především to, že pro něj neexistují státní hranice, je ve své podstatě tedy neomezený.[4]

1.2 Kybernetická trestná činnosti

Aby bylo možné definovat kybernetickou trestnou činnost, tedy trestnou činnost nacházející se v kyberprostoru je nejprve nutné definovat trestný čin. Podle trestního zákoníku je trestným činem *„protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně.“*[5] Konkrétními trestnými činy v této oblasti se věnuje kapitola třetí. **Kybernetickými trestnými činy lze tedy chápat takové trestné činy, které se nachází v kyberprostoru.**

Kybernetická trestná činnost neboli kybernetická kriminalita či kybernalita dle Jirovského může být namířena přímo proti počítačům, jejich hardwaru, softwaru, datům, sítím apod., nebo v ní vystupuje počítač pouze jako nástroj pro páchání trestného činu, případně počítačová síť a k ní připojená zařízení jsou prostředím, v němž se taková činnost odehrává.[6]

Skutečnost, že se virtuální svět[7] stává stále větší součástí či stále významnější paralelou světa reálného je i důvodem pro vznik a neustálý rozvoj kybernetické trestné činnosti. Lze předpokládat, že postupem času budou ozbrojená přepadení například bank nahrazeny kybernetickými útoky, které budou stále sofistikovaněji a účinněji narušovat bezpečnostní systémy.

Následující tabulka poukazuje na rozdíly mezi průměrným ozbrojeným přepadením a průměrným kybernetickým útokem.

---

[4] GŘIVNA, Tomáš; POLČÁK, Radim. Kybernetika a právo. 1. vydání Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7 -4.

[5] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

[6] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. Acta Universitatis Carolinae. ISBN 978-80-247-1561-2.

[7] Neboli kyberprostor.

Tabulka 1 Porovnání ozbrojeného přepadení s kybernetickým útokem

	průměrné ozbrojené přepadení	**průměrný kybernetický útok**
riziko	pachatel riskuje, že bude zraněn nebo zabit	bez rizika fyzického zranění
zisk	průměrně 3 až 5 tisíc USD	od 50 až do 500 tisíc USD
pravděpodobnost dopadení	dopadeno 50 % až 60 % útočníků	dopadeno přibližně 10 % útočníků
pravděpodobnost odsouzení	odsouzeno 95 % dopadených útočníků	u dopadených dojde k soudu pouze u 15 % útočníků a z nich je odsouzeno asi 50 %
trest	průměrně 5 až 6 let, pokud pachatel někoho nezranil	průměrně 2 až 4 roky

Zdroj: [33]

Je nesporné, že ekonomické následky kybernetických útoků nabývají neúměrně vyšších hodnot než následky klasických přepadení. To je také jedním z důvodů proč tomuto tématu věnovat zvýšenou pozornost.

Pro ucelení definice kybernetické trestné činnosti je zde kumulativně uvedena definice kyberzločinu[8] jak uvádí T. Gřivna a R. Polčák. Za kyberzločin se považuje[9]:

a) trestný čin ohrožující informační a komunikační technologie (dále jen ICT) – informační síťovou bezpečnost (trestný čin proti počítačové integritě)
b) trestný čin využívající ICT ke spáchání tradičních trestných činů (trestný čin vztahující se, k počítačům)
c) trestný čin vztahující se k obsahu, jako například dětská pornografie, pomluva a porušení práv k duševnímu vlastnictví (trestný čin vztahující se, k obsahu počítačových dat)

1.3 Kybernetický útok

Vytvořením kybernetického prostoru vznikl jako nechtěný produkt určitý prostor pro společensky nebezpečné aktivity nového typu – kybernetické útoky. Útoky v kyberprostoru

[8] Kyberzločinem se rozumí kybernetická trestná činnost.

[9] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-809-0378-674.

jsou velmi efektivní. Umožňují z jednoho místa zasáhnout chráněné zájmy na mnoha jiných místech ve velmi krátkém čase, v podstatě se zanedbatelnými finančními náklady.[10]

Kybernetickým útokem rozumíme útok hackera[11] či skupiny hackerů proti informačnímu systému. Jeho výsledkem může být buď „pouhé" prolomení zabezpečení nějakého systému bez motivace finančního obohacení, přes získávání informací až po velké finanční ztráty bankovních a jiných institucí nebo přerušení dostupnosti důležitého energetického zdroje.

Útok je v podstatě realizací hrozby. Hrozbu lze definovat jako „*cokoliv, co nějakým způsobem může vést k nežádoucí změně informace, chování systému nebo změně jeho parametrů*"[12] Hrozby mohou být úmyslné (úmyslný průnik útočníka do systému) a neúmyslné (chyba operátora). Dále lze hrozby dělit do tří skupin[13] - základní hrozby, aktivační hrozby a podkladové hrozby:

Základní hrozby

Můžeme rozeznat čtyři typy základních hrozeb:

- Únik informace – důvěrná informace je prozrazena neautorizovanému subjektu, nebo je jím odhalena.
- Narušení integrity – porušení konzistence dat, dochází k tvorbě nových dat, změně nebo vymazání dat.
- Potlačení služby – úmyslné bránění přístupu legitimního subjektu k informacím.
- Nelegitimní přístup – zdroj je používán neautorizovaným subjektem nebo neadekvátním způsobem.

Aktivační hrozby

Realizace aktivační hrozby vede k vytvoření základní hrozby, lze je členit na pět hrozeb:

- Maškaráda – případ, kdy se neautorizovaná entita (osoba či systém) vydává za odpovídající autorizovanou entitu.

[10] GŘIVNA, Tomáš. *Český právní řád a ochrana kyberprostoru: (vybrané problémy)*. Vyd. 1. V Praze: Karolinum, 2008, 140 s. Acta Universitatis Carolinae. ISBN 978-80-246-1703-9.

[11] Definice viz následující podkapitola.

[12] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. Acta Universitatis Carolinae. ISBN 978-80-247-1561-2.

[13] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. Acta Universitatis Carolinae. ISBN 978-80-247-1561-2.

- Obejití řízení – útočník využije systémové nebo bezpečnostní slabiny k získání neautorizovaných práv nebo privilegií.
- Narušení autorizace – zneužití autorizovaného přístupu ke zdroji pro neautorizované účely.
- Trojský kůň – nejběžnější případ útoku, kdy software obsahuje nepozorovatelnou část, která naruší bezpečnostní prvky systému, příkladem může být program na tvorbu textu, který je stažený z internetu. Editor potom odesílá text napsaný uživatelem autorovi trojského koně.
- Zadní vrátka – je případem, kdy je do systému vložena součást, která umožňuje při poskytnutí specifického datového řetězce na svůj vstup, obejít bezpečnostní nástroje systému.

1.4 Hacker

Pojem „hack“ nebo „hacking“ či „hacker“ je dnešní veřejností chápán spíše jako negativní výraz pro páchání nezákonné činnosti v počítačovém prostředí. Ne vždy však tomu tak bylo. Přesný původ slova „hack“ nebo „hacker“ není jednoduché nalézt, hlavně z důvodu rozdílností vysvětlení v jednotlivých zdrojích informací. V čem se zdroje shodují je to, že výraz hacker začal být používán studenty na Massachusettském technologickém institutu. Hacker byl tehdy výraz pro počítačového programátora manipulujícího s technologií. V dnešní době lze hackery rozdělit dle Encyclopedie of cybercrime na tři typy[14]:

- Black hat hackers (černý klobouk) – hackeři, kteří se podílejí na nezákonné činnosti, s cílem obohatit se.
- White hat hackers (bílý klobouk) – jsou ti, kteří používají své schopnosti pro činnosti, které nejsou v rozporu s etickými zásadami, může se jednat o hackery, kteří se zabývají testováním bezpečnostních systémů.
- Grey hat hackers (šedý klobouk) – je něco mezi černým a bílým kloboukem, pojem je používán například pro hackery, kteří nabourají systém, ale data nijak nezneužijí, namísto toho upozorní administrátora o bezpečnostních nedostatcích systému.

[14] MCQUADE, Samuel C. *Encyclopedia of cybercrime*. Westport, Conn.: Greenwood Press, 2009, xxiii, 210 p. ISBN 03-133-3974-0 .

Další možné rozlišování hackerů dle jejich zkušeností a motivace je následující[15] :

- Novice (novici) – tato skupina je tvořena jedinci s omezenými schopnostmi a znalostmi v programování, bezpečnosti sítí a systémů. Jedná se o nováčky v hackování. Tito hackeři užívají programy, které vytvořil někdo jiný. Důvod hackingu těchto lidí je založen na hledání vzrušení a objevování nového.
- Cyber-punks (cyber-pankerové) – tyto osoby oproti novicům disponují většími schopnosti v oblasti hackingu. Jejich činností je napadání webových stránek a změna jejich obsahu, posílání spamů atd.
- Petty Thieves (drobní zloději) – zloději pouze využívají internetu a počítačových technologií, aby dosáhli svých cílů. Mezi ty patří bankovní instituce, kreditní karty a lidé. Pro svou činnost využívají pouze existujících možností. Pro tuto skupinu jsou bezpochyby největší motivací finance.
- Internals (insideři) – tato skupina je již tvořena opravdovými profesionály v oblasti informačních technologií (IT). Jejich činnost je účelná, pracují pro společnosti zabývající se bezpečností.
- Old guard hackers (staří hackeři) – tato skupina má velmi dobré technické dovednosti a znalosti z oblasti IT. Jejich ideologií není škodit ale rozvíjet se a překonávat překážky. Primární motivací této skupiny je zvědavost poznání a výzva.
- Virus Writers (tvůrci virů) – tato skupina chce být vidět a chce, aby něco bylo vidět. Součástí viru mohou být různá sdělení. Své výtvory často neuvedou do oběhu, pouze je zpřístupní ostatním uživatelům.
- Profesional criminals (profesionální zločinci) – tato skupina je nejnebezpečnější. Jedná se o profesionály v dané oblasti, kteří jsou velmi dobře vytrénováni k hackerským útokům.
- Information Warriors (informační bojovníci) – tato skupina se snaží internet chránit proti předchozím skupinám. Je tvořena profesionály v oblasti IT, jedná se o vysoce kvalifikované jedince. Často pracují ve službách vlád, bezpečnostních sborech nebo odděleních velkých společností. Jejich motivací je ochrana dat.

Další pojem, který se často v oblasti kybernetické trestné činnosti vyskytuje je cracker. Crackera lze chápat jako hackera s tím rozdílem, že crackeři se již nerozlišují na

[15] CERIAS. *The Development of a meaningful hacker taxonomy: A two dimensional approach* [online]. 2005 [cit. 2015-05-31]. Dostupné z: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-43.pdf

„dobré“ a „špatné“. Crackeři jsou jen ti „špatní“. Crackera lze definovat jako *„člověka, který se nelegálně nabourává do počítačových systémů cizích lidí či firem* [16]*“,* nebo také jako *„člověka, který deaktivuje a obchází cizí softwary* [17]*“* jeho cílem je tedy získávání přístupu k citlivým datům, slídění v počítačích cizích atp.

1.4.1 Popis a etika hackera

Hackeři jsou často popisování jako uzavřené osoby, které vytváří své vlastní komunity, jedná se o velké individualisty, kteří jsou často neschopni pracovat v týmu. Hacker neuznává autority, pohrdá hierarchií. Peníze pro hackera znamenají pocit respektu ostatních členů komunity, obdiv a uznání. Základním vyznáním hackerů je svoboda. Hacker neřeší problém vícekrát, po vyřešení problému se k němu nevrací. Nový člen v komunitě hackerů získává respekt až potom co prokáže své schopnosti, ale také ochotu sdílet své znalosti s ostatními členy. Existují dva principy hackerské etiky, které jsou mezi touto komunitou přijímány:

- První princip je víra, že informace, které jsou sdílené, jsou správné. Etickou povinností hackera je dělit se o získané poznatky a usnadňovat přístup k informacím v co nejvyšší míře.
- Mezi druhý princip patří přesvědčení, že pokud se hacker naboural do systému pouze pro zábavu a získání zkušeností, je to eticky v pořádku. Ovšem jen v případě pokud nedojde k vandalismu, odcizení nebo narušení informací nebo porušení jejich utajení.[18]

1.5 Současné problémy

Tato podkapitola popsuje současné problémy v oblasti kybernetické trestné činnosti v souvislosti s legislativou, policií a justicí a chápáním bezpečnosti společností.

[16] BEZPEČNÝ INTERNET. *Slovník výrazů* [online]. 2015 [cit. 2015-05-31]. Dostupné z: http://www.bezpecnyinternet.cz/slovnik/.

[17] VÝZNAM SLOVA. *Význam cracker* [online]. 2015 [cit. 2015-05-31]. Dostupné z: http://www.vyznam-slova.com/cracker.

[18] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. Acta Universitatis Carolinae. ISBN 978-80-247-1561-2.

1.5.1 Legislativa

Hlavním problémem v oblasti legislativy je samotná definice kybernetické trestné činnosti, která se s neustálým vývojem technologií mění. Obecně lze ovšem kybernalitu chápat jako *„páchání trestné činnosti, v níž je aktivní složkou informační technologie jako souhrn technického a programového vybavení včetně dat“.*[19] Vzhledem k obtížnosti této definice a složitosti dokazování trestného činu často dochází k beztrestnosti páchání trestného činu a nepostihnutelnosti pachatelů.

Dalším problémem je legislativa v jednotlivých zemích. Právní normy nejsou schopny jednoznačně konkretizovat jednotlivé trestné činy. Některé státy v oblasti kybernality nemají žádný zákon, případně se existující zákon v jednotlivých jurisdikcích odlišuje. Tím pak mohou nastat případy, kdy určitá činnost v jedné zemi je trestná, zatímco v druhé zemi není do legislativy zahrnuta. Soudní řízení jsou tak nejasná a zbytečně zdlouhavá.[20]

1.5.2 Policie a justice

Kybernalita je pro policii a justici specifická oblast a to z důvodu, že je zde nedostatek kvalifikovaných pracovníků, kteří jsou schopni pojmout problematiku této oblasti. Jak po stránce technologické, právní i policejní. Stopy, které zůstávají po kybernetickém trestném činu, se značně liší od stop u klasického trestného činu. U kybernality stačí pro zajištění potřebných stop pár minut naopak u klasického trestného činu je to otázka dní. Kybernetický trestný čin je specifický tím, že dochází k neustálému technologickému vývoji a modifikacím jednotlivých oblastí. Rychlost vyšetřování neodpovídá současným technologickým trendům. Stejně je tomu tak i v případě justice. Je velmi obtížné odhalit, dokázat a odsoudit trestnou činnost pachatele. Také soudci nedisponují dostatečnými znalostmi z oblasti informačních technologií, je tedy nutné využít znalostí soudních znalců a spoléhat na ně.[21]

---

[19] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. Acta Universitatis Carolinae. ISBN 978-80-247-1561-2.

[20] ECOSOC. *Kybernalita* [online]. 2010 [cit. 2015-05-31]. Dostupné z: http://www.studentsummit.cz/data/1296412130369BGR_ECOSOC_Kybernalita.pdf.

[21] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. Acta Universitatis Carolinae. ISBN 978-80-247-1561-2.

1.5.3 Společnost

Společnost nepovažuje činy páchané v kyberprostoru za vážné. Na jedince, který převede peníze z účtu svého zaměstnavatele na svůj účet je nahlíženo jinak, než kdyby přepadl banku a peníze získal násilně. K laxnímu postoji ze strany veřejnosti dochází také proto, že policie a justice mnoho trestných činů neodhalí, nebo pro nedostatek důkazů neodsoudí, jak již bylo zmíněno v předchozí části.[22]

Velké části lidí se tento problém dotkne až v případě, že je na nich samotných trestný čin spáchán. V současné době stále častěji dochází k trestným činům jako je například zneužití osobních údajů nebo odcizení peněz z běžných účtů, pomocí phishingu.

1.5.4 Chápání bezpečnosti

Jak již bylo zmíněno v předchozím odstavci ze strany společnosti, nepředstavuje kybernalita takovou hrozbu jako přímé ohrožení. Většina lidí považuje používání počítače za bezpečné. Uživatelé často volí jednoduchá hesla, nebo posílají osobní informace prostřednictvím emailu nebo sociálních sítí a neuvědomují si možné následky.

Aby lidé svůj názor na tuto problematiku přehodnotili, je potřeba, zvyšovat povědomí o možných nebezpečí, používání internetu, zvyšovat gramotnost a informovanost běžného uživatele. A dosáhnout tak co nejvyšší bezpečnosti.[23]

[22] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. Acta Universitatis Carolinae. ISBN 978-80-247-1561-2.

[23] ECOSOC. *Kybernalita* [online]. 2010 [cit. 2015-05-31]. Dostupné z: http://www.studentsummit.cz/data/1296412130369BGR_ECOSOC_Kybernalita.pdf.

2 Příčiny vzniku a historický vývoj kybernetické trestné činnosti

Kapitola je zaměřena na stále se zvyšující sofistikovanost a promyšlenost kybernetické trestné činnost v souvislosti vývojem výpočetní techniky a věnuje se příčinám vzniku počítačové trestné činnosti.

2.1 Příčiny vzniku počítačové kriminality

S masovým rozvojem využívání počítačů a internetu a vzájemným propojováním jednotných systémů bylo pro pachatele stále více lákavé nelegitimní zneužití systémů za účelem krádeže osobních dat nebo elektronických loupeží na bankovní účty. Konkrétní příčiny vzniku počítačové kriminality lze vymezit následovně[24]:

- Složitost informačních technologií – informační technologie jejich provoz je vnímaný značným procentem uživatelů jako neproniknutelný.
- Důvěra uživatelů – uživatel věří informačnímu systému a málokoho napadne například zkontrolovat správnost výpočtu, který provedl počítač, či připravený počítačový systém, z těchto důvodů může dojít k odhalení počítačového podvodu až po určité době, či neodhalení pachatele.
- Objem dat – z důvodu enormního objemu dat, je prakticky nemožné efektivně zkontrolovat veškerá data, která sítěmi procházejí.
- Nedostatečné právní povědomí – v oblasti informačních technologií je povědomí populace o právu ještě nižní než v běžných oblastech a to z důvodu složitosti norem, které se vztahují k IT oblasti, pro většinu občanů je také velmi složité například už jen vytvořit povědomí o zákoně o elektronickém podpisu, natož si vytvořit představu co je v tomto zákoně obsaženo.
- Způsob páchání trestné činnosti – spáchat trestný čin v oblasti IT je mnohem snazší než v běžném občanském životě, například složitost bankovní loupeže přes internet za pomoci stisknutí několika kláves oproti klasické bankovní loupeži nesrovnatelná.
- Nedokonalost legislativy – opět souvisí se složitostí právní úpravy v oblasti IT. V dalších částech práce je tomuto problému věnována pozornost, je zde uvedena právní úprava základních typů kybernetických trestných činů a jejich trestně právní postih.

[24] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-722-6419-2.

2.2 Historie počítačové kriminality

Tato podkapitola je věnována historii a vývoji počítačové kriminality. Vývoj trestné činnosti v této oblasti lze dle literatury dělit mnoha způsoby. V této práci je historie rozdělena dle autora Matějky na tři období, která jsou následně popsána z hlediska jednotlivých případů trestné činnosti v souvislosti s vývojem výpočetní techniky. Jedná se o období:

- pravěk - období od vynálezu telefonu po uvedení prvního PC na trh do roku 1981,
- středověk - od roku 1981 do roku 1991,
- novověk - od roku 1994 do současnosti.

2.2.1 Pravěk

Za první „počítačový“ zločin je považován případ z roku 1801. Tehdy tkadlec jménem Jacquard sestrojil primitivní zařízení, které umožňovalo automatizovat a vykonávat jednotlivé úkoly při tkaní látek. Zaměstnanci manufaktury byli z tohoto vynálezu natolik vyděšeni před ztrátou zaměstnání, že po několika sabotážích donutili pana Jacquarda od vývoje vynálezu upustit. Jako další případ lze uvést období kolem roku 1878, kdy si náctiletí chlapci, kteří pracovali jako obsluha telefonní ústředny, zpestřovali pracovní dobu spojováním k sobě nepatřících hovorů. Ovšem po opakovaných stížnostech byli mladíci nahrazeni pečlivějšími dívkami.[25]

Počátky počítačového věku směřují do roku 1946. Toho roku přesně 14. února byl na pensylvánské univerzitě sestrojen první elektronický počítač jménem Eniac.[26] V tomto období ovšem ještě nelze uvažovat o možnosti kriminálního zneužití. Především proto, že první počítače zabíraly téměř celé místnosti, kde musela být neustále regulována teplota. Dále vysoká cena těchto počítačů znamenala, že místnosti, kde byly počítače uloženy, se staly nejlépe hlídanými prostory v celé firmě.

Sedmdesátá léta jsou známa jako období, kdy se začala rozmáhat trestná činnost v podobě nelegálního kopírování hudby. To souviselo především s rozšířením kazetového magnetofonu.

[25] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-722-6419-2.

[26] WEIK, Martin H. *The ENIAC Story* [online]. 1961 [cit. 2015-06-01]. Dostupné z: http://ftp.arl.mil/mike/comphist/eniac-story.html.

Známou osobností této doby byl John Draper, který v roce 1971 proslul jménem „*Captian Crunch"*. Draper dokázal oklamat telefonní síť pomocí dětské píšťalky, která byla přidávána do dětských cereálií značky *Cap „n " Crunch*. Píšťalka vydávala tón o kmitočtu 2600 Hz, kterým se řídilo přepínání dálkových hovorů.[27] Tuto událost lze považovat jako první hackerský útok, který známe ze současnosti.

K rozvoji hackingu došlo v osmdesátých letech, kdy byla vynalezena technologie BBS neboli Bulletin Board Systém. Pomocí BBS se mohl uživatel počítače připojit na vzdálenější síť a čerpat informace z databáze uložené na počítači pomocí standardizovaných dotazů.[28] V tomto období také začaly vznikat první hackerské skupiny, které si vyměňovaly přístupové kódy a hesla. Právě první pokusy hackerů se soustřeďovaly na prolamování uživatelských hesel.

2.2.2 Středověk

Datum 12. srpna 1981 se dá považovat za přelom v oblasti počítačových technologií. Byly vytvořeny předpoklady k tomu, aby se počítače rozšířily do všech firem i domácností. Hlavními aspekty bylo jednoduché uspořádání a rozšíření komponentů. V osmdesátých letech také došlo ke sloučení počítače a telefonní linky, díky tomu bylo umožněno rozšíření předchůdce internetu v podobě již zmíněného systému BBS.[29]

S rozšířením webových technologií se začaly objevovat hackerské nástroje, které byly označovány jako „easy-to-use". Mezi hackery se objevovali i lidé, bez potřebného vzdělání v oboru a dostatku vědomostí. Začaly vznikat weby určené pro hackery, na kterých bylo možné stáhnout programy využívající bezpečností mezery v systému.[30]

V tomto období jsou za významné hackery považováni Kevin Mitnick, Robert Morris a Kevin Poulsenov. Kevin Mitnick je známý díky útoku na počítače společnosti Digital Equipment, který uskutečnil v roce 1988 a také tím, že se stal prvním pachatelem počítačového trestného činu, který se objevil na listině FBI Most Wanted. Ve stejném roce poslal Robert Morris virus zvaný InternetWorm. Tím upozornil na nový typ počítačové kriminality, tedy průnik do jiného počítače pomocí vytvořené infekce počítačovým virem.

---

[27] WEBCRUNCHERS. *Who is John Draper AKA Captain Crunch* [online]. 2015 [cit. 2015-06-01]. Dostupné z: http://www.webcrunchers.com/who-is-john-draper-aka-captain-crunch/.

[28] ROUSE, Margaret. *Bulletin board system* [online]. 2005 [cit. 2015-06-01]. Dostupné z: http://whatis.techtarget.com/definition/bulletin-board-system-BBS.

[29] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. Acta Universitatis Carolinae. ISBN 978-80-247-1561-2.

[30] Tamtéž.

Oba dva hackeři byli zadrženi a Mitnick byl odsouzen na jeden rok vězení nepodmíněně a Morris dostal peněžní trest ve výši deset tisíc dolarů. Třetí hacker Kevin Poulsen se proslavil tím, že v roce 1991 se cíleně naboural do telefonních linek rozhlasové stanice v Kalifornii, aby vyhrál automobil značky Porsche v posluchačské soutěži. Kevin Poulsen byl odsouzen na čtyři roky vězení a dostal pokutu padesát osm tisíc dolarů.[31]

Konec období středověk znamenal profesionalizaci v oblasti počítačového zločinu. Zatímco do té doby představoval počítačový pachatel osobu, pro niž je proniknutí do systému výzvu a zábavu. Cíl se změnil ze snahy získat slávu, vydělat peníze.[32]

2.2.3 Situace v ČSSR

Až do konce roku 80 nelze o počítačové kriminalitě v ČSSR uvažovat. V této době téměř neexistovaly domácnosti, které by vlastnily osobní počítač. Informační technologie patřily k embargovanému zboží. Výpočetní techniku vlastnilo pouze pár univerzit a podniků, která byla navíc komunistickým režimem neustále podezřívána a kontrolována. Koncem 80. let se situace změnila. Do ČSSR byly dováženy počítače značek Sinclair, Atari nebo Commodore. K tomu se připojila výroba domácích počítačů značky Didaktik IQ či PMD. Za nedlouho začal fungovat trh s hrami a aplikacemi pro tyto počítače, jednalo se ovšem o nelegální šíření. Přesto se v této době objevily případy, které se řadí mezi počítačovou kriminalitu.[33]

Jedním z příkladů je poškození záznamových pásek magnetem, které způsobil pracovník Úřadu důchodového zabezpečení. Dalším případem byla zpronevěra za pomoci počítače, kdy pracovnice obchodu Magnet cíleně měnila statusy objednávek z „nezaplaceno“ na „zaplaceno“. Dále zneužívání výpočetní techniky ve mzdových účtárnách. Objevovaly se také delikty, jako bylo zasílání faktur na jiné velkoodběratele a manipulace s výplatami zaměstnanců. Jednalo se o nejčastější odhalený počítačový zločin, jehož podstatou byly manipulace v mzdových účtárnách, odbytech a na jiných pracovištích, kde pracovníci měli možnost manipulovat s penězi. Pouze v osmdesátých letech to bylo 14 případů trestního stíhání.[34]

---

[31] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-722-6419-2.

[32] Tamtéž.

[33] Tamtéž.

[34] SMEJKAL, Vladimír. *Informační a počítačová kriminalita v České Republice* [online]. 1999 [cit. 2015-06-01]. Dostupné z: http://www.mvcr.cz/casopisy/studie/diskuse/analyza.html.

Významnou událostí pro Českou a Slovenskou Federativní republiku bylo datum 13. února 1992 tohoto roku byla země oficiálně připojena k internetu. V této době ovšem ještě nelze uvažovat o zneužití internetu na našem území k nekalým praktikám. Internet nebyl k dispozici mimo akademickou půdu.[35]

2.2.4 Novověk

V období novověku tedy od roku 1994 docházelo k masovému rozšíření počítačů, zejména na platformě PC s operačním systémem Microsoft Windows. Dále došlo k rozšíření sítě internet a její nejviditelnější podoby WWW (World Wide Web). Internet přestává být výhradou akademických kruhů, ale vstupují do něj i podnikatelské subjekty. To začíná stále více přitahovat počítačové podvodníky, jejichž hlavním cílem je dosažení zisku. Prozatím nedochází k ovládnutí internetu organizovanými skupinami, ale pouze jednotlivci, kteří se zaměřují převážně na podvody s ukradenými kreditními kartami, útoky na bankovní systémy, finanční instituce a aktivity spojené s internetovými kasiny.[36]

Příkladem počítačové kriminality z této doby, lze zmínit případ Citibank. V roce 1994 hacker Vladimir Levin se svou skupinou zneužili přístupové kódy a hesla potřebná k tomu, aby se nabourali do systému americké banky Citibank. Během krátké doby se Levin osmnáctkrát nalogoval[37] do systému banky a postupně převedl 10,7 miliónů dolarů. Uloupené peníze převáděl na účty rozmístěné ve Spojených státech, Nizozemí, Finsku, Německu a Izraeli. Útoky vykonával mimo domov, údajně z Petrohradu, a pracoval ve večerních hodinách. Tedy v době, kdy byla v New Yorku špička, z důvodu aby nevzbudil pozornost. První problém nastal, když si banka ve spolupráci se svými klienty všimla ztracených čtyři sta tisíc dolarů. Po kontaktování FBI bylo jasné, že se jedná o nelegální transfery. FBI pracovala velmi rychle a za pomoci Levinových spojenců, kteří byli přinuceni Levina vylákat na schůzku do Londýna, byl na londýnském letišti zadržen. Po neúspěšných třiceti měsících, kdy jeho právníci bojovali, aby Levin zůstal v Londýně, byl v roce 1997 deportován do USA, kde byl odsouzen k třem rokům vězení a pokutě dvě stě čtyřicet tisíc dolarů.[38]

---

[35] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-722-6419-2.

[36] Tamtéž.

[37] Tzn. přihlásil do systému.

[38] BRZOBOHATÝ, Michal. *Galerie nejlepších hackerů historie* [online]. 2008 [cit. 2015-06-01]. Dostupné z: http://pcworld.cz/ostatni/galerie-nejlepsich-hackeru-historie-12-dil-3475.

2.2.5 Situace v České republice

V České republice se situace v této oblasti po roce 1989 výrazně zhoršila. Krátce po revoluci se začalo významně obchodovat s nelegálními hudebními a video nahrávkami a prodejem nelegálního softwaru. S nástupem internetu se šíření nelegálního softwaru ještě zhoršilo. Policie se nelegálním praktikám zpočátku snažila zabránit. Ovšem počátkem 90. let byla znalost této problematiky velmi nízká a nelegální softwary představovaly téměř 80 % podílu.[39]

[39] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-722-6419-2.

3 Právní úprava a konkrétní případy počítačové kriminality

Kapitola se věnuje popisem kybernetických útoků, jejich trestně právním postihem podle platných znění zákonů a u jednotlivých typů trestných činů jsou uvedeny příklady ze současnosti.

Počítačovou kriminalitu lze rozdělit na trestné činy proti důvěřivosti, integritě a dostupnosti počítačových dat a systémů. Dále na trestné činy se vztahem k počítači, trestné činy související s obsahem a trestné činy související s porušováním autorského práva a souvisejících práv. Konkrétněji se jednotlivým formám a konkrétním činům věnují následující podkapitoly. Komplikovanost samotného posouzení jednotlivých trestných činů je potom na odbornících z oblasti trestního práva. V tomto textu jsou pouze základní údaje a nejjednodušší příklady kyberkriminality a jejich posouzení z hlediska diplomové práce.

3.1 Krádež, loupež

Tato protiprávní jednání zařadíme pod počítačovou kriminalitu jen okrajově a to v případech, kdy dochází k odcizení počítače, hardwaru, záznamových medií atd. Proto je toto jednání zařazeno samostatně. V případě loupeže je při odcizení výše uvedeného použito násilí, nebo pohrůžka bezprostředního násilí s úmyslem zmocnit se příslušného zařízení.[40] Postih těchto protiprávních jednání se především odvíjí od výše způsobené škody.

3.2 Trestné činy proti důvěřivosti, integritě a dostupnosti počítačových dat a systémů

3.2.1 „Hacking“

Termínem hacking zjednodušeně označujeme proniknutí do počítačového systému a bezpečnostního opatření tohoto systému jinou, než standardní cestou. Tento pojem je celosvětově užívaný. V minulosti se hackeři snažili o zjištění funkčnosti systému a opravy jeho chyb. Nepochybně byl tedy tento termín chápán v kladném slova smyslu. V dnešní době je tomu naopak a hacking je chápán spíše v protiprávním slova smyslu.[41]

„Počítačovým systémem se rozumí jakékoli zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat. Počítačovým systémem je tedy zařízení, sestávající

[40] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

[41] Podrobněji viz. kapitola 1 .4.

z technického (hardware) a programového (software) vybavení, které je určené k automatickému zpracování digitálních dat. Bezpečnostním opatřením je třeba rozumět každé opatření, jehož cílem je zabránit volnému přístupu k počítačovému systému nebo nosiči informací (např. heslo nebo použití firewallu).''[42]

Dle § 230 zákona č. 40/2009 Sb., trestního zákoníku (dále jen TZ) je překonání bezpečnostního opatření, a tím neoprávněné získání přístupu k počítačovému systému postihnuto trestem odnětí svobody v rozsahu až jednoho roku, zákazem činnosti nebo propadnutím věci, či jiné majetkové hodnoty. Kdo získá přístup k počítačovému systému nebo nosiči informací a zároveň data neoprávněně užije, vymaže, zničí, nebo poškodí, padělá, nebo pozmění, nebo neoprávněně data do systému vloží, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty. Přitěžující okolností, která způsobí zvýšení trestu, je úmysl způsobit jinému škodu, nebo újmu, nebo získat sobě, nebo jinému neoprávněný prospěch, nebo úmysl neoprávněně omezit funkčnost systému. Další přitěžující okolností je, pokud je spáchán tento trestný čin ve skupině, způsobená škoda je značného rozsahu, nebo získání značného prospěchu. V tomto případě může být pachatel potrestán odnětím svobody v délce trvání až pěti let. Trestní zákoník nově upravuje a postihuje i nedbalostní formu poškození systému. Účel ustanovení § 232 TZ[43] je především v postihu jednání spočívajícího v hrubé nedbalosti u správců sítě, informatiků apod.

Konkrétním příkladem této nelegální aktivity je případ brněnského hackera, kterého se podařilo policii dopadnout, a který celých sedm let využíval systémové chyby a napadal osobní počítače s operačním systémem Linux.[44]

3.2.2 Narušování systému – DoS útoky

Zkratka DoS znamená Denial of Service, v překladu jde o odmítnutí služby. Jde o kybernetické útoky, které mají za cíl znepřístupnit určitou službu, počítač, nebo síť.[45] DoS

[42] ŠÁMAL, Pavel. 2010. *Trestní zákoník: komentář*. 1. vyd. V Praze: C. H. Beck, 2 v. ISBN 97880740017892.

[43] Trestné činy podle TZ jsou uváděny ze zvláštní části TZ, jinak je u § uvedena část obecná.

[44] MASARYKOVA UNIVERZITA. *Bezpečnostní tým z Masarykovy univerzity odhalil hackera* [online]. 2014. [cit. 2015-05-14]. Dostupné z: http://www.online.muni.cz/udalosti/4814-bezpecnostni-tym-z -masarykovy-univerzity-odhalil-hackera#.VVRlrPDUeq9.

[45] SECURITY PORTAL. *Seznamte se – DoS a DDoS útoky* [online]. 2013. [cit. 2015-05-14]. Dostupné z: http://www.security-portal.cz/clanky/.

útok zahlcuje webové servery mnoha požadavky, takže dochází k zahazování legitimních požadavků.[46]

Protiprávnost jednání spočívá v neoprávněném zásahu do počítače, který zapříčiní jeho vyřazení činnosti, nebo snížení výkonu. Tímto je znemožněno oprávněnému uživateli počítač využít.

Nejčastějšími útoky tohoto typu jsou:[47]

- Mass mailing list - hlavní podstatou tohoto útoku je zahlcení e -mailové schránky, tak, aby se stala nepoužitelnou.
- E -mail bombs - útok velice podobný Mass mailingu. Všechny e -maily zde však generuje útočník. Cílem není pouze zahlcení schránky, ale i snaha o to, zhroutit celý poštovní server.
- Fork bomb – lokální útok, k jehož provedení se používá programů, které pouští do nekonečna samy sebe. To má za následek jednak postupné zpomalování počítače, kterému dochází volná paměť. Lze použít pouze na počítač, který má pachatel fyzicky k dispozici.

Postih tohoto jednání je v platné právní úpravě velice špatně dohledatelný. § 230 TZ zde nemůžeme uplatnit, neboť zde není naplněna skutková podstata tohoto trestného činu. Při tomto jednání nedochází k získání přístupu k danému systému. Při právní kvalifikaci je možno užít § 132 v obecné části TZ, ve kterém je upřesněn pojem zařízení a elektronických komunikací a to tak, že tato zařízení jsou zařazena mezi prospěšná. Tyto útoky je na základě tohoto paragrafu možno zařadit pod § 276 TZ - poškození a ohrožení provozu obecně prospěšného zařízení a ve vybraných případech také pod skutkovou podstatu ustanovení § 272 TZ, tedy trestný čin obecného ohrožení. Za tyto útoky by tedy pachatel mohl být potrestán odnětím svobody až na 15 let.

K jednomu z nejznámějších případů masivního DDoS[48] útoku v ČR došlo v březnu roku 2013. Tehdy tomuto typu kybernetické trestné činnosti podlehlo několik bankovních serverů, konkrétně se jednalo o Českou spořitelnu, ČSOB a Komerční banku. Tyto banky měly vyřazeny na několik hodin internetové stránky, internetové a mobilní bankovnictví.

[46] SCAMBRAY, Joel a Mike SHEMA. *Hacking bez tajemství: webové aplikace*. Vyd. 1. Brno: Computer Press, 2003, xxix, 328 s. ISBN 80-722-6769-8.

[47] HALLER, Martin. *Denial of Service (DoS) útoky: záplavové typy* [online]. 2006. [cit. 2015-05-14]. Dostupné z: http://www.lupa.cz/clanky/denial-of-service-dos-utoky-zaplavove-typy/.

[48] DDoS (Distrbuted Denial of Service) narozdíl od DoS útoku je iniciován z více strojů - dva a více (statisíce).

Také server České národní banky nezůstal nedotknutý. Internetové stránky ČNB nešly aktualizovat a zaměstnanci byli nuceni zpřístupňovat informace přes Twitter a přes Facebook. Několik dní předtím podlehli útoku také zpravodajské servery mezi nimi například Ihned.cz a také Seznam.cz.[49]

3.2.3 Spamming – zasílání nevyžádané elektronické pošty

Znakem spammingu je hromadný charakter nevyžádané zprávy, která je rozesílána na mnoho e-mailů současně. Tato elektronická pošta nejčastěji obsahuje nějakou reklamu.[50] Spam nejčastěji obsahuje obchodní, společensky nebezpečné, politické nebo náboženské sdělení.[51] Pro nalezení právní úpravy, která upravuje spaming, je třeba se obrátit na normy správního práva, konkrétně do zákona č. 480/2004 Sb., o některých službách informační společnosti. § 7 tohoto zákona upravuje zasílání „obchodních sdělení" a to tak, že je vyžadován předchozí souhlas s jejich zasíláním, jinak se takováto sdělení považují za zakázané. V § 11 odst. 1 jsou poté různé formy spammingu definovány za správní delikt a díky tomu můžou být rozesílatelé za některý druh spammingu trestány pokutou až do výše 10 mil. Kč.[52] Spamming můžeme dále podřadit pod skutkovou podstatu přestupku dle zákona č. 127/2005 Sb., o elektronických komunikacích, který stanovuje, že fyzická osoba, která použije adresu elektronické pošty za účelem odeslání zprávy nebo zpráv třetím osobám, bez souhlasu držitele této e-mailové adresy se dopouští přestupku dle tohoto zákona a toto jednání může být potrestáno pokutou až do výše 100.000,-Kč, v případě právnické osoby až do výše pěti milionů korun.[53]

3.2.4 Sniffing – odposlech dat

Sniffing znamená neoprávněné „odposlouchávání" komunikace v počítačové síti.[54] K tomuto účelu se požívají především speciální programy (sniffery), které umožňují

[49] FRANCOVÁ, Pavla. *Největší banky v Česku napadli hackeři. Vyřadili jim z provozu internetové bankovnictví* [online]. 2013. [cit. 2015-05-14]. Dostupné z: http://byznys.ihned.cz/c1-59450640-nejvetsi-banky-v-cesku-napadli-hackeri-vyradili-jim-z-provozu-internetove-bankovnictvi.

[50] JIROVSKÝ, Václav. 2007. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada (s. XX).

[51] POLČÁK, Radim a Mike SHEMA. *Právo na internetu: spam a odpovědnost ISP*. Vyd. 1. Brno: Computer Press, 2007, v, 150 s. Právo a IT. ISBN 978-80-251-1777-4.

[52] Zákon č. 480/2004 Sb., o některých službách informační společnosti ve znění pozdějších předpisů.

[53] Zákon č. 127/2005 Sb., o elektronických komunikacích ve znění pozdějších předpisů.

[54] JIROVSKÝ, Václav. 2007. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 284 s. ISBN 978-80-247-1561-2.

monitorovat veškerou komunikaci procházející přes dotyčný uzel sítě. Takto je možno získat veškerý obsah nešifrované komunikace, to znamená, že se sniffer může dostat na různá přístupová jména a hesla, na soubory posílané po síti a také i na znění e-mailu.[55] Na toto jednání lze uplatnit § 230 TZ v případě, že pachatel získal přístup k počítačovému systému. Dále můžeme aplikovat § 182 TZ porušování tajemství doručovaných zpráv a také § 183 TZ porušování tajemství listin a jiných dokumentů uchovávaných v soukromí, kdy jsou tato jednání postihnuta trestem odnětí svobody až na 10 let, dle závažnosti a naplnění upravených skutkových podstat, peněžitým trestem, nebo zákazem činnosti.

Mezi další způsoby sniffingu řadíme používání speciálních zařízení a programů, které např. snímají stisky jednotlivých kláves na počítačové klávesnici, s jejichž pomocí je poměrně snadné zjistit zadávaná hesla jiných lidí. Tato jednání jsou taktéž postihnutelná ustanovením § 182 odst. 1 písm. c) TZ.

Konkrétní případy sniffingu zde nejsou uvedeny především z důvodu, že nebyly nikde evidovány. Nicméně pro konkrétní představu tohoto trestného činu, je zde uveden způsob, jakým bylo možné ještě do nedávna „odposlouchat“ přihlašovací údaje například do sociální sítě Facebook. Do mobilního telefonu (předpokladem je operační systém android) stačí nainstalovat aplikaci s názvem FaceNiff, připojit se na místní Wi-Fi síť (například v restauraci nebo ve firmě) a spustit danou aplikaci. Program začne sledovat komunikaci v této síti a následně odhalí tzv. session ID, což je v podstatě jedinečný identifikátor pro přihlášení do sociální sítě. Aplikace poté vypíše seznam napadnutelných kontaktů, u kterých tento identifikátor zachytil a jediné co stačí, kliknout na ikonu dotyčného a otevře se jeho Facebookový profil. V současné době je již Facebook chráněn o něco více a tedy tento konkrétní způsob sniffingu již není aplikovatelný.[56]

3.3 Trestné činy se vztahem k počítači

3.3.1 Phishing

Slovo phishing označuje podvodné e-mailové útoky na uživatele internetu, jejichž cílem je vylákat důvěrné informace (údaje k platebním kartám, přihlašovací údaje k účtům). Mezi základní znaky phishingového e-mailu patří grafická podoba e-mailu, která se snaží

[55] MATĚJKA, Michal. 2002. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, x, 106 s. ISBN 80-722-6419-2.

[56] HACKOVANÍPC. *Nabourání FB účtu* [online]. 2012. [cit. 2015-05-14]. Dostupné z: http://hackovanipc.webnode.cz/hacking/nabourani-fb-uctu/.

vyvolat dojem, že byl e-mail odeslán příslušnou organizací (banka, nebankovní spol., exekutorský úřad. Text většinou připomíná informaci o neprovedené platbě, výzvu k aktualizaci bezpečnostních údajů, oznámení o dočasném zablokování účtu.[57] Pokud na tento e-mail dotyčná osoba odpoví, stává se obětí phishingu.

Na toto jednání se vztahuje skutková podstata trestného činu podvodu, dle § 209 TZ, kdy jde o podvod spáchaný za pomocí počítače. Aby byla skutková podstata naplněna, musí dojít ke škodě a zároveň obohacení pachatele. Tento skutek může být potrestán odnětím svobody v délce trvání až 10 let, peněžitým trestem, zákazem činnosti, nebo odebráním věci majetkové hodnoty.

3.3.2 Pharming

Slovem pharming můžeme označit zdokonalenou formu phishingu. *„Pharming využívá speciální počítačové programy, které uživatele při přihlášení do internetového bankovnictví přesměrují na stránky, jež sice vypadají jako stránky jeho banky, ale ve skutečnosti jsou pouze jejich napodobeninou. Zde pak klienta požádají o zadání všech přihlašovacích hesel a kódů. Pokud tak klient učiní, mohou se neoprávnění uživatelé přihlásit do internetbankingu pod jeho jménem, a pokud klient nemá nastaveno další zabezpečení (např. potvrzování transakcí pomocí autorizační SMS nebo klientský certifikát), mohou mu nepozorovaně převést peníze z jeho účtu.“*[58] Tato metoda, která je postihována také dle § 209 TZ, tedy jako trestný čin podvodu, naplňuje navíc skutkovou podstatu trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ.

Phishing a pharming jsou v současné době v České republice jedněmi z nejrozšířenějších druhů kybernetické trestné činnosti. Mediálně známou kauzou z roku 2014 je případ klienta Fio banky, který přišel o své peníze ze svého bankovního účtu. Klientovi přišel podvodný e-mail s přílohou. V příloze byl malware – tedy škodlivý program, který klienta po přihlášení do internetového bankovnictví přesměroval na podvodné stránky vypadající jako stránky Fio banky. Zde zadal přihlašovací údaje s heslem a následně byl vyzván pro stažení aplikace na mobilní telefon „kvůli zvýšení zabezpečení bankovního

[57] HOAX. *Co je to phishing* [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing.

[58] BEZPEČNÝ INTERNET. *Phishing a pharming* [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx.

účtu“. Tato podvodná aplikace pak přeposlala potvrzovací SMS kód útočníkovi, který toho následně využil.[59]

3.3.3 Škodlivé šíření informací - HOAX

Termínem HOAX označujeme šíření poplašných, nebezpečných a zbytečných řetězových zpráv. Všechny verze HOAXů obsahují společný znak a tím je prosba adresovaná příjemci elektronické zprávy, aby byla tato zpráva shlédnuta pokud možno co největším počtem lidí. Jedná se ve své podstatě o určitou formu spamu. Zda se jedná o HOAX je možné si ověřit na webovém serveru, který je právě tomuto jednání věnován.[60]

Toto šíření je regulováno trestním právem. Můžeme zde uplatnit více ustanovení, např. § 357 TZ - šíření poplašné zprávy, § 184 TZ pomluva, § 356 TZ podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod podle, § 365 TZ schvalování trestného činu. Sankce je zde dle závažnosti, míry poškození a naplnění jednotlivých skutkových podstat výše zmíněných trestných činů, obvykle trest odnětí svobody, peněžitý trest, zákaz činnosti, nebo odebrání věci majetkové hodnoty.

Mezi nejrozšířenější HOAXY patří „Infikované jehly na sedadlech, Nebezpečný moderní jogurt, V nouzi zadej PIN opačně, Windows live aktualizace, Recyklované mléko, Cikánka a úvěr, Telefonáty z čísla 00420 477 100 111“.[61]

3.3.4 Neoprávněné nakládání s osobními údaji

Tato forma počítačové kriminality je sice upravena v § 180 TZ jako trestný čin neoprávněné nakládání s osobními údaji, ale dané ustanovení postihuje jen neoprávněné zveřejnění, sdělení, zpřístupnění, či jiné zpracování nebo přisvojení si osobních údajů shromážděných v souvislosti s výkonem veřejné moci. Co se týče problematiky neoprávněného nakládání s údaji získanými v rámci soukromého sektoru, musíme se opět obrátit na normy správního práva a to konkrétně do zákona č. 101/2000 Sb., o ochraně osobních údajů, jenž toto neoprávněné zpracování osobních údajů sankcionuje poměrně vysokými pokutami (až do výše 10 mil. Kč).

---

[59] VOPAT, Radek. *Fio banka a phishing v praxi: Aktuální zkušenost* [online]. 2014 [cit. 2015-06-06]. Dostupné z: http://finexpert.e15.cz/fio-banka-a -phishing-v -praxi-aktualni-zkusenost.

[60] HOAX [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://hoax.cz/cze/.

[61] Tamtéž.

3.3.5 Kybernetické vydírání

Pojmem kybernetické vydírání označujeme takové jednání, kdy jsou majitelé systémů připojených k internetu zastrašováni hrozbou provedení určitého typu počítačové kriminality, pokud nebudou splněny požadované podmínky. Může se tedy jednat o průnik do systému, zničení či zneužití dat apod. Protože žádný systém si nemůže být zcela jist dokonalým zabezpečením, takto vydírané osoby či instituce raději nedobrovolně spolupracují.[62] Takovéto jednání je považováno za trestný čin vydírání podle § 175 TZ a sankcionováno v krajním případě odnětím svobody na dobu 16 let, nebo peněžitým trestem.

Příklad tohoto trestného činu byl zveřejněn v dubnu roku 2015. Samotný průběh útoku je podobný jako u phishingu nebo pharmingu. Opět je potenciální oběti odeslán podvodný e-mail od nějaké důvěryhodné instituce a upozorňuje na nedoplatek faktury, informaci o zásilce nebo nevyřízenou objednávku. E-mail obsahuje v příloze malware, v tomto konkrétním případě se jedná o downloader Elenoočka. V minulosti byl program Elenoočka používán právě pro trestnou činnost phishingu a pharmingu. Nyní je použit pro stažení programu zvaný FileCoder, který v počítači zašifruje soubory a zamkne obrazovku a zobrazí na ní výzvu k zaplacení výkupného.[63]

3.3.6 Padělání

Trestní zákoník obsahuje ustanovení o padělání a pozměnění peněz v § 233, padělání a pozměňování známek v § 246, padělání a pozměnění předmětů k označení zboží pro daňové účely a předmětů dokazujících splnění poplatkové povinnosti v § 245 a padělání a pozměnění veřejné listiny v § 348. K padělání těchto peněz, dokumentů a veřejných listin zpravidla slouží moderní výpočetní technika a příslušný software. Trestní zákoník zařazuje počítačový program mezi padělatelské náčiní. (§ 236 TZ), kdy se takovýmto zařízením k padělání a pozměnění rozumí jakýkoli přístroj nebo jiné technické zařízení přizpůsobené pachatelem k padělání a pozměnění peněz, veřejných listin a jiných dokumentů. Sankcí za takovéto jednání je odnětí svobody, zákaz činnosti nebo propadnutím věci nebo jiné majetkové hodnoty a to opět dle naplnění jednotlivých skutkových podstat a mírou závažnosti trestné činnosti.

---

[62] MATĚJKA, Michal. 2002. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, x, 106 s. ISBN 80-722-6419-2.

[63] ČTK. *Obávaný počítačový vir je zpět. Tentokrát napadené vydírá* [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://zpravy.aktualne.cz/finance/obavany-pocitacovy-vir-je-zpet-tentokrat-napadene-vydira/r ~51cdf416e44711e4bc74002590604f2e.

3.4 Trestné činy související s obsahem

3.4.1 Závadná pornografie

Úpravu šíření pornografie nalezneme v § 191 až § 193 TZ. Jedná se o trestné činy šíření pornografie, výroba a jiné nakládání s dětskou pornografií a zneužití dítěte k výrobě pornografie. Tento trestný čin je postihován odnětím svobody, nebo propadnutím majetku.

3.4.2 Extremismus

Pojmem extremismus lze označovat ideologické postoje, které vybočují z ústavních nebo zákonných norem a útočí proti základním demokratickým principům.[64] V této oblasti kriminality je internet pomocným prostředkem, který výše zmíněné skupiny využívají k tomu, aby se zviditelnily, zpřístupnily a rozšířily své názory a také je užíván na komunikaci uvnitř těchto skupin, nejčastěji při organizování a pořádání akcí.

Extremismus je celosvětovým problémem, právní úpravu v Úmluvě o lidských právech však nenajdeme. V našem právu se opět obrátíme na TZ a to konkrétně na § 311, kde je upraven trestný čin teroristického útoku; § 352, který upravuje násilí proti skupině obyvatelů a proti jednotlivci; v § 355 jde poté o hanobení národa, rasy, etnické nebo jiné skupiny osob; v § 356, najdeme úpravu podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod; § 403 obsahuje ustanovení o založení, podpoře a propagaci hnutí směřujícího k potlačení práv a svobod člověka; § 404 poté projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka; § 405, popírání, zpochybňování, schvalování a ospravedlňování genocidy; § 407, podněcování útočné války. Toto jednání je postihováno dle naplnění jednotlivých skutkových podstat trestné činnosti, nejčastěji odnětím svobody a zákazem činnosti.

[64] POLICIE CR. *Co je extremismus?* [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://www.policie.cz/clanek/prevence-informace-o -extremismu-co-je-extremismus.aspx.

3.5 Trestné činy související s porušováním autorského práva a souvisejících práv

3.5.1 Počítačové pirátství, Warez, P2P

Počítačové pirátství

Počítačové pirátství je jednou z mnoha forem počítačové kriminality, k samotné protiprávní činnosti je využíván právě počítač. Tento pojem zahrnuje veškerou protiprávní činnost, která je realizována pomocí počítačové techniky a jejím důsledkem je porušování práv k duševnímu vlastnictví. Zjednodušeně pod něj můžeme podřadit kopírování, distribuci a používání autorsky chráněného softwaru, filmů, hudby nebo elektronických knih bez povolení jejich vlastníka. V současné době o pirátství hovoříme nejčastěji ve spojitosti s filmovými a hudebními díly a počítačovými programy jako o filmovém, hudebním a softwarovém pirátství.[65]

„Kdo neoprávněně, tedy bez souhlasu nositele autorského práva a práv souvisejících s právem autorským, nakládá s dílem, uměleckým výkonem, zvukově či obrazově - zvukovým záznamem nebo vysíláním rozhlasu nebo televize, které jsou předmětem ochrany podle autorského zákona, dopouští se porušení autorského práva a práv s ním souvisejících a měl by si být vědom nepříznivých důsledků, které pro něho z jeho jednání vyplývají.“[66]

V důsledku porušování autorského práva odlišujeme tři základní typy odpovědnosti, a to odpovědnost občanskoprávní, trestněprávní a přestupkovou.

Občanskoprávní odpovědnost je upravena v § 40 zákona č. 121/2000 Sb. Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (dále jen autorský zákon), který vymezuje, čeho se může autor domáhat v případě porušení jeho autorského práva, jde především o určení autorství, zákazu ohrožení svého práva, poskytnutí přiměřeného zadostiučinění, odstranění následků zásahu do autorského práva.

V rovině trestněprávní se jedná o § 270 TZ, který upravuje porušení autorského práva, práv souvisejících s právem autorským a práv k databázi, kdy za tento trestný čin hrozí pachateli pokuta až 150 000,- Kč, trest odnětí svobody až na dva roky; případně šest

[65] ČPU. *Co je pirátství* [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://www.stoppiratstvi.cz/cs/o-piratstvi/co-je-piratstvi.shtml.

[66] ČPU. *Odpovědnost za porušení autorského práva* [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://www.cpufilm.cz/new/www/odpovednost.html.

měsíců až pět let, získal-li pachatel činem značný prospěch nebo dopustil-li se takového činu ve značném rozsahu, a v případě získání prospěchu velkého rozsahu nebo způsobení škody velkého rozsahu tři až osm let, peněžitý trest, trest propadnutí věci – (počítače, kamery, kopií filmu).

V roce 2012 byla zavřena pirátská stránka Kinotip.cz. Tato stránka zpřístupňovala desetitisíce filmů a seriálů a to i takových, které ještě běžely v kinech nebo nebyly v České republice vysílány. Provozovatelé stránek za necelé dva roky si přišli na částku okolo dvou milionů korun. Tento server zpřístupňoval pirátské kopie filmů a seriálů umístěné na serveru Megaupload.[67]

Warez

Hlavní podstata warezu spočívá v nelegálním šíření a zpřístupnění autorsky chráněných děl tak, aby je mohli nelegálně a bezplatně využívat i ostatní.[68] Rozdíl mezi pirátstvím a warezem je v získání finančního prospěchu, zatímco u počítačových pirátů jde o šíření děl za účelem získat finanční prostředky, u warezu jde o sdílení zdarma.

V případě warezu je třeba odlišovat, zda se jedná o osoby, jež neoprávněně autorská díla třetím osobám poskytují a osoby, které takto neoprávněně šířená autorská díla přijímají. V České republice je kopírování (tedy i stahování) autorských děl (nikoli však softwaru či databází) pro vlastní (osobní) potřebu zcela legální. Samotné šíření takových děl bez povolení autora je však nelegální a je postihnuto v souladu s § 270 TZ trestem odnětí svobody až na dvě léta (nebo na šest měsíců až pět let pokud tak pachatel konal ve značném rozsahu) nebo peněžitým trestem nebo propadnutím věci.

Kokrétním případem kybernetické trestné činnosti tohoto typu se zabývala policie České republiky v roce 2013. Jednalo se o pachatele, který uploadoval na filehostingové servery tisíce neoprávněných kopií filmů a na warezových fórech potom zveřejňoval odkazy na nelegální kopie. Pachatel si přišel přibližně na 110 tisíc korun za čtyři roky. Poškozeným způsobil odhadovanou škodu okolo 52 miliónů korun.[69]

P2P

P2P síť (Peer-to-peer, neboli klient-klient) je nejrozšířenějším způsobem šíření

[67] ČPU. *Archiv tiskových zpráv* [online]. 2012. [cit. 2015-05-14]. Dostupné z: http://cpufilm.cz/press.html.

[68] JIROVSKÝ, Václav. 2007. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 284 s. ISBN 978-80-247-1561-2.

[69] ČPU. *Archiv tiskových zpráv* [online]. 2012. [cit. 2015-05-14]. Dostupné z: http://cpufilm.cz/press.html.

warezu, tyto sítě můžeme označit jako sítě výměnné, které umožňují šířit a zpřístupňovat obsah mezi uživateli těchto sítí. Nejčastěji se jedná o šíření hudebních nahrávek, filmů a softwarů. Pokud je tento obsah šířen bez souhlasu autora, jedná se o porušení autorského práva a postih je zde v souladu s tímto zákonem a § 270 TZ, tedy trestem odnětí svobody nebo peněžitým trestem.

Celosvětově proslulým případem šíření nelegálního obsahu na internetu je bezesporu případ kolem skupiny The Pirate Bay neboli Pirátské zátoky. Tento případ dosáhl takového rozměru, že mu bude věnována následující podkapitola.

Fenomén The Pirate Bay

Za počátek vzniku The Pirate Bay (TPB) lze považovat klient Napster, což byl v podstatě katalog s MP3 nahrávkami, které si mezi sebou sdíleli lidé prostřednictvím P2P sítě. V roce 2003 Napster na nátlak autorských svazů zanikl. Což mělo za následek, že místo Napsteru začalo vznikat ohromné množství nových P2P systémů. Mezi nimiž začal vznikat i jeden v současnosti nejznámější BitTorrent.

Aby mohlo docházet ke sdílení torrentů (souborů s příponou .torrent) je potřeba tzv. trackerů neboli serverů, které zprostředkují prvotní spojení mezi uživateli a nabízejí katalog s obsahem. Takovýto tracker si vytvořili i Švédové, kteří si chtěli sdílet hudbu, filmy a software ve skandinávském regionu. Myšlenky se chopilo uskupení Piratbyran, které se 15. září 2003 transformovalo do TPB v čele se zakladateli Peter Sunde, Fredrik Neij a Gottfried Svartholm.

Po otevření Pirátské zátoky se brzy ukázalo, že její zájemci netvoří pouze Skandinávci, ale lidé z celého světa. Proto byl web následně přeložen do několika jazyků.

Protože Pirátská zátoka nevznikla za účelem zisku, ale spíše jako názorová iniciativa, položila základy švédské politické straně Piratpartiet. Tato strana se stala základem pro vznik dalších pirátských stran po celé Evropě.

V roce 2006 po neúspěšné apelaci úřadů na vymazání obsahu ze serveru TPB, došlo k razii ve švédském datovém centru, kde byla zabavena veškerá technika pirátské zátoky. Dalo se předpokládat, že vše skončí jako již zmiňovaný případ Napster, ale opak se stal pravdou. TPB po pouhých třech dnech od zabavení spustilo stránky na nových serverech na jiném místě a jejich popularita a hlavně návštěvnost stránek exponenciálně rostla. Takový efekt se v budoucnu stal více krát. Vždy když úřady zakročily, proti pirátům zvedla se vlna odporu, psaly o tom média a na webové stránky přicházejí lidé, kteří o TPB neměli

nejmenší tušení.

V následujících letech se spustila smršť žalob od hudebních a filmových vydavatelství proti TPB a vyvrcholila v roce 2009 soudem s jejími zakladateli. Ti byli odsouzeni k ročnímu vězení a pokutě 46 miliónů švédských korun. Ani toto ovšem nebyl důvod k ukončení provozu pirátské zátoky a ta se z trackeru proměnila pouze na torrentový katalog.

Autorské svazy se ovšem také nevzdaly a začaly nabádat jednotlivé země k omezení přístupu k serverům TPB. A tak se TPB z domén v USA tedy org. a com. přesunuly na švédskou doménu se., ale ani zde nevydrželi dlouho a TPB se přesouvalo dál mezi doménami států jako je Island, Grónsko nebo Svatý Martin.[70]

V roce 2012 učinila TPB krok jak se vyhnout odpovědnosti za porušování zákona a na svém serveru začali používat namísto torrentů tzv. magnet linky. Ty nepotřebují pro své fungování koordinaci z jednoho centrálního místa, ale fungují nezávisle na tom, odkud byly staženy. Přenáší se tak zodpovědnost za sdílení na samotné uživatele, kteří mezi sebou sdílí data.[71]

Dalším krokem TPB byl přesun provozování webových stránek z vlastních serverů do cloudu, tedy do virtuálních strojů poskytovatelů cloudových služeb. Samotní provozovatelé ani nevědí, že na jejich serverech TPB běží a v podstatě ani nemají možnost to zjistit.[72]

Dá se říci, že TPB dokonale využívá nové technologie k páchání trestné činnosti a předbíhá tak samotnou tvorbu norem a možnost postihovat trestnou činnost v kyberprostoru. V současné době TPB opět běží na stránkách se švédskou doménou. Stále je tedy možné si stáhnout software, hudbu nebo světový film, který v České republice ještě ani nedorazil do kin.

3.5.2 Cybersquatting - doménové pirátství

Cybersquatting je označení pro doménové spekulantství. Jedná se o zaregistrování a užívání domény na úkor obchodní značky, názvu nebo jména osoby. Jeho snahou je

[70] ČÍŽEK, Jakub. *Deset let Pirátské zátoky: Hollywood nemůže vyhrát* [online]. 2013. [cit. 2015-05-14]. Dostupné z: http://www.zive.cz/clanky/deset-let-piratske-zatoky-hollywood-nemuze-vyhrat/sc-3 -a -168689/default.aspx.

[71] MIKLICA, Tomáš. *The Pirate Bay se zbavuje odpovědnosti. Začíná éra magnetů* [online]. 2012. [cit. 2015-05-14]. Dostupné z: http://www.cnews.cz/pirate-bay-se-zbavuje-odpovednosti-zacina-era-magnetu.

[72] FIALA, Lukáš. *The Pirate Bay se stěhuje do cloudu, stránka je opět odolnější vůči raziím* [online]. 2012. [cit. 2015-05-14]. Dostupné z: http://www.cnews.cz/pirate-bay-se-stehuje-do-cloudu-stranka-je-opet-odolnejsi-vuci-raziim.

dosažení zisku prodejem domény osobě, proti níž je vedeno spekulantství nebo konkurenčním nekalosoutěžním jednáním, především parazitováním na pověsti.[73]

Spory z doménového pirátství jsou řešeny většinou na soukromoprávní úrovni. Tyto škodlivé činnosti jsou následně vyhodnoceny jako nekalosoutěžní jednání, nebo také porušení práva z ochranné známky. Dle § 248 TZ můžeme takovéto jednání podřadit pod skutkovou podstatu trestného činu porušení předpisů o pravidlech hospodářské soutěže podle a porušení práv k ochranné známce a jiným označením podle § 268 TZ. Takovéto jednání je sankcionováno zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty, odnětím svobody v délce až pěti let nebo peněžitým trestem.

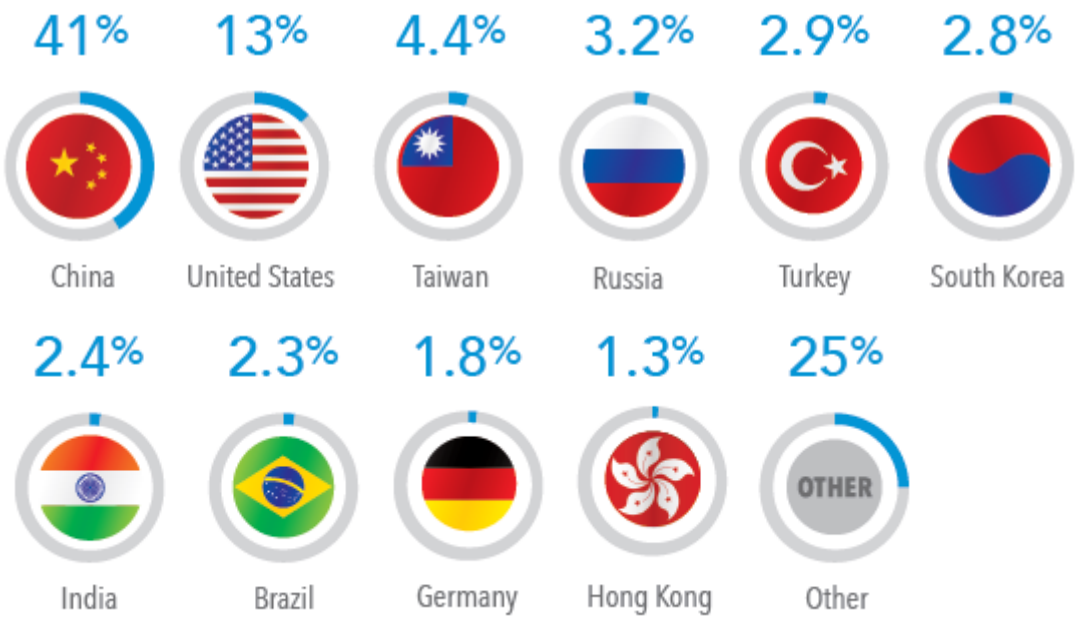
[73] JANSA, Lukáš. *Cybersquatting a jeho podoby* [online]. 2008. [cit. 2015-05-14]. Dostupné z: http://www.pravoit.cz/article/cybersquatting-a -jeho-podoby.

4 Mezinárodní legislativa pro kybernetickou trestnou činnost

4.1 Mezinárodní kyberkriminalita

Na kybernetické útoky je potřeba adekvátně reagovat. O to se snaží většina vyspělých států. Jejich úsilí je však omezeno státními hranicemi. Jediným efektivním způsobem, kterým lze konflikt omezené jurisdikce a neomezeného kyberprostoru překonat, je společný a koordinovaný postup.[74] Tato kapitola je tedy věnována mezinárodním organizacím, institucím a jejich aktivitám vztahující se k problematice kybernetické trestné činnosti.

V současné době se na globálních kybernetických incidentech velkou měrou podílí Čína, která je zemí původu největšího počtu kybernetických útoků, což ilustruje následující obrázek.



Obrázek 1 Podíly zemí na kybernetických útocích

Zdroj: [1]

Podle studie americké společnosti Akamai z března roku 2015 byl ke čtvrtému čtvrtletí roku 2014 evidován největší počet kybernetických útoků právě z Číny. Ta je na

[74] GŘIVNA, Tomáš, et al. Český právní řád a ochrana kyberprostoru: vybrané problémy. Praha: Karolinium, 2008. 140 s. ISBN 978-80-246-1703-9.

přední příčce s ohromným náskokem před druhými Spojenými státy. Z evropských zemí se do tohoto žebříčku dostalo pouze Německo s necelým dvouprocentním podílem.

4.2 Mezinárodní instituce

Tato podkapitola obsahuje výčet mezinárodních organizací a legislativních dokumentů vztahujících se ke kybernetické trestné činnosti. Vybrány byly nejdůležitější mezinárodní organizace se vztahem k České republice a skupina G7. Mezi aktuální priority v oblasti legislativní a organizační spolupráce na nadnárodní úrovni patří především:[75]

- Potírání nelegálního obsahu na internetu.
- Potírání tzv. „nechtěného" obsahu na internetu – zejména spam.
- Technologická spolupráce v boji proti kybernetickým incidentům.
- Prevence hospodářských dopadů kybernetických incidentů.
- Ochrana kritické infrastruktury před kybernetickými incidenty.

4.2.1 Organizace spojených národů

Oblasti ochrany kyberprostoru se v rámci OSN věnuje především Rada bezpečnosti a také Hospodářská a sociální rada. Aktivita OSN v oblasti počítačové kriminality je oproti ostatním organizacím téměř zanedbatelná. Pro boj s kybernetickou trestnou činností lze jmenovat následující rezoluce:

1. Rezoluce o boji se zneužíváním informačních technologií z 22. 1. 2001 (A /RES/55/63). Vyzývá státy, aby jejich zákony a praxe eliminovaly bezpečná útočiště pro ty, kteří trestně zneužijí informační technologie. Dále mimo jiné říka, že právní systémy států by měli chránit důvěrnost, integritu a dostupnost dat před neoprávněným poškozením a zajistit penalizaci za jejich trestní zneužití.[76]
2. Rezoluce o plánu činnosti pro implementaci Vídeňské deklarace o zločinu a trestní spravedlnosti: Výzvy 21. století. Ta stanovuje v části, která se zabývá boji proti high-technology a počítačové kriminalitě, že státy na národní úrovni budou usilovat o to, aby zneužití informačních technologií bylo kriminalizováno.

[75] MVČR. *Mezinárodní spolupráce v boji proti informační kriminalitě* [online]. 2009 [cit. 2015-06-01]. Dostupné z: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-mezinarodni-pdf.aspx.

[76] UN. *Combating the criminal misuse of information technologies* [online]. 2001 [cit. 2015-06-01]. Dostupné z: http://www.itu.int/ITU-D /cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

3. Rezoluce (S /RES/1624) z 14. 9. 2005 zavazuje členské státy k zákazu podněcování páchání aktů terorismu. Její text vyzývá k přijetí opatření jako je zákonem zakázat nabádání terorismu i jeho obhajování, zabránění vzniku útočišť pro osoby podezřelé z teroristických aktivit atp.[77]
4. Rezoluce o mezinárodní spolupráci a oblasti prevence, vyšetřování, stíhání a trestání hospodářských podvodů a trestných činů souvisejících s identitou osob z 26. 7. 2007. Rezoluce podněcuje státy, aby novelizovaly právní předpisy týkající se trestné činnosti nedovoleného získání, kopírování, padělání a zneužití dokumentů, které identifikují osoby.[78]

4.2.2 Rada Evropy

Rada Evropy se začala zabývat problematikou kybernetické trestné činnosti již v roce 1989. Tehdy publikovala studii[79] obsahující pokyny pro tvorbu národní legislativy a také doporučení (Doporučení č. 9 / 1989) pro úpravy a vytváření nových zákonů jednotlivých států, které kriminalizují trestnou činnost prostřednictvím počítačových sítí. V roce 1995 vydala další studii, obsahující principy týkající se trestně právního postupu souvisejícího s informačními technologiemi. Roku 1997 byla ustanovena komise expertů na kybernetické zločiny.[80] Po čtyřleté práci expertů z USA, Kanady, Japonska a dalších se stala výsledkem Úmluva o kybernetické kriminalitě. Ta byla přijata dne 8. listopadu 2001 a otevřena k podpisu v Budapešti dne 23. listopadu 2001. V platnost vstoupila dne 1. července 2004. Ke dni 9. listopadu 2008 Úmluvu podepsalo 45 států, z nichž ji ratifikovalo jen 23.[81] Česká republika ratifikovala Úmluvu až v srpnu roku 2013.

---

[77] UN. *Resolution 1624 (2005)* [online]. 2005 [cit. 2015-06-01]. Dostupné z: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/510/52/PDF/N0551052.pdf?OpenElement.

[78] COE. *International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identityrelated crime* [online]. 2007 [cit. 2015-06-01]. Dostupné z: http://www.un.org/en/ecosoc/docs/2007/resolution%202007-20.pdf.

[79] COE. *Computer-related crime: recommendation no. R. (89) 9 on computer-related crime and final report of the European Committee on Crime Problems*. Croton, N. Y. : Manhattan Pub. Co. [distributor], 1990, 114 p. ISBN 92-871-1792-6.

[80] MVČR. *Mezinárodní spolupráce v boji proti informační kriminalitě* [online]. 2009 [cit. 2015-06-01]. Dostupné z: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-mezinarodni-pdf.aspx.

[81] GŘIVNA, Tomáš, et al. Český právní řád a ochrana kyberprostoru: vybrané problémy. Praha: Karolinium, 2008. 140 s. ISBN 978-80-246-1703-9.

Úmluva o počítačové kriminalitě[82]

Úmluva se zabývá definicemi některých trestných činů v kyberprostoru, obsahuje závazky k přijetí procesních opatření nezbytných k zajištění důkazů, odhalení a potrestání pachatelů a také závazky v oblasti mezinárodní spolupráce.[83] Úmluva obsahuje preambuli a 48 článků rozdělených do čtyř kapitol.

Kapitola 1. obsahuje definice pojmů jako počítačový systém, počítačová data, poskytovatel služby nebo provozní data.

Kapitola 2. je zaměřena na opatření, která mají být přijata na vnitrostátní úrovni. V první části se pro oblast kybernetické trestné činnosti zabývá trestním právem hmotným. Tato část je rozdělena do pěti oddílů konkrétně obsahující:

- Oddíl 1. - Trestné činy proti důvěryhodnosti, integritě a použitelnosti počítačových systémů. Zde jsou v jednotlivých článcích vypsány trestné činy jako nezákonný přístup, nezákonný odposlech, zasahování do dat, zasahování do systému a zneužívání zařízení. Pro tyto činnosti musí státy přijmout taková legislativní opatření, aby podle vnitrostátních předpisů byly trestným činem. (Stejně tak platí i pro následující oddíly.)
- Oddíl 2. - Trestné činy související s počítačem. Oddíl obsahuje dva články zabývající se počítačovým padělám, a počítačovým podvodem.
- Oddíl 3. - Trestné činy související s obsahem. Oddíl se zabývá trestnou činností související s dětskou pornografií.
- Oddíl 4. - Trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským.
- Oddíl 5. - Další formy odpovědnosti a trestů. Články 11, 12 a 13 tohoto oddílu se zaměřují na pokus trestného činu a účastenství, odpovědnost právnických osob, tresty a opatření.

Následující část kapitoly druhé je zaměřena na právo procesní a je rozdělena do následujících oddílů:

- Oddíl 1. - Obecná ustanovení. V článku 14. je popsán rozsah procesních ustanovení a článek 15. obsahuje podmínky a záruky.

[82] COE. *Convention on Cybercrime* [online]. 2001 [cit. 2015-06-02]. Dostupné z: www.psp.cz/sqw/text/orig2.sqw?idd=79483.

[83] GŘIVNA, Tomáš; POLČÁK, Radim. Kybernetika a právo. 1. vydání Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7 -4.

- »Oddíl 2. - Urychlené uchování uložených počítačových dat. Oddíl se zabývá opatřeními, která umožní příslušným orgánům urychlené uchování uložených počítačových dat, a také urychlené zachování a urychlené, částečné zpřístupnění provozních dat.
- »Oddíl 3. - Příkaz k předložení. Podle tohoto oddílu musí každá strana přijmout taková opatření, aby umožnila příslušným orgánům nařídit předložení specifikovaných počítačových dat.
- »Oddíl 4. - Prohlídka a zajištění uložených počítačových dat. V článku 19. tohoto oddílu je uvedeno umožnění příslušným orgánům prohledat či získat přístup k počítačovému systému nebo k médiu pro ukládání počítačových dat.
- »Oddíl 5. - Shromažďování počítačových dat v reálném čase. Oddíl se zabývá shromažďováním provozních dat a odposlechem obsahových dat.

Ve třetí části kapitoly jsou v článku 22 vyzývány státy, aby přijímaly opatření nezbytná k tomu, aby stanovila soudní pravomoc ve vztahu k jakémukoli trestnému činu, které jsou uvedeny v kapitole první této Úmluvy.

Kapitola 3. se zabývá mezinárodní spoluprací v oblasti kybernetické trestné činnosti. V první části jsou uvedeny obecné zásady mezinárodní spolupráce, do nichž spadají následující oddíly:

- »Oddíl 1. - Obecné zásady týkající se mezinárodní spolupráce. Na základě ustanovení této kapitoly mají státy vzájemně spolupracovat v trestních věcech.
- »Oddíl 2. - Zásady týkající se vydávání. Článek 24 obsažen v tomto oddílu se zaměřuje na vydávání osob mezi státy pro trestné činy stanovené v kapitole první.
- »Oddíl 3. - Obecné zásady týkající se vzájemné pomoci.
- »Oddíl 4. - Postupy vztahující se na žádosti o vzájemnou pomoc při neexistenci příslušných mezinárodních dohod. Oddíl popisuje postup v případech, kdy neexistuje smlouva o vzájemné pomoci nebo ujednání na základě jednotných právních předpisů mezi stranami.

Další částí třetí kapitoly jsou zvláštní ustanovení. Ta obsahují článek 29 - urychlené uchování uložených počítačových dat, článek 30 - urychlené sdělení uchovaných provozních dat, článek 31 - vzájemná pomoc týkající se přístupu k uloženým, počítačovým datům, článek 33 - vzájemná pomoc týkající se shromažďování provozních dat v reálném čase, 34 - vzájemná pomoc týkající se odposlechu obsahových dat a také článek 35 - 24/7 síť, který

mimo jiné říká, že každá strana musí mít kontaktní místo, jež bude k dispozici 24 hodin denně, 7 dnů v týdnu, aby bylo možné poskytovat okamžitou pomoc pro účely vyšetřování nebo řízení ohledně trestných činů spojených s počítačovými systémy a daty.

Kapitola 4. se věnuje závěrečným ustanovením jako podpis a vstup Úmluvy v platnost, přístup státu k Úmluvě, územní působnost Úmluvy, její účinky. Dále prohlášení, federální doložku, výhrady, dodatky, urovnání sporů, porady stran, výpověď a oznámení.

Ostatní dokumenty Rady Evropy

Vedle Úmluvy se kybernetické trestné činnosti věnují i další dokumenty:

- Dodatkový protokol o kriminalizaci činů rasistické a xenofobní povahy, spáchaných prostřednictvím počítačového systému (ETS 189)
- Doporučení Rady ministrů č. 13 z roku 1995, zabývající se trestním právem procesním v oblasti informačních technologií
- Doporučení Rady ministrů č. 5 z roku 1999, týkající se ochrany soukromí na internetu.

4.2.3 Evropská unie

V rámci Evropské unie bylo vydáno množství dokumentů souvisejících s problematikou kybernetické trestné činnosti. Lze jmenovat:

- Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Směrnice se vztahuje na údaje zpracovávané automaticky, tedy například počítačové databáze zákazníků, a také na tradiční lístkové rejstříky.[84]
- Směrnice Evropského parlamentu a Rady 97/66/ES ze dne 15. prosince 1997, vztahující se k nakládání s osobními údaji a k ochraně soukromí v telekomunikačním sektoru.[85]
- Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v telekomunikačním sektoru.

[84] EU. *Směrnice Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů* [online]. 1995 [cit. 2015-06-01]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:31995L0046.

[85] GŘIVNA, Tomáš, et al. Český právní řád a ochrana kyberprostoru: vybrané problémy. Praha: Karolinium, 2008. 140 s. ISBN 978-80-246-1703-9.

Směrnice nahradila dvě výše uvedené. Stanovuje pravidla pro zpracování a provozních údajů a lokalizačních údajů vytvářených při používání služeb elektronických komunikací. Problémem tohoto předpisu je, že vnitrostátní předpisy členských zemí se v oblasti uchovávání údajů pro účely předcházení, vyšetřování, odhalování a stíhání trestných činů značně liší. [86]

- Směrnice 2006/24/EC ze dne 15. 3. 2006 o uchování údajů vytvářených nebo zpracovaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí slouží právě pro harmonizaci vnitrostátních předpisů členských států. Členské státy mají zajistit, aby se provozní a lokalizační údaje o právnických a fyzických osobách a související údaje, které jsou nezbytné k identifikaci účastníka, uchovávaly po dobu nejméně šesti měsíců a nejvýše dvou let ode dne komunikace.[87]
- Dalším legislativním dokumentem Evropské unie v této oblasti je Rozhodnutí Rady 2005/222/SVV ze dne 24. 2. 2005 o útocích proti informačním systémům. Dokument má za cíl harmonizovat trestněprávní předpisy členských zemí v oblasti útoků proti informačním systémům.[88] Ukázalo se totiž, že existují rozdíly v právních předpisech členských států a významně se tak ztěžuje boj proti organizované kybernetické trestné činnosti, a také se komplikuje policejní a soudní spolupráce.[89]

Evropská unie vydala mnoho dalších legislativních dokumentů v oblasti kybernetické trestné činnosti. Za zmínku stojí například:

- Rozhodnutí Evropského parlamentu ze dne 19. května 2000, k legislativní akci proti zločinu za použití vyspělých technologií.
- Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu.
- Rozhodnutí Rady ze dne 29. května 2000, o boji s dětskou pornografií na internetu.

---

[86] EU. *Směrnice o soukromí a elektronických komunikacích* [online]. 2002 [cit. 2015-06-01]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:cs:HTML.

[87] EU. *Directive of the european parliament and of the council* [online]. 2006 [cit. 2015-06-01]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024.

[88] EU. *Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům* [online]. 2005 [cit. 2015-06-02]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:CS:PDF.

[89] GŘIVNA, Tomáš, et al. Český právní řád a ochrana kyberprostoru: vybrané problémy. Praha: Karolinium, 2008. 140 s. ISBN 978-80-246-1703-9.

» Doporučení Rady ze dne 25. června 2001, o kontaktních bodech 24hodinové služby pro boj s kriminalitou za použití vyspělých technologií.

» Rámcové rozhodnutí Rady 2002/465/JHA ze dne 13 července 2002, o společných vyšetřovacích týmech.

4.2.4 Organizace pro hospodářskou spolupráci a rozvoj

V rámci organizace OECD se oblasti kybernetické trestné činnosti věnuje Výbor pro informační, počítačovou a komunikační politiku.

Již v roce 1986 Organizace pro hospodářskou spolupráci přijala doporučení, které se zabývá manipulací s počítačovými systémy padělání pomocí počítače, zasahování do počítačového systému nebo telekomunikačnímu systému.[90]

V roce 2002 byl vydán dokument Pokyny pro bezpečnost informačních systémů a sítí: Směrem ke kultuře bezpečnosti.[91] Dokument vyzývá členské země, aby zřídily nové nebo posílily existující zásady, praktiky, opatření a postupy prostřednictvím přijetí tzv. kultury bezpečnosti. Aby koordinovaly postupy a spolupracovaly na národní i mezinárodní úrovni a také aby podávaly každých pět let zprávu o plnění aktivit souvisejících s mezinárodní spoluprácí, vztahujících se k bezpečnosti informačních systémů a sítí. Dokument obsahuje devět principů, kterými by se měly členské státy řídit.

1. Uvědomění - účastníci by si měli být vědomi potřeby zabezpečení informačních systémů a sítí.
2. Odpovědnost - všichni účastníci jsou zodpovědní za bezpečnost informačních systémů a sítí.
3. Schopnost reagovat - účastníci by měli jednat včas a kooperativním způsobem tak, aby byli schopni zabránit, odhalit a reagovat na bezpečnostní incidenty.
4. Etika - účastníci by měli respektovat legitimní zájmy ostatních.
5. Demokracie - bezpečnost informačních systémů a sítí by měla být kompatibilní se základními hodnotami demokratické společnosti.
6. Hodnocení rizik - účastníci by měli provádět hodnocení rizik.
7. Návrh a implementace zabezpečení - účastníci by měli začlenit bezpečnost jako základní prvek informačních systémů a sítí.

---

[90] GŘIVNA, Tomáš, et al. Český právní řád a ochrana kyberprostoru: vybrané problémy. Praha: Karolinium, 2008. 140 s. ISBN 978-80-246-1703-9.

[91] OECD. *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* [online]. 2002 [cit. 2015-06-01]. Dostupné z: http://www.oecd.org/sti/ieconomy/15582260.pdf.

8. Řízení bezpečnosti - účastníci by měli přijmout komplexní přístup k řízení bezpečnosti.
9. Přezkoumávání - účastníci by měli revidovat a přehodnocovat bezpečnost informačních systémů a sítí, a provádět příslušné úpravy bezpečnostní politiky, praktik, opatření a postupů.

V roce 2008 byla přijata deklarace věnující se otázce budoucnosti internetu. V současnosti je pozornost zaměřena na trestné činnosti jako je spamming, krádež identity nebo šíření malwaru.

4.2.5 Severoatlantická obraná aliance

Politika NATO v oblasti kybernetické obrany je realizována prostřednictvím politických, vojenských a technických orgánů NATO, jakož i jednotlivých spojenců.[92] Hlavním orgánem zabývající se kyberneticko-bezpečnostním krizovým řízením je Rada (The North Atlantic Council, NAC). Dalším orgánem pro tuto oblast je Výbor pro kybernetickou obranu (The Cyber Defence Committee), který je podřízený Radě a je zodpovědný za dohled a poradenství spojeneckým zemím. Kybernetické bezpečnosti se věnuje také Výbor pro konzultace, kontrolu a velení (The Consultation, Control and Command Board, NC3). Ten je zodpovědný za poradenství ohledně technických a implementačních aspektů kyberentické obrany.

V září 2014 NATO schválilo na Summitu ve Walesu akční plán, který stanovuje, že kybernetická obrana je součástí hlavní úlohy kolektivní obrany Aliance. Dále potvrzuje, že mezinárodní právo platí pro kyberprostor a zintenzivňuje spolupráci NATO s průmyslem. Hlavní prioritou je ochrana komunikačních systémů vlastněných a provozovaných Aliancí.[93]

4.2.6 Skupina sedmi průmyslově vyspělých států světa

Ministři spravedlnosti a vnitřních věcí G7 (v té době G8, tedy společně s Ruskem) přijali v roce 1997 na summitu deset principů, které shrnují cíle v boji proti high-tech zločinu. Principy byly následně konkretizovány v Akčním plánu pro potírání high-tech zločinu. Mezi principy patří například:

---

[92] NATO. *Cyber security* [online]. 2015 [cit. 2015-06-01]. Dostupné z: http://www.nato.int/cps/en/natohq/topics_78170.htm.

[93] NATO. *Wales Summit Declaration* [online]. 2014 [cit. 2015-06-01]. Dostupné z: http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

- nesmí existovat bezpečné útočiště pro ty, kteří zneužívají informační technologie,
- vyšetřování a trestní řízení v oblasti high-tech zločinu musí být koordinováno mezi všemi zúčastněnými státy bez ohledu na to, kde škoda nastala,
- orgány prosazující právo je třeba k potírání high-tech zločinu dostatečně vyškolit a vybavit,
- vzájemná spolupráce vlád musí zajistit včasný sběr a výměnu důkazů v případech zahrnující high-tech zločin.[94]

[94] MVČR. *Mezinárodní spolupráce v boji proti informační kriminalitě* [online]. 2009 [cit. 2015-06-01]. Dostupné z: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-mezinarodni-pdf.aspx.

5 Ekonomické aspekty kybernetické trestné činnosti

5.1 Globální aspekty

Globální škody způsobené kybernetickou trestnou činností[95] za rok 2014 se odhadují na 400 miliard dolarů. Přičemž konzervativní odhad je 375 miliard a maximální 575 miliard dolarů.[96] Při porovnání se světovým HDP, které činilo v roce 2013 75,6 bilionů dolarů[97] lze celkové ztráty odhadnout na 0, 5 % globálního HDP. Odhad škod zahrnuje také ztráty způsobené krádežemi osobních informací. V roce 2014 bylo zasaženo více než 40 miliónu lidí v USA, 54 miliónů lidí v Turecku, 20 miliónů lidí v Koreji, 16 miliónů lidí v Německu, a více než 20 miliónů lidí v Číně. Známým případem nedávné doby bylo odcizení 1, 2 miliardy uživatelských jmen a hesel, a také 500 miliónů emailových adres ruskými hackery. Pokud se podíváme na firmy, tak v roce 2013 bylo oznámeno americkou vládou, že bylo napadeno na 3000 společností. Dále lze narazit na mnohé zajímavé případy. Například jedna Britská společnost oznámila, že přišla o 1, 3 miliard dolarů jediným útokem. Nebo dalším zajímavým případem bylo odcizení 40 miliónů informací o kreditních kartách.[98]

Je nutné připomenout, že informace poskytované jednotlivými státy a společnostmi nemusí být kompletní. A to především z důvodu, že některé společnosti zatajují informace o kybernetických incidentech z obav o snížení důvěryhodnosti nebo z důvodu, že státy především z rozvojových zemí vůbec tyto data neevidují.

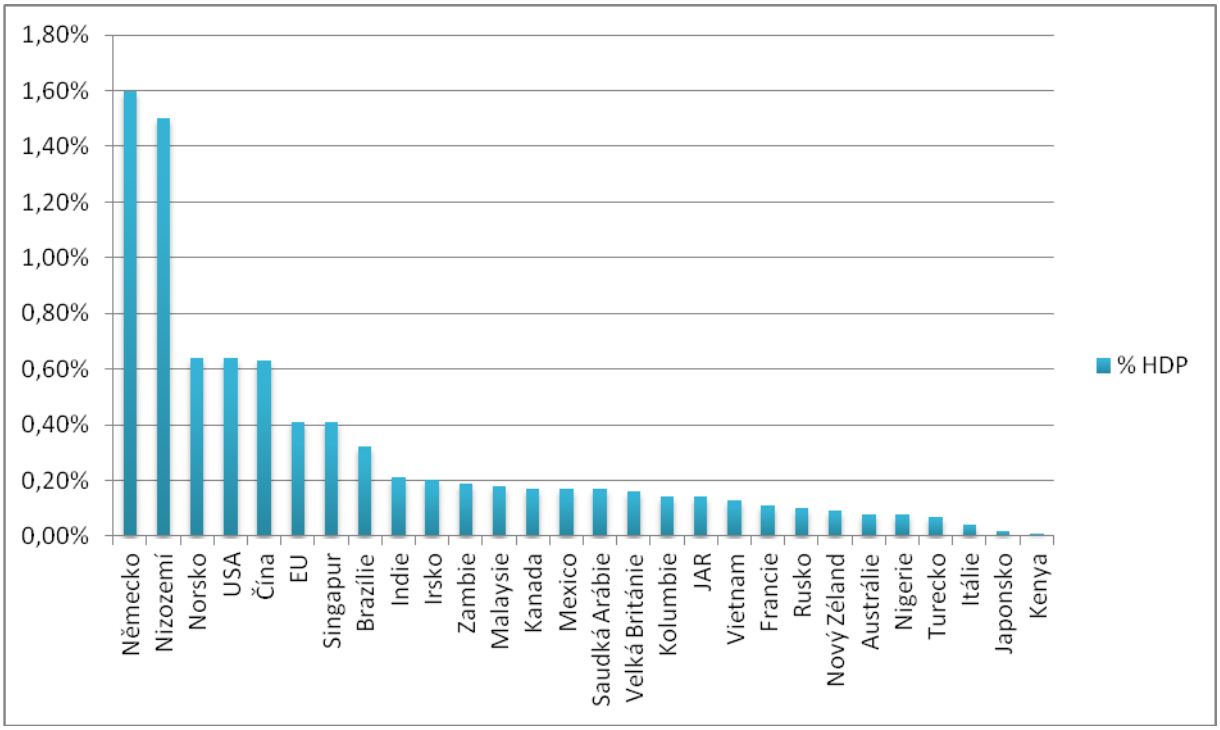
Pokud se budeme zabývat ztrátami způsobenými kybernetickou trestnou činností pro jednotlivé země plus celou EU měřeno v procentu HDP, tak z posledního výzkumu v roce 2014 provedeného společností CSIS (Center for Strategic and International Studies) vyplívá, že první pozici v tomto měření zaujímá Německo, které je následováno Holandskem. Konkrétní data jsou možné vidět na následujícím grafu.

[95] Do odhadu škod jsou započítany náklady vztahující se ke ztrátě duševního vlastnictví, krádeže finančních aktiv, náklady ušlé příležitosti, náklady na zabezpečení a znovuobnovení systému a také na poškození dobré pověsti společností.

[96] CSIS. *Net Losses: Estimating the Global Cost of Cybercrime* [online]. 2014 [cit. 2015-06-05]. Dostupné z: http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

[97] THE WORLD BANK. *Gross domestic product 2013* [online]. 2015 [cit. 2015-06-05]. Dostupné z: http://databank.worldbank.org/data/download/GDP.pdf.

[98] CSIS. *Net Losses: Estimating the Global Cost of Cybercrime* [online]. 2014 [cit. 2015-06-05]. Dostupné z: http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.



Obrázek 2 Grafické zobrazení ztrát způsobených kyberkriminalitou v % HDP, 2014

Zdroj: vlastní zpracování, podle [7]

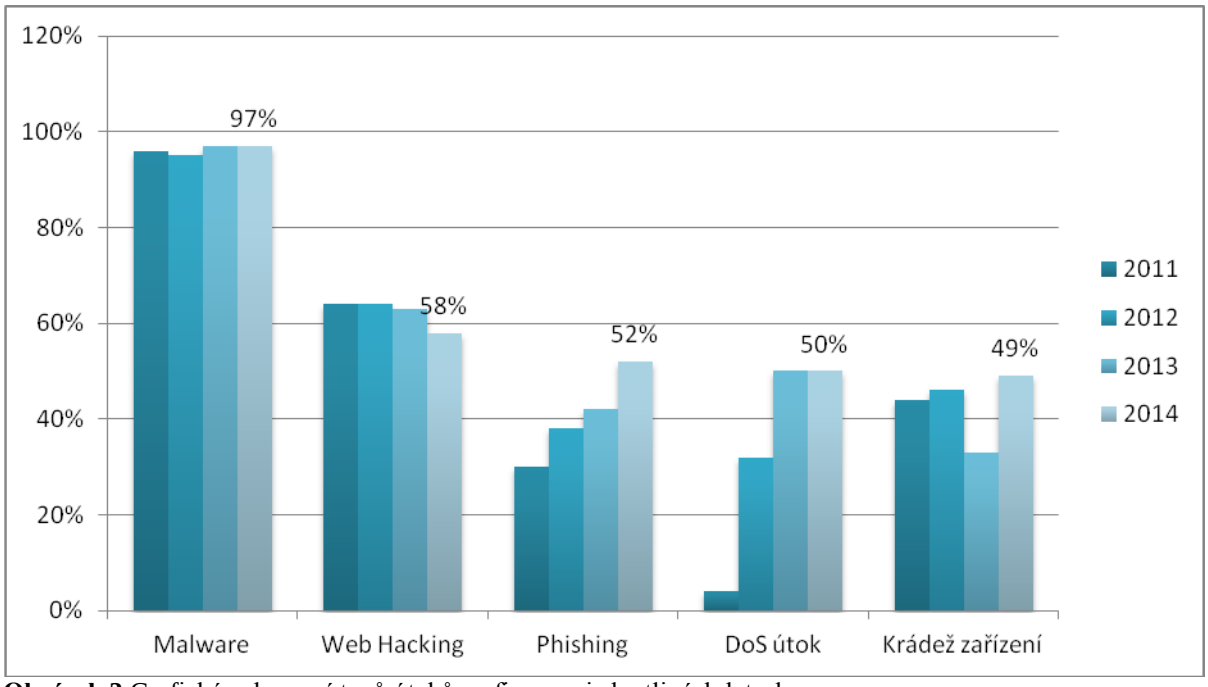
Země, které se potýkají s nejvyššími škodami vlivem kybernetické trestné činnosti, jsou Evropské státy, USA a Čína. Lze říci, že důvodem je nedostatečný, obraný systém, proti kybernetickým útokům všech zemí a společností na světě, proto hackeři raději napadají bohatší země, u kterých mají stejnou práci s proniknutím do systémů organizací a vyšší pravděpodobnost většího výdělku.

Dalším důležitým důvodem v rozdílnosti škod vlivem kybernetické kriminality je to, jaký podíl má tvorba duševního vlastnictví na celkové tvorbě bohatství daného státu. CSIS uvádí, že v zemích kde je tento podíl vyšší jsou vyšší i ztráty, než u zemí, kde se na tvorbě bohatství podílí nejvíce spíše zemědělství či těžební průmysl.

Následující podkapitola je již zaměřena na škody způsobené různými typy kybernetických útoků jednotlivým společnostem z vybraných zemí.

5.2 Náklady na kyberkriminalitu

Náklady na kyberkriminalitu[99] u jednotlivých společností ve vybraných státech se značně liší. Do průzkumu[100] jsou zařazeny pouze velké společnosti s minimálně tisíci zaměstnanci. Pokud se podíváme na konkrétní typy útoků, se kterými měly jednotlivé organizace zkušenost, či jimi byli napadeny, a byla jim způsobena škoda, můžeme pozorovat, že téměř každá firma byla terčem malware útoku. Malwarem se rozumí všechny druhy programů, které nějakým způsobem uživateli škodí. Jsou to například počítačové viry, červi a trojské koně.[101]



Obrázek 3 Grafické zobrazení typů útoků na firmy v jednotlivých letech

Zdroj: vlastní zpracování, podle [46]

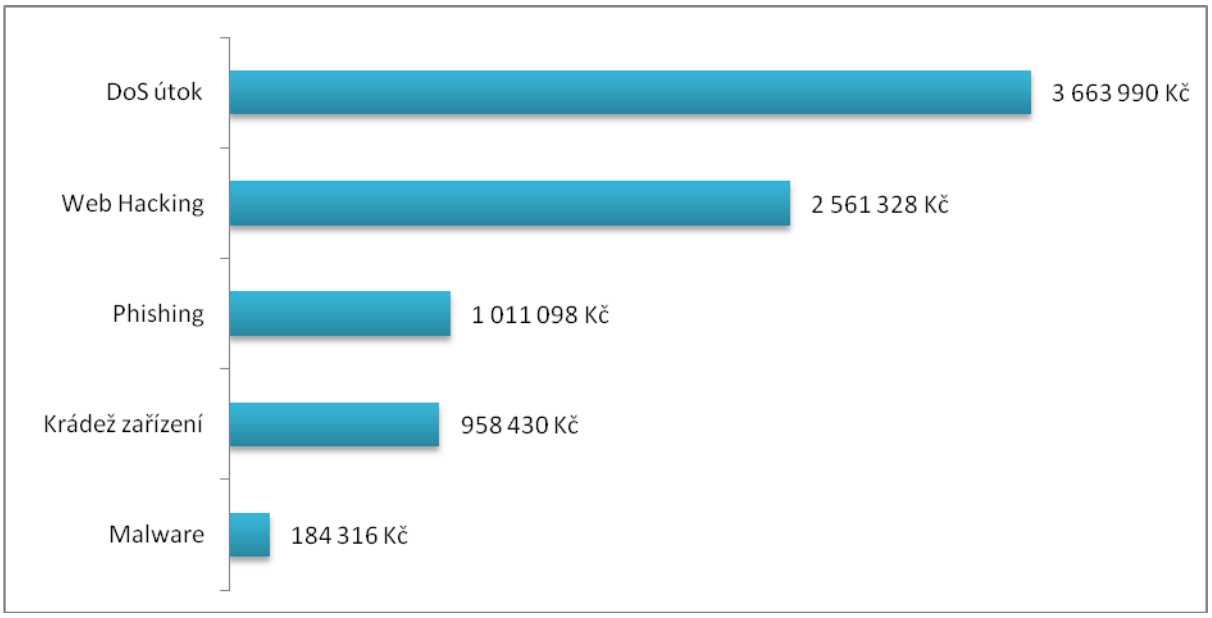
Na grafu 3 pozorujeme, že téměř 100% firem bylo již někdy napadeno malware. Zatímco s hacknutím webových stránek se setkává přibližně 60% firem, a trend je klesající u phishingu nebo DoS útoků pozorujeme markantní nárůst případů. V roce 2011 se s DoS útokem setkala 4 % společností, v roce 2014 to bylo již 50%.

[99] Pod náklady na kyberkriminalitu budeme rozumět krádeže finančních aktiv, náklady na zabezpečení a znovuobnovení systému, náklady související se ztrátou zákazníků.

[100] Provedeným společností Ponemon Institute.

[101] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat.* Vyd. 1. Brno: Computer Press, 2004, ix, 190 s. ISBN 80-251-0106-1.

Průměrné náklady firem v roce 2014[102] na jednotlivé kybernetické incidenty lze vidět na následujícím grafu.



Obrázek 4 Grafické zobrazení průměrných nákladů na jednotlivé typy kybernetických útoků

Zdroj: vlastní zpracování, podle [46]

Nejvyšší škody z uvedených typů útoků způsobují DoS útoky. Průměrné náklady firem spojené s tímto incidentem dosahují téměř 3, 7 mil. Kč.[103] Následují útoky spojené s hacknutím webových stránek, jež poškozují firmy v průměru 2, 5 mil. Kč. Ačkoli se všechny firmy potýkají s malwarem, tak způsobená škoda tímto útokem je oproti DoS útoku přibližně dvacetkrát nižší.

Znepokojivou informaci o stavu kybernetického zabezpečení u jednotlivých společností poskytuje Tabulka 2. Detailní statistiky o stavu zabezpečení jsou uvedeny v příloze A.

Tabulka 2 Frekvence úspěšně provedených kybernetických útoků

	počet organizací	počet úspěšných útoků	počet úspěšných útoků za týden
2012	199	262	1, 3
2013	234	343	1, 4
2014	257	429	1, 7

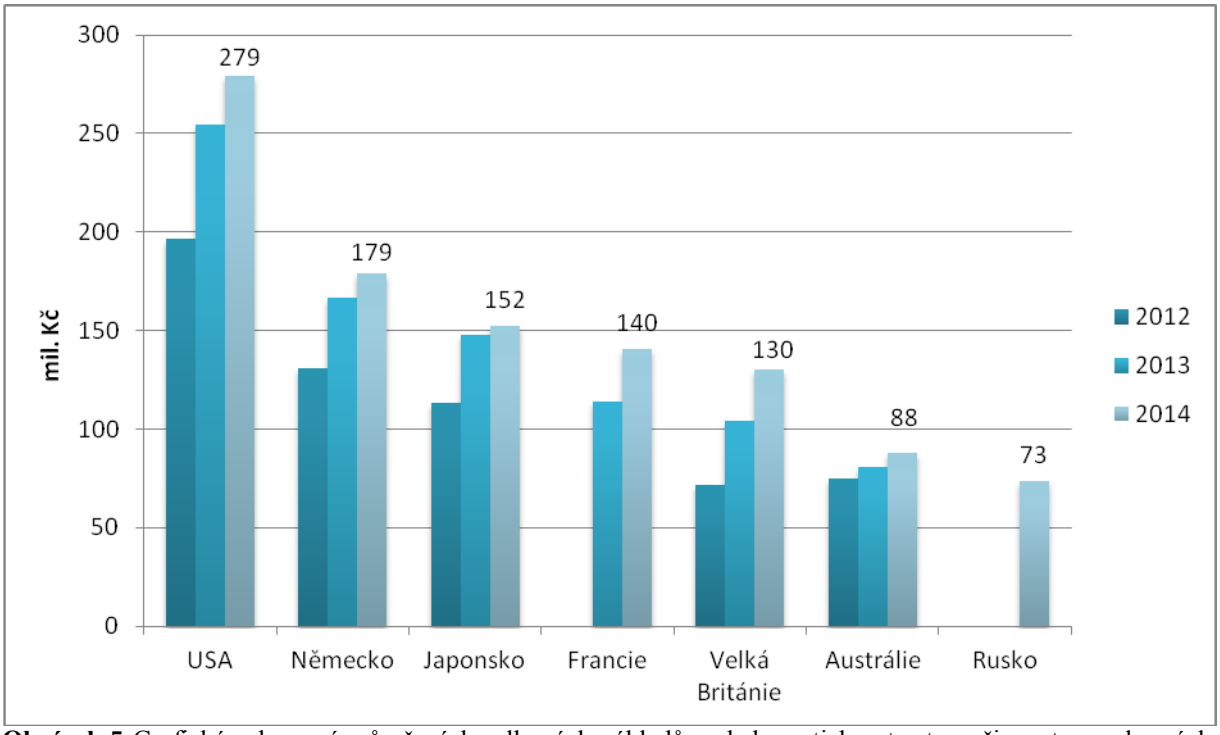
Zdroj: vlastní zpracování, podle [45]

[102] Tedy celkové náklady dělené počtem útoků v daném roce.

[103] Data jsou přepočtena kurzem koruny vůči dolaru, který byl v říjnu 2014 dle kurzovního lístku ČNB přibližně 22 Kč.

V roce 2014 se hackerům podařilo překonat bezpečností systémy firem bezmála dvakrát za týden. Znepokojující je především to, že úspěšnost prolomení bezpečnostních opatření stoupá. Vysvětlením může být zvyšující se sofistikovanost a profesionalita kybernetických útoků, na což firmy nedokážou adekvátně reagovat.

Další část podkapitoly je zaměřena na náklady na kybernetickou trestnou činnost z pohledu vybraných zemí. Přesněji řečeno na náklady organizací sídlící v daných státech, které byly cílem kybernetického útoku. Průměrné celkové náklady na kyberkriminalitu jednotlivých společností ve vybraných zemích v letech 2012 až 2014 lze vidět na obrázku 5.[104] Konkrétní data lze vidět v tabulce v příloze B.



Obrázek 5 Grafické zobrazení průměrných celkových nákladů na kybernetickou trestnou činnost ve vybraných zemích

Zdroj: vlastní zpracování, podle [46]

Spojené státy americké mají v porovnání s ostatními zeměmi nejvyšší způsobené škody. Od druhého Německa jsou ztráty vyšší o 100 mil. Kč. Naopak nejméně škod napáchaných hackery mají firmy v Rusku. Dále je zajímavé, že u všech zemí je pozorován nárůst nákladů v každém roce.

Při porovnání nákladů na kyberkriminalitu v jednotlivých průmyslových sektorech studie společnosti Ponemon Institute uvádí, že nejvíce jsou postižena odvětví energetiky, dále finanční sektor a technologický sektor.

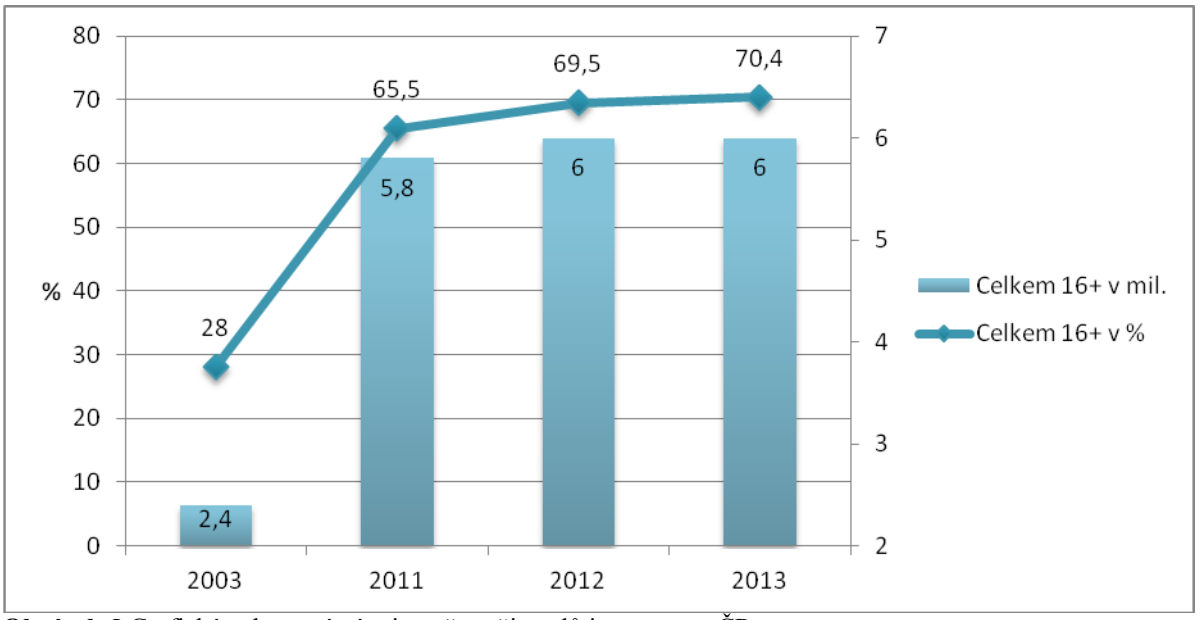
[104] Francie byla přidána do průzkumu v roce 2013 a Rusko 2014.

6 Analýza kybernetické trestné činnosti v České republice

Tato část práce popisuje stav kybernetické trestné činnosti v ČR, zaměřuje se na výše škod[105] způsobené kybernetickými incidenty a pachatele těchto trestných činů. Dále v omezené míře, vzhledem k rozsahu poskytnutých dat, popisuje vývojové trendy kybernetické kriminality v ČR. Autor vychází z dat poskytnutých policií ČR na základě zákona o svobodném přístupu k informacím. Statistická data poskytují kompletní informace až od roku 2011 do 2013, neboť v roce 2010 byl novelizován trestní zákon, do kterého byly zařazeny paragrafy vztahující se ke kybernetické trestné činnosti, a za rok 2014 poskytnutá data nebyla kompletní.

6.1 Česká republika a internet

V České republice v současnosti je kyberkriminalitou ohroženo minimálně 70% populace.[106] Podle údajů Českého statistického úřadu totiž internet využívá sedm lidí z desíti ve věku 16+. Obrázek 6 ilustruje vývoj počtu uživatelů internetu od roku 2011 do 2013. A pro srovnání jsou uvedeny hodnoty naměřené v roce 2003.



Obrázek 6 Grafické zobrazení vývoje počtu uživatelů internetu v ČR.

Zdroj: vlastní zpracování, podle [11]

[105] Škody pro tuto část zahrnují pouze ztrátu finančních aktiv.

[106] Pokud předpokládáme, že každý uživatel internetu je potenciálním cílem kyberútoku.

Lidí ve věku 16 a více let používající internet v roce 2013 bylo 6 miliónů, což představuje 70 % populace. Pokud to porovnáme s rokem 2003, vidíme, že jde o nárůst o 3, 6 miliónů uživatelů. Nejčastěji využívají internet lidé ve věku 16 - 24 let, téměř 100 % a nejméně lidé nad 65 let, 19%. Také lze spatřovat rozdíly ve využívání internetu uživateli, dle dokončeného vzdělání. Uživatelů se základním vzděláním jej využívá 20 % a s vysokoškolským vzděláním 90 %.[107]

Téměř všechny podniky v České republice využívají pro svoji činnost internet. V roce 2013 to bylo 96,3 %. Rozdíly ve využívání internetu lze sledovat v souvislosti s velikostí firem. Podniků s maximálně 50 zaměstnanci jej využívalo 95 % a podniků s více než 250 zaměstnanci jej využilo 99 %.[108]

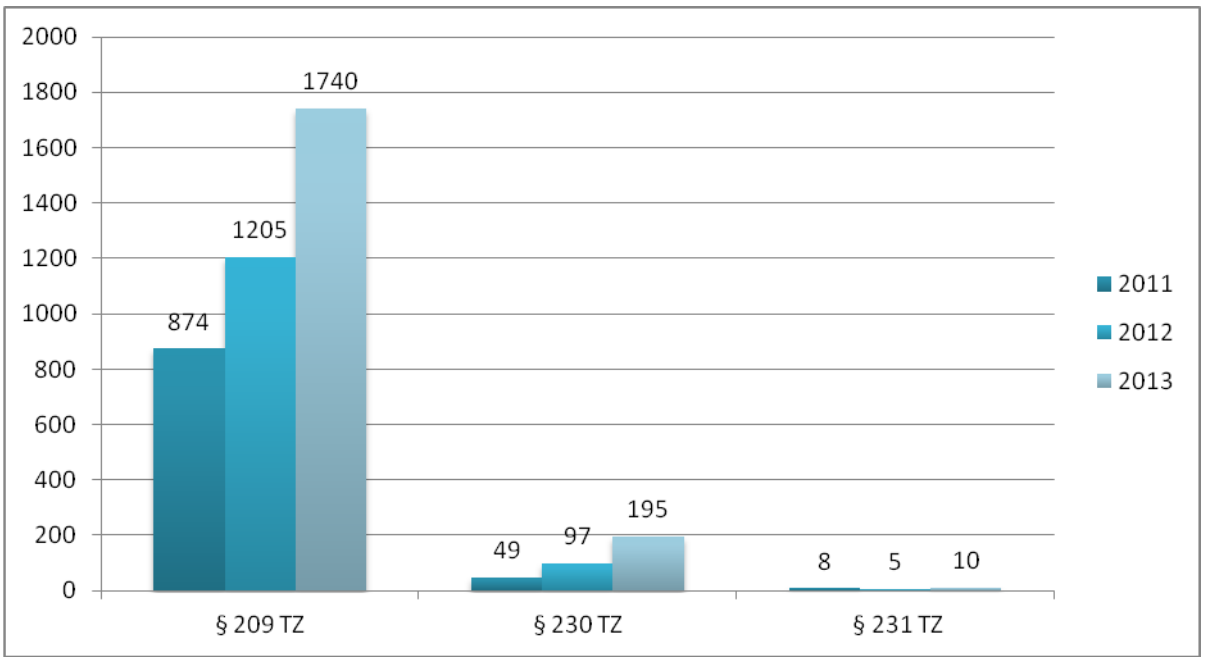
6.2 Kybernetická trestná činnost v České republice

Na základě dat poskytnutých Policií ČR můžeme jednoznačně říci, že největší mírou na způsobených škodách se podílí kybernetické podvody. Jedná se o trestné činy kvalifikované podle § 209 trestního zákona. V kapitole o právní úpravě je popsáno, jaké konkrétní kybernetické útoky pod tento paragraf spadají. Lze jmenovat například trestnou činnost pod názvem phishing a nebo například pharming.

Na obrázku 7 je uveden přehled o počtu trestných činů rozdělených podle uvedených paragrafů.

[107] ČESKÝ STATISTICKÝ ÚŘAD. *Informační technologie* [online]. 2015 [cit. 2015-06-07]. Dostupné z: https://www.czso.cz/csu/czso/informacni_technologie_pm.

[108] Tamtéž.



Obrázek 7 Grafické zobrazení počtu kybernetických trestných činů v ČR

Zdroj: vlastní zpracování, podle [43]

Největší měrou na kybernetické kriminalitě v České republice se podílí trestné činy kvalifikované podle § 209 TZ. Můžeme vidět, že od roku 2011 stoupl počet trestných činů více než dvojnásobně. Také podle nejnovějších informací Policie ČR v roce 2014 počet stále roste. Do poloviny roku 2014 bylo spácháno již 1280 kybernetických podvodů.[109] Mezi trestné činy podle § 230 řadíme například hacking. Podle dat Policie se této trestné činnosti nedopouští pachatelé tak často jako u podvodů. Nicméně jejich počet také stále stoupá. Co se týká § 231 TZ. Kam spadá např. trestná činnost sniffingu, bylo evidováno pouze 10 incidentů v roce 2013.

Tabulka 3 popisuje celkové výše škod způsobené kybernetickými incidenty v jednotlivých letech. Zajisté by zde bylo vhodné zmínit i škody způsobené porušením § 270 TZ. Jedná se o pirátství, warez či P2P trestné činy. Bohužel v současné době v České republice není ustálena jednotná metodika jak tyto škody (finanční ztráty majitelů autorských práv) přesně vyčíslit. Důkazem o tom může být případ brněnského piráta, který měl podle Městského soudu v Brně způsobit škodu ve výši 11 mil. Kč. Tuto výši škody soud vyčíslil tak, že vynásobil počet stažení nelegálního softwaru cenou originálních CD a DVD nosičů. Vyčíslenou částku po odvolání potvrdil i Krajský soud. Soudy tedy předpokládaly, že všichni

[109] POLICIE ČR. *Aktuální trendy informační kriminality* [online]. 2014 [cit. 2015-06-09]. Dostupné z: http://www.saferinternet.cz/attachments/article/457/Aktualni_trendy_informacni_kriminality_PCR.pdf.

ti, kteří si daný software stáhli, by si ho jinak koupili. Po dovolání Nejvyšší soud rozsudky soudů zrušil s tím, že nelze akceptovat způsob výpočtu škody. NS dále poukazuje na Směrnici Evropského parlamentu a Rady 2004/48/ES o vymáhání práv duševního vlastnictví, která byla implementována do českého právního řádu, a která má vést členské státy k tomu, aby stanovovaly výši škody například podle výše licenčních poplatků, které by musel pachatel zaplatit. Dále uvádí, že ne ve všech státech je metodika výpočtu škody stejná. Například ve Švédsku je určena pravděpodobnost, že by si člověk stažený software koupil 1: 3.[110] Lze tedy říci, že vyčíslení škody na základě porušení autorského práva je velmi obtížné, a jednotnou metodiku výpočtu škody pro individuální případy nelze použít.

Tabulka 3 Celkové způsobené škody v jednotlivých letech

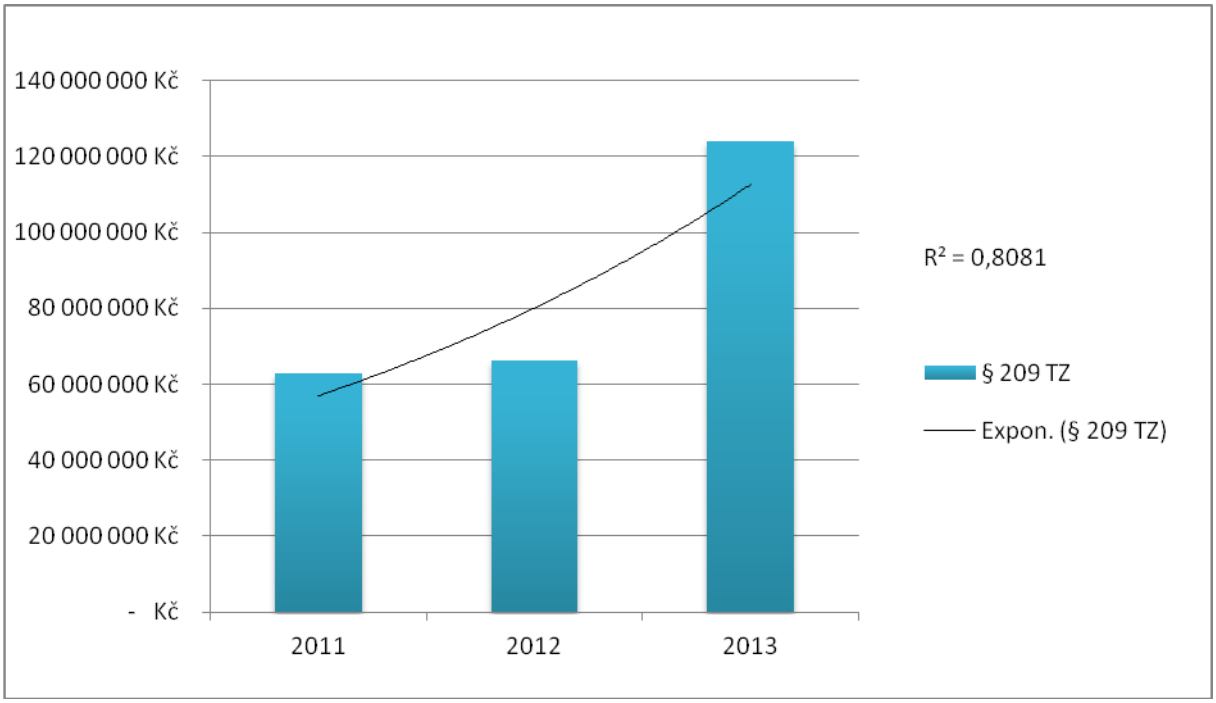
	§ 209 TZ	**§ 230 TZ**	**§ 231 TZ**
2011	62 700 800 Kč	0 Kč	0 Kč
2012	66 125 300 Kč	0 Kč	0 Kč
2013	123 960 700 Kč	352 400 Kč	0 Kč

Zdroj: vlastní zpracování podle [45]

V roce 2013 bylo způsobeno dvojnásobně více škod kybernetickými podvody oproti roku 2011. Škody trestných činů kvalifikovaných podle § 230, § 231 TZ byly téměř vždy nulové až na rok 2013. Důvodem může být například to, že oběti neposkytli informace o výši škody nebo hackerům šlo jen o to prolomit bezpečnostní systém a nikoli o finanční obohacení.

Na obrázku 8 je zobrazen trend růstu výše škod napáchaných kybernetickými podvody.

[110] blíže viz rozhodnutí NS dostupné n: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/675636E6F4A8497FC1257DB6003698A6?openDocument&Highlight=0.



Obrázek 8 Grafické zobrazení trendu růstu výše škod napáchaných kyberkriminalitou

Zdroj: vlastní zpracování, podle [45]

Na grafu vidíme exponenciální růst výše napáchaných škod kybernetickými podvody. Vzhledem k tomu, že v polovině roku 2014 bylo policií evidováno již 1280 kybernetických podvodů, což jsou ¾ celkového počtu za rok 2013, lze předpokládat, že trend růstu škod bude stále stoupat.

Tabulka 4 zkoumá detailněji škody způsobené kybernetickými útoky. Ty jsou rozděleny do kategorií podle toho, jaká byla způsobená škoda jedním útokem.

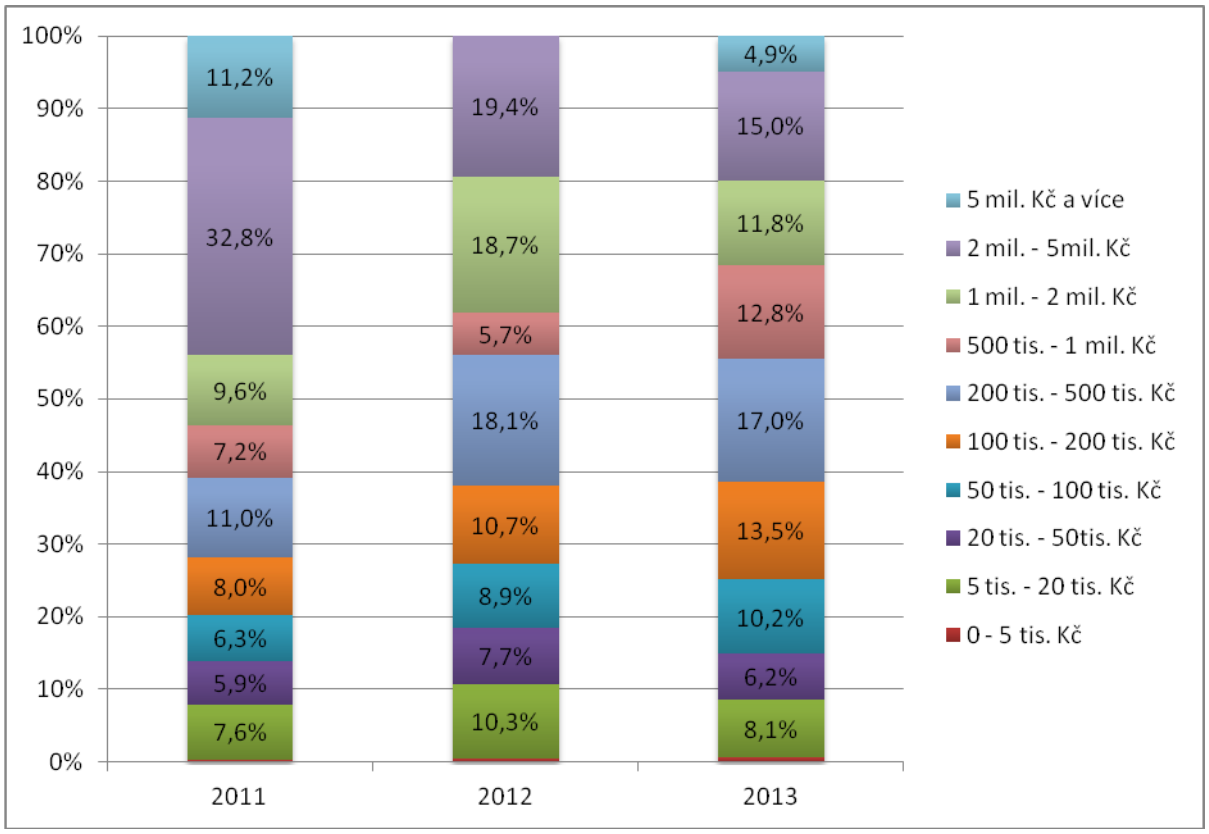
Tabulka 4 Počty kybernetických trestných činů rozdělených podle výše způsobené škody

rozmezí způsobené škody v Kč	počet trestných činů v roce 2011	počet trestných činů v roce 2012	počet trestných činů v roce 2013
0 - 5000	162	283	460
5001 - 20000	521	680	903
20001 - 50000	118	157	224
50001 - 100000	56	81	156
100001 - 200000	36	51	105
200001 - 500000	22	36	60
500001 - 1000000	6	6	20
1000001 - 2000000	4	9	10
2000001 - 5000000	6	4	6
5000001 - více	1	0	1

Zdroj: vlastní zpracování, podle [45]

Nejvíce trestných činů se od roku 2011 pohybovalo v rozmezí škod pěti až dvaceti tisíc korun následováno trestnými činy v rozmezí nula až pět tisíc. Zajímavé je, že ve všech třech letech počty škod v jednotlivých kategoriích stoupají mimo kategorie od dvou miliónů korun a výše. Grafické znázornění je uvedeno v příloze C.

Procentuální vyjádření škod jednotlivých kategorií kybernetických incidentů na celkových škodách lze vidět na obrázku 9.

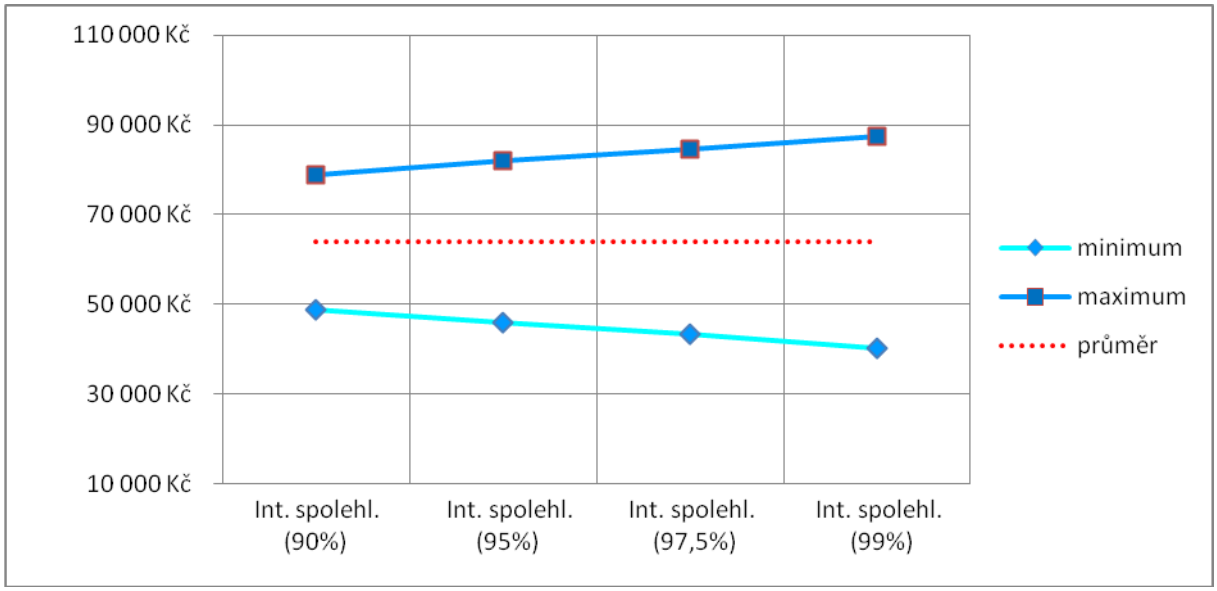


Obrázek 9 Grafické zobrazení procentuálního vyjádření výše škod způsobených jednotlivými kategoriemi kybernetických útoků

Zdroj: vlastní zpracování, podle [45]

Ačkoli počty škod v rozmezí od nuly až do pěti tisíc nebo od pěti tisíc do dvaceti tisíc korun byly absolutně nejvyšší dle tabulky 4, obrázek 9 ukazuje, že na celkové výši škod se tyto kategorie nepodílí velkou měrou. V roce 2011 představovaly škody od dvou miliónů do pěti téměř třetinu všech kybernetických útoků, poté se jejich podíl snižuje. Naopak konstantně se zvyšují kategorie v rozmezí od padesáti do dvě stě tisíc korun.

Průměrné hodnoty kybernetických útoků a intervaly, ve kterých jsme mohli očekávat škodu způsobenou kyberútokem v roce 2013 ukazuje obrázek 10. Hodnoty za roky 2011 a 2012 jsou uvedeny v příloze D.

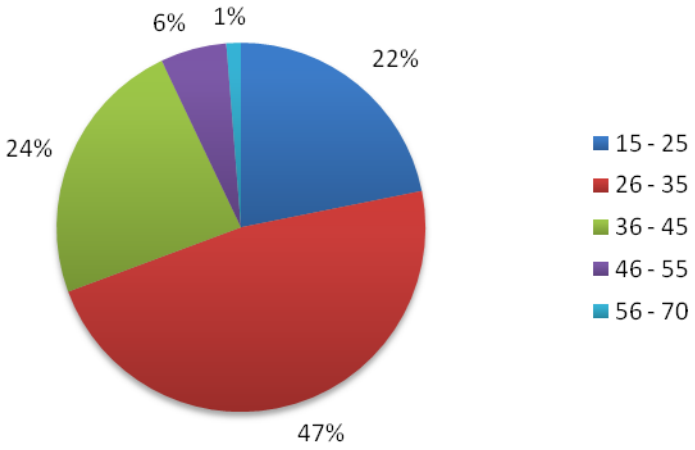


Obrázek 10 Grafické zobrazení průměrné hodnoty a intervalů spolehlivosti škod způsobených kyberútoky v roce 2013

Zdroj: vlastní zpracování, podle [45]

Průměrná hodnota škod způsobených kybernetickými útoky v roce 2012 o proti roku 2011 klesla téměř o dvacet tisíc na padesát tisíc korun, ovšem v roce 2013 se opět přiblížila k sedmdesáti tisícům. Pokud se podíváme na intervaly spolehlivosti, tak vidíme, že se přibližují k průměrné hodnotě. Zatímco v roce 2011 bychom mohli s 99% pravděpodobností očekávat způsobenou škodu od třiceti do sta tisíc korun při průměrné hodnotě sedmdesát tisíc, v roce 2013 to bylo od čtyřiceti tisíc do devadesáti tisíc s podobnou průměrnou hodnotou.

Pro zajímavost jsou dále uvedeny grafy zabývající se samotnými pachateli kybernetické trestné činnosti. Obrázek 11 dělí pachatele podle věku.

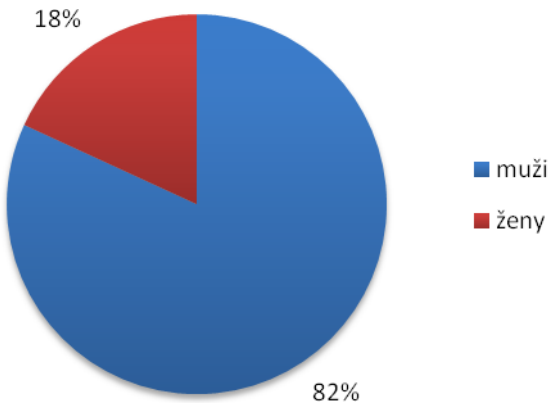


Obrázek 11 Grafické zobrazení věkového rozdělení pachatelů kyberkriminality

Zdroj: vlastní zpracování, podle [45]

Nejvíce se na kyberkriminalitě podílejí pachatelé ve věku 26 až 35 let, je jich téměř polovina.

Obrázek 12 rozlišuje pachatele podle pohlaví.



Obrázek 12 Grafické zobrazení rozdělení pachatelů kyberkriminality dle pohlaví

Zdroj: vlastní zpracování, podle [45]

Na základě uvedených informací v této kapitole lze shrnout, že se počet kybernetických incidentů v České republice exponenciálně zvyšuje. Nejvyšší měrou se na škodách podílejí kybernetické podvody, kam můžeme zařadit například kyberútok phishing. Nejvíce kybernetických útoků co do počtu jednotlivých útoků a způsobených škod se pohybuje v rozmezí od nuly do dvaceti tisíc korun, ale v případě podílu na celkové výši škod se jedná pouze o desetiprocentní část. Dále můžeme pozorovat konstantní nárůst trestných činů, jejichž škody se pohybovaly v rozmezí padesáti až dvě stě tisíci korunami. Podíl škod těchto kategorií na celkových škodách se od roku 2011 do 2013 zvýšil o deset procent.

Policie ČR eviduje i další incidenty jako jsou například mravnostní činy, extremistické projevy, vydírání, šíření poplašné správy (HOAX) nebo nebezpečné pronásledování, avšak do této analýzy nebyly zahrnuty. Analýza se zaměřovala na trestné činy, u kterých se předpokládala způsobená škoda ve formě ztráty finančních aktiv.

7 Závěr

Kybernetickou trestnou činnost můžeme vymezit jako trestnou činnost, která je prováděna v kyberpostoru, přičemž kyberprostor definujeme jako digitální prostředí umožňující vznik, zpracování a výměnu informací, které je tvořené informačními systémy. Informačním systémem se potom rozumí jakékoli zařízení, sestávající se z technického a programového vybavení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat.

Kyberkriminalita se vyvíjí paralelně s vývojem nových technologií. O kybernetické trestné činnosti jako takové lze hovořit až od poloviny dvacátého století. Průkopníkem z této doby byl hacker John Draper neboli „Captain Crunch“. V průběhu let jeho následovníci využívali stále sofistikovanější metody k prolomení bezpečnostních systémů. A dnes můžeme říci, že velmi využívanými metodami hackerů jsou útoky typu phishing, pharming, DDoS a samozřejmě sem patří počítačové pirátství, či warez. V dnešní době stále neexistuje účinná legislativa ani způsob boje proti počítačovému pirátství. Důkazem o tom může být pirátská skupina The Pirate Bay. A také nelze přesně vyčíslit náklady a způsobené škody pirátstvím viz. rozhodnutí Nejvyššího soudu[111].

Cílem diplomové práce bylo vymezit kybernetickou trestnou činnost podle platného a účinného znění zákona a její vliv na ekonomiku. Tento cíl byl splněn ve třetí kapitole prostřednictvím zpracování trestně právních předpisů České republiky, jež jsou po ústavních zákonech druhým nejdůležitějším veřejným právním odvětvím. Práce se zabývá i právní úpravou na mezinárodní úrovni, která je popsána v kapitole čtvrté. Ekonomické vlivy kybernetické trestné činnosti jsou zkoumány v páté kapitole.

Celkové náklady na kybernetickou kriminalitu lze jen odhadovat. Nejaktuálnější studie zabývající se kyberkriminalitou vyčíslují globální náklady na půl procenta světového HDP. U zemí kde se na tvorbě HDP podílí více tvorba duševního vlastnictví, se odhadují nejvyšší náklady. V rámci jednotlivých průmyslových sektorů se odhaduje, že nejvíce postiženy jsou společnosti v energetickém, finančním nebo technologickém průmyslu. Téměř každá společnost s více jak tisíci zaměstnanci se setkala s kybernetickou kriminalitou. Nejvážnější škody jsou způsobeny DDoS útoky a útoky na webové stránky, po nich následují phishingové útoky.

[111] Na straně 58.

Součástí práce je případová studie, která se zabývá analýzou kybernetické trestné činnosti v České republice. Jsou zkoumány jednotlivé typy trestných činů, z pohledu jejich četnosti a způsobených škod.

Situace v České republice potvrzuje, že phishingové útoky jsou v současné době velmi rozšířeným druhem kybernetické trestné činnosti. Tyto útoky klasifikujeme dle § 209 trestního zákoníku jako podvody. Škody způsobené kybernetickými podvody byly v ČR v roce 2013 vyčísleny na necelých 124 mil. Kč. Při porovnání s trestnými činy kvalifikovanými dle § 230, kam řadíme například hacking a § 231, kam spadá sniffing, jsou finanční škody mnohonásobně vyšší. Problémem u phishingu i pharmingu je, že je cílený primárně na majitele bankovních účtů. Ti s nevelkou znalostí tohoto problému snadno podléhají iluzi dostatečného zabezpečení svého počítače a nepřiřazují takový důraz na počítačové napadení jako na napadení přímé. Proto by se měla věnovat zvýšená pozornost tomuto problému. Například již na středních školách v předmětech zaměřených na informační technologie nebo by finanční instituce mohly novým zákazníkům a majitelům účtů poskytovat brožury s informacemi o možnostech napadení.

Otázkou také je do jaké míry by měly společnosti investovat do zabezpečení svých informačních systémů. Dle provedené analýzy se v ČR finanční náklady na jeden kybernetický útok pohybovaly v roce 2013 s 99 % pravděpodobností v rozmezí od čtyřiceti tisíc do devadesáti tisíc korun. A pokud předpokládáme, že frekvence útoku je dvakrát do týdne, měla by být přijata taková opatření, aby byly tyto náklady minimalizovány.

8 Použitá literatura

[1] AKAMAI. *Akamai's State of the Internet: Q4 2014 Report* [online]. 2015 [cit. 2015-06-01]. Dostupné z: http://www.stateoftheinternet.com/resources-connectivity-2014-q4-state-of-the-internet-report.html.

[2] AVAST SOFTWARE. *Statistiky* [online]. 2015 [cit. 2015-06-27]. Dostupné z: https://www.avast.com/cs-cz/stats.

[3] BEZPEČNÝ INTERNET. *Phishing a pharming* [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a -pharming.aspx.

[4] BEZPEČNÝ INTERNET. *Slovník výrazů* [online]. 2015 [cit. 2015-05-31]. Dostupné z: http://www.bezpecnyinternet.cz/slovnik/.

[5] BRZOBOHATÝ, Michal. *Galerie nejlepších hackerů historie* [online]. 2008 [cit. 2015-06-01]. Dostupné z: http://pcworld.cz/ostatni/galerie-nejlepsich-hackeru-historie-12-dil-3475.

[6] CERIAS. *The Development of a meaningful hacker taxonomy: A two dimensional approach* [online]. 2005 [cit. 2015-05-31]. Dostupné z: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-43.pdf.

[7] CSIS. *Net Losses: Estimating the Global Cost of Cybercrime* [online]. 2014 [cit. 2015-06-05]. Dostupné z: http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

[8] COE. *Convention on Cybercrime* [online]. 2001 [cit. 2015-06-02]. Dostupné z: www.psp.cz/sqw/text/orig2.sqw?idd=79483.

[9] COE. *Computer-related crime: recommendation no. R. (89) 9 on computer-related crime and final report of the European Committee on Crime Problems*. Croton, N. Y. : Manhattan Pub. Co. [distributor], 1990, 114 p. ISBN 92-871-1792-6.

[10] COE. *International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identityrelated crime* [online]. 2007 [cit. 2015-06-01]. Dostupné z: http://www.un.org/en/ecosoc/docs/2007/resolution%202007-20.pdf.

[11] ČESKÝ STATISTICKÝ ÚŘAD. *Informační technologie* [online]. 2015 [cit. 2015-06-07]. Dostupné z: https://www.czso.cz/csu/czso/informacni_technologie_pm.

[12] ČÍŽEK, Jakub. *Deset let Pirátské zátoky: Hollywood nemůže vyhrát* [online]. 2013. [cit. 2015-05-14]. Dostupné z: http://www.zive.cz/clanky/deset-let-piratske-zatoky-hollywood-nemuze-vyhrat/sc-3 -a -168689/default.aspx.

[13] ČPU. *Archiv tiskových zpráv* [online]. 2012. [cit. 2015-05-14]. Dostupné z: http://cpufilm.cz/press.html.

[14] ČPU. *Co je pirátství* [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://www.stoppiratstvi.cz/cs/o -piratstvi/co-je-piratstvi.shtml.

[15] ČPU. *Odpovědnost za porušení autorského práva* [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://www.cpufilm.cz/new/www/odpovednost.html.

[16] ČTK. *Obávaný počítačový vir je zpět. Tentokrát napadené vydírá* [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://zpravy.aktualne.cz/finance/obavany-pocitacovy-vir-je-zpet-tentokrat-napadene-vydira/r ~51cdf416e44711e4bc74002590604f2e.

[17] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004, ix, 190 s. ISBN 80-251-0106-1.

[18] ECOSOC. *Kybernalita* [online]. 2010 [cit. 2015-05-31]. Dostupné z: http://www.studentsummit.cz/data/1296412130369BGR_ECOSOC_Kybernalita.pdf.

[19] EU. *Směrnice Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů* [online]. 1995 [cit. 2015-06-01]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:31995L0046.

[20] EU. *Směrnice o soukromí a elektronických komunikacích* [online]. 2002 [cit. 2015-06-01]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:cs:HTML.

[21] EU. *Directive of the european parliament and of the council* [online]. 2006 [cit. 2015-06-01]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024.

[22] EU. *Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům* [online]. 2005 [cit. 2015-06-02]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:CS:PDF.

[23] FRANCOVÁ, Pavla. *Největší banky v Česku napadli hackeři. Vyřadili jim z provozu internetové bankovnictví* [online]. 2013. [cit. 2015-05-14]. Dostupné z: http://byznys.ihned.cz/c1-59450640-nejvetsi-banky-v -cesku-napadli-hackeri-vyradili-jim-z -provozu-internetove-bankovnictvi.

[24] FIALA, Lukáš. *The Pirate Bay se stěhuje do cloudu, stránka je opět odolnější vůči raziím* [online]. 2012. [cit. 2015-05-14]. Dostupné z: http://www.cnews.cz/pirate-bay-se-stehuje-do-cloudu-stranka-je-opet-odolnejsi-vuci-raziim.

[25] GIBSON, William. *Neuromancer*. Unabridged ed. Westminster, Md: Books on Tape, 2011. ISBN 978-030-7969-958.

[26] GŘIVNA, Tomáš, et al. *Český právní řád a ochrana kyberprostoru: vybrané problémy*. Praha: Karolinium, 2008. 140 s. ISBN 978-80-246-1703-9.

[27] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-809-0378-674.

[28] HALLER, Martin. *Denial of Service (DoS) útoky: záplavové typy* [online]. 2006. [cit. 2015-05-14]. Dostupné z: http://www.lupa.cz/clanky/denial-of-service-dos-utoky-zaplavove-typy/.

[29] HACKOVÁNÍ PC. *Nabourání FB účtu* [online]. 2012. [cit. 2015-05-14]. Dostupné z: http://hackovanipc.webnode.cz/hacking/nabourani-fb-uctu/.

[30] HOAX [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://hoax.cz/cze/.

[31] HOAX. *Co je to phishing* [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing.

[32] JANSA, Lukáš. *Cybersquatting a jeho podoby* [online]. 2008. [cit. 2015-05-14]. Dostupné z: http://www.pravoit.cz/article/cybersquatting-a -jeho-podoby.

[33] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vydání Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

[34] MASARYKOVA UNIVERZITA. *Bezpečnostní tým z Masarykovy univerzity odhalil hackera* [online]. 2014. [cit. 2015-05-14]. Dostupné z: http://www.online.muni.cz/udalosti/4814-bezpecnostni-tym-z -masarykovy-univerzity-odhalil-hackera#.VVRlrPDUeq9.

[35] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-722-6419-2.

[36] MCQUADE, Samuelson C. Encyclopedia of cyber crime. Westport, Conn.: Greenwood Press, 2009, xxiii, 210 p. ISBN 03-133-3974-0.

[37] MIKLICA, Tomáš. *The Pirate Bay se zbavuje odpovědnosti. Začíná éra magnetů* [online]. 2012. [cit. 2015-05-14]. Dostupné z: http://www.cnews.cz/pirate-bay-se-zbavuje-odpovednosti-zacina-era-magnetu.

[38] MVČR. *Mezinárodní spolupráce v boji proti informační kriminalitě* [online]. 2009 [cit. 2015-06-01]. Dostupné z: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-mezinarodni-pdf.aspx.

[39] NATO. *Cyber security* [online]. 2015 [cit. 2015-06-01]. Dostupné z: http://www.nato.int/cps/en/natohq/topics_78170.htm.

[40] NATO. *Wales Summit Declaration* [online]. 2014 [cit. 2015-06-01]. Dostupné z: http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[41] OECD. *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* [online]. 2002 [cit. 2015-06-01]. Dostupné z: http://www.oecd.org/sti/ieconomy/15582260.pdf.

[42] POLČÁK, Radim a Mike SHEMA. *Právo na internetu: spam a odpovědnost ISP*. Vyd. 1. Brno: Computer Press, 2007, v, 150 s. Právo a IT. ISBN 978-80-251-1777-4.

[43] POLICIE ČR. *Aktuální trendy informační kriminality* [online]. 2014 [cit. 2015-06-09]. Dostupné z: http://www.saferinternet.cz/attachments/article/457/Aktualni_trendy_informacni_kriminality_PCR.pdf.

[44] POLICIE ČR. *Co je extremismus?* [online]. 2015. [cit. 2015-05-14]. Dostupné z: http://www.policie.cz/clanek/prevence-informace-o -extremismu-co-je-extremismus.aspx.

[45] POLICIE ČR. *IT kriminalita* [online]. 2014 [cit. 2015-06-28]. Dostupné z: http://www.policie.cz/clanek/it-kriminalita.aspx.

[46] PONEMON INSTITUTE. *2014 Global Report on the Cost of Cyber Crim* [online]. 2014 [cit. 2015-06-06]. Dostupné z: http://h20195.www2.hp.com/v2/getpdf.aspx/4AA5-5207ENW.pdf?ver=1 .0.

[47] ROUSE, Margaret. *Bulletin board system* [online]. 2005 [cit. 2015-06-01]. Dostupné z: http://whatis.techtarget.com/definition/bulletin-board-system-BBS.

[48] SCAMBRAY, Joel a Mike SHEMA. *Hacking bez tajemství: webové aplikace*. Vyd. 1. Brno: Computer Press, 2003, xxix, 328 s. ISBN 80-722-6769-8.

[49] SECURITY PORTAL. *Seznamte se – DoS a DDoS útoky* [online]. 2013. [cit. 2015-05-14]. Dostupné z: http://www.security-portal.cz/clanky/.

[50] SMEJKAL, Vladimír. *Informační a počítačová kriminalita v České Republice* [online]. 1999 [cit. 2015-06-01]. Dostupné z: http://www.mvcr.cz/casopisy/studie/diskuse/analyza.html.

[51] ŠÁMAL, Pavel. 2010. *Trestní zákoník: komentář*. 1. vyd. V Praze: C. H. Beck, 2 v. ISBN 97880740017892.

[52] THE WORLD BANK. *Gross domestic product 2013* [online]. 2015 [cit. 2015-06-05]. Dostupné z: http://databank.worldbank.org/data/download/GDP.pdf.

[53] UN. *Combating the criminal misuse of information technologies* [online]. 2001 [cit. 2015-06-01]. Dostupné z: http://www.itu.int/ITU-D /cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

[54] UN. *Resolution 1624 (2005)* [online]. 2005 [cit. 2015-06-01]. Dostupné z: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/510/52/PDF/N0551052.pdf?OpenElement.

[55] VOPAT, Radek. *Fio banka a phishing v praxi: Aktuální zkušenost* [online]. 2014 [cit. 2015-06-06]. Dostupné z: http://finexpert.e15.cz/fio-banka-a -phishing-v -praxi-aktualni-zkusenost.

[56] VÝZNAM SLOVA. *Význam cracker* [online]. 2015 [cit. 2015-05-31]. Dostupné z: http://www.vyznam-slova.com/cracker.

[57] WEBCRUNCHERS. *Who is John Draper AKA Captain Crunch* [online]. 2015 [cit. 2015-06-01]. Dostupné z: http://www.webcrunchers.com/who-is-john-draper-aka-captain-crunch/.

[58] WEIK, Martin H. *The ENIAC Story* [online]. 1961 [cit. 2015-06-01]. Dostupné z: http://ftp.arl.mil/mike/comphist/eniac-story.html.

[59] Zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů.

[60] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

[61] Zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů.

[62] Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

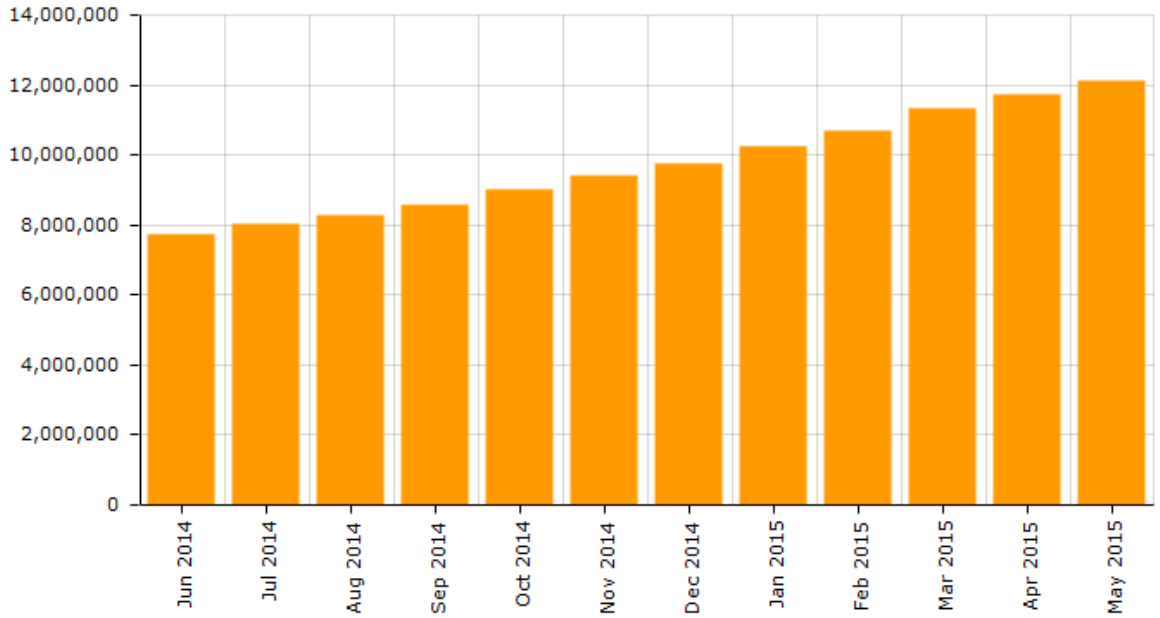
[63] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským, ve znění pozdějších předpisů.

[64] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

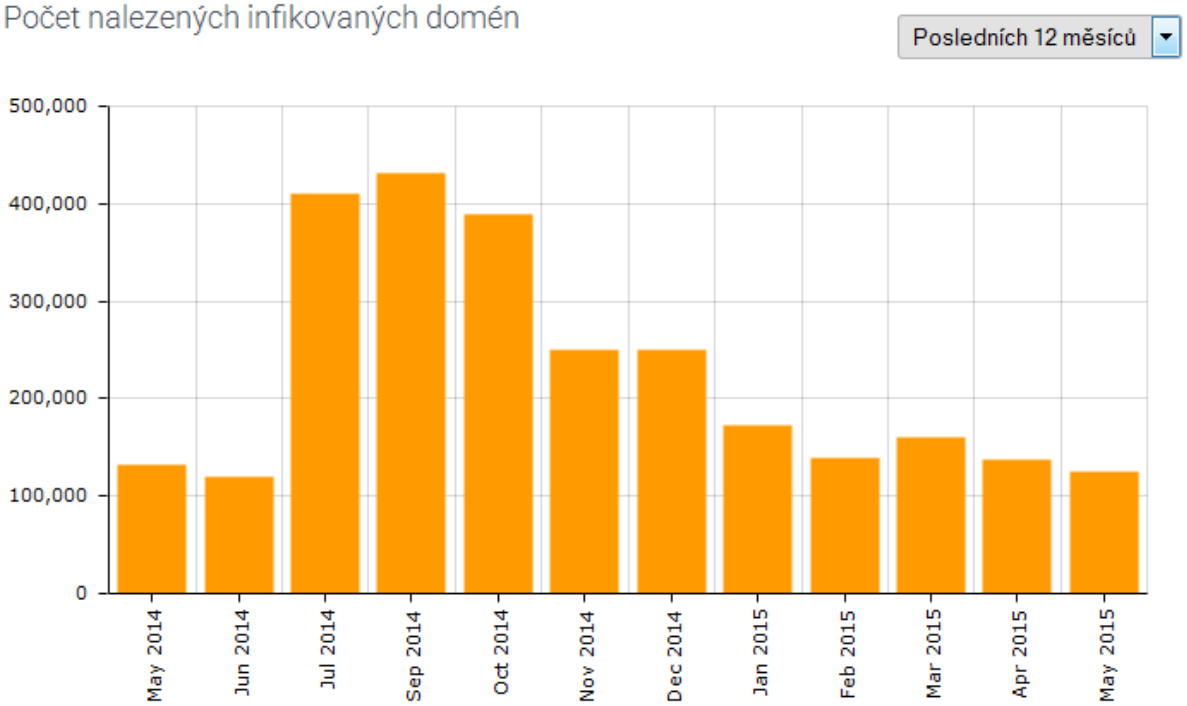
9 Přílohy

Příloha A *Bezpečnostní statistiky evidované společností Avast*[112]

Nově přidané virové definice (posledních 12 měsíců)

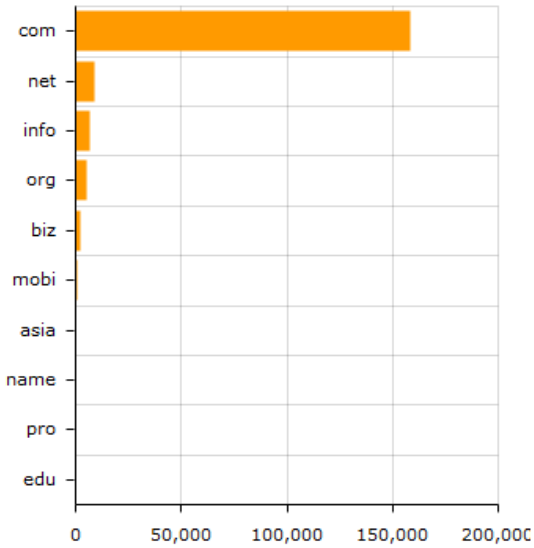


Počet nalezených infikovaných domén

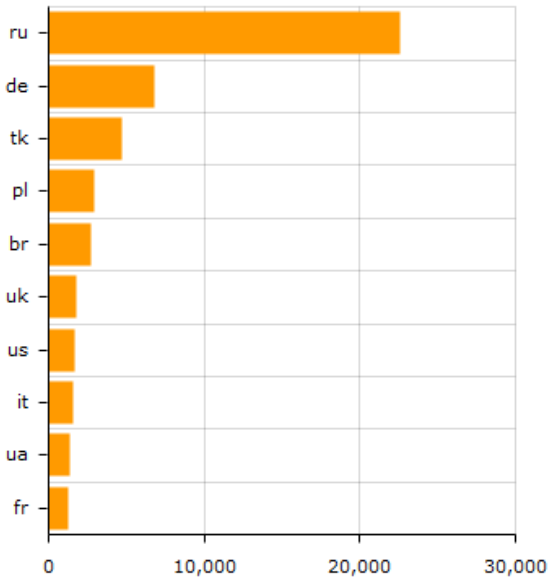


[112] AVAST SOFTWARE. *Statistiky* [online]. 2015 [cit. 2015-06-27]. Dostupné z: https://www.avast.com/cs-cz/stats.

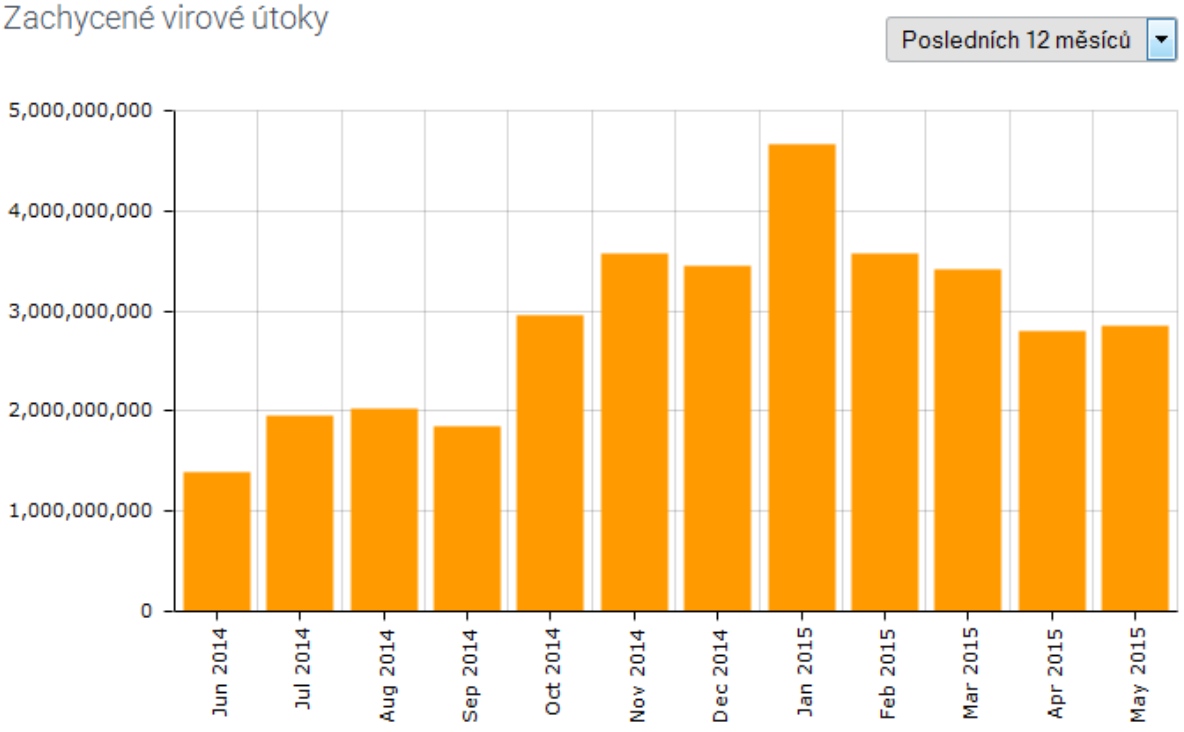
10 nejvíce nakažených nadnárodních TLDs
(minulý měsíc)



10 nejvíce nakažených národních TLDs
(minulý měsíc)

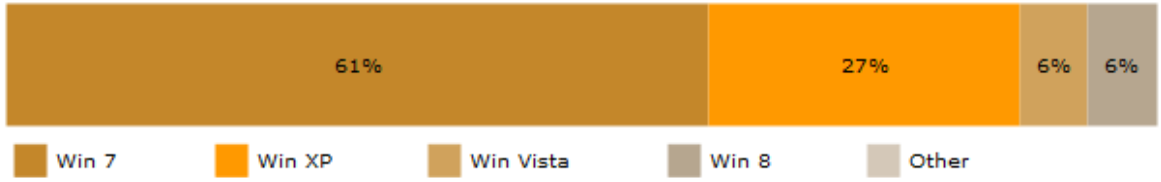


Zachycené virové útoky



Aktivně chráněná zařízení podle OS

PC uživatelé podle OS

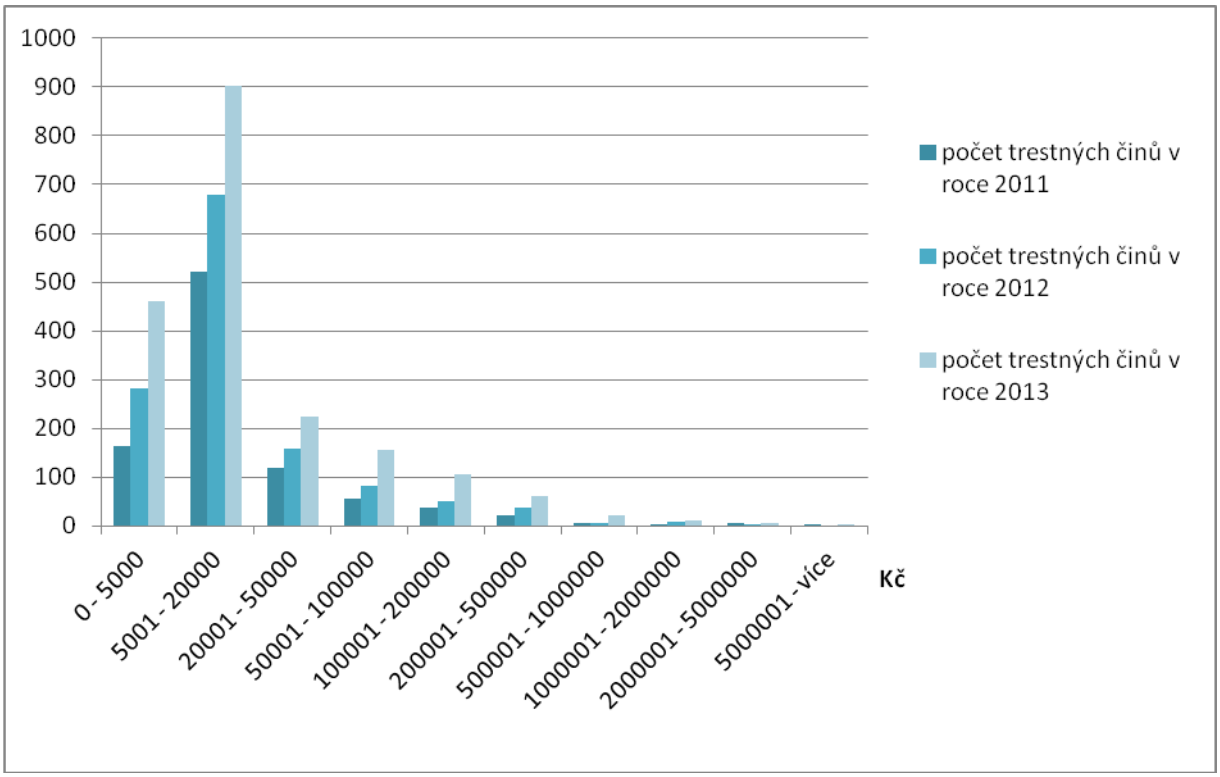


Příloha B *Průměrné celkové náklady na kyberkriminalitu ve vybraných zemích*[113]

v mil. Kč	USA	Německo	Japonsko	Francie	VB	Austrálie	Rusko
2012	196	131	113	-	72	75	-
2013	254	166	148	114	104	81	-
2014	279	179	152	140	130	88	73

[113] PONEMON INSTITUTE. *2014 Global Report on the Cost of Cyber Crim* [online]. 2014 [cit. 2015-06-06]. Dostupné z: http://h20195.www2.hp.com/v2/getpdf.aspx/4AA5-5207ENW.pdf?ver=1 .0.

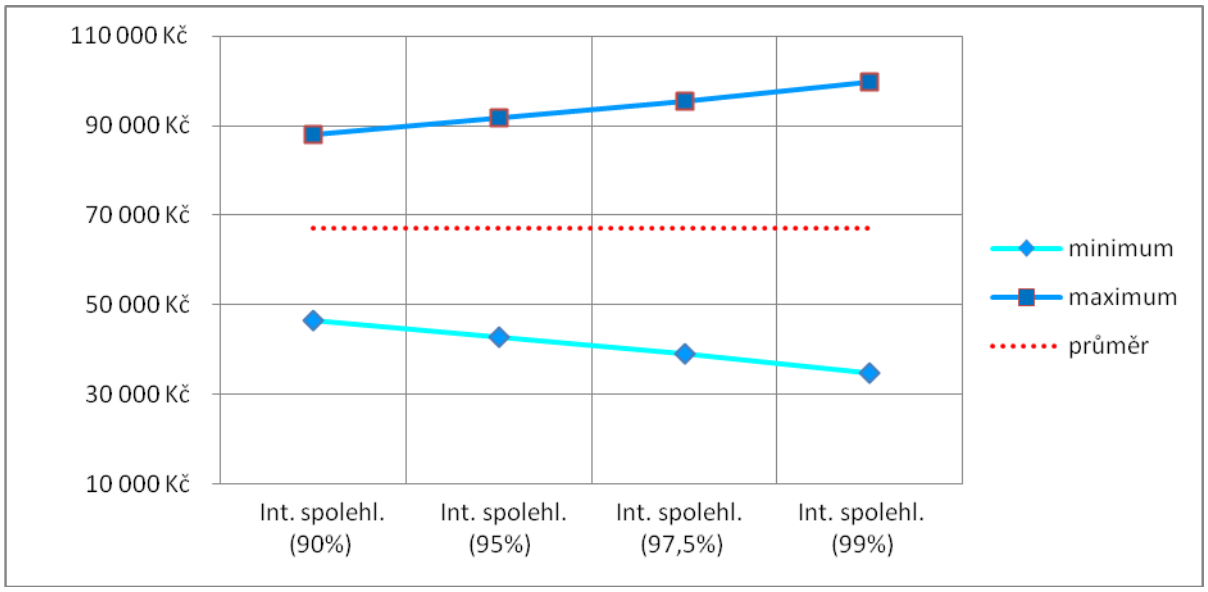
Příloha C *Počty kybernetických trestných činů rozdělených podle výše způsobené škody.*[114]



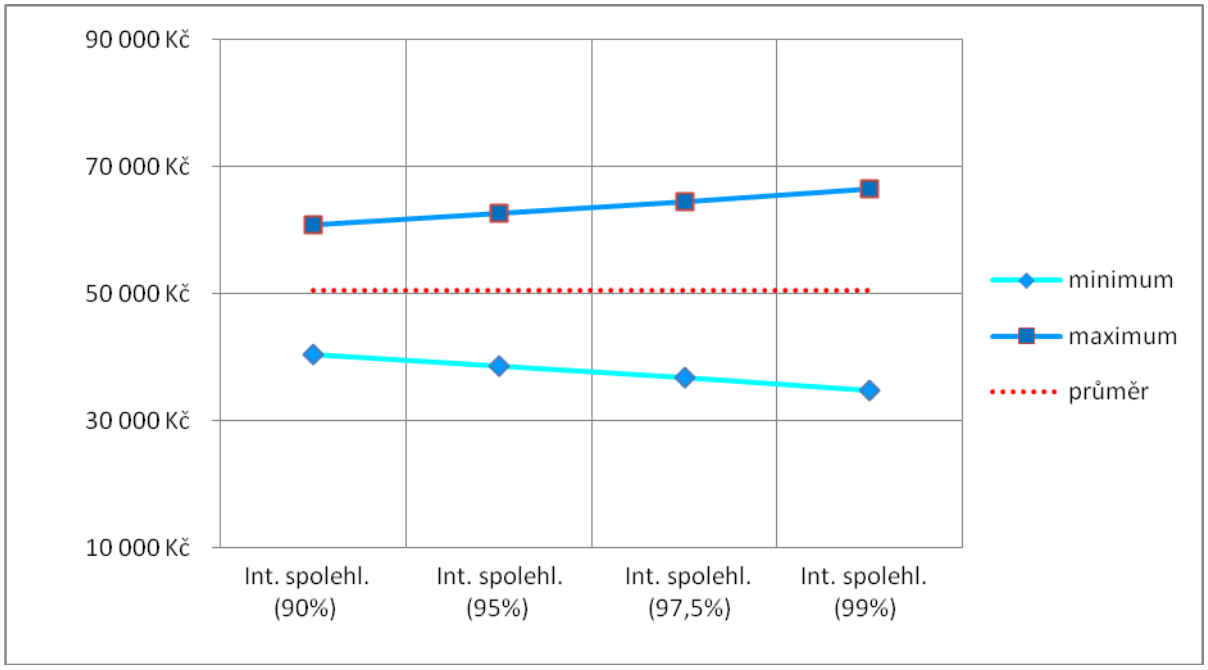
[114] POLICIE ČR. *IT kriminalita* [online]. 2014 [cit. 2015-06-28]. Dostupné z: http://www.policie.cz/clanek/it-kriminalita.aspx.

Příloha D *Grafické zobrazení průměrné hodnoty a intervalů spolehlivosti škod způsobených kyberútoky v roce 2011 a 2012.*[115]

2011



2012



[115] POLICIE ČR. *IT kriminalita* [online]. 2014 [cit. 2015-06-28]. Dostupné z: http://www.policie.cz/clanek/it-kriminalita.aspx.