JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
PEDAGOGICKÁ FAKULTA
A
VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE
FAKULTA MANAGEMENTU V JINDŘICHOVĚ HRADCI

BAKALÁŘSKÁ PRÁCE

2011/2012 **Petr Maroušek**

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
PEDAGOGICKÁ FAKULTA
A
VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE
FAKULTA MANAGEMENTU V JINDŘICHOVĚ HRADCI

Využití internetu při páchání majetkové trestné činnosti
(Internet utilization for commission of crimes against property)

Autor bakalářské práce: Petr Maroušek
Vedoucí bakalářské práce: doc. JUDr. Dr. Jan Hejda
Studijní program: Sociální pedagogika
Datum odevzdání bakalářské práce: 31.3. 2012

Prohlášení

Prohlašuji, že bakalářskou práci na téma

„**Využití internetu při páchání majetkové trestné činnosti**“

jsem zpracoval samostatně a že jsem vyznačil prameny, z nichž jsem pro svou práci čerpal, způsobem ve vědecké práci obvyklým.

Dále prohlašuji, že v souladu s § 47b zákona č.111/1998 Sb. v platném znění, souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě, elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedením zákona č. 111/1998 Sb. zveřejněny posudky školitele i záznam o průběhu a výsledku obhajoby kvalifikační práce.

Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

České Budějovice, dne 21. února 2012

.....

Petr Maroušek

Poděkování:

Zvláštní poděkování bych chtěl věnovat doc. JUDr. Dr. Janu Hejdovi, za odborné vedení, ochotu a cenné rady při psaní bakalářské práce.

Anotace

Bakalářská práce je zaměřena na problematiku využití internetu při páchání majetkové trestné činnosti.

Teoretická část obsahuje vymezení základních pojmů týkající se informační kriminality, jejího rozdělení a odhalování. Další část práce se zabývá definováním internetového obchodování, jeho charakteristickými znaky a specifiky.

Cílem praktické části je analýza nejčastějších trestných činů souvisejících s tzv. počítačovou kriminalitou s důrazem na majetkovou trestnou činnost. V práci je navržena metodika postupů a činností pro obchodování na internetu, demonstruje racionální postup při obchodování na internetu. Závěr praktické části tvoří statistika oznámení týkajících se podvodného jednání na aukčních serverech.

Annotation

This bachelor´s work is focused on abusing the internet in committing crime against property.

In this bachelor's work are defined basics concepts regarding information crime, its sorting and detection. The other part of this work is dealing with definition of internet business, its typical features and specifics.

The aim of practical part is the analysis of the most common crimes related with so called „pc crime" with accent to crimes against property. The methods of procedure and activities for the internet business is suggested in this work. It is illustrated the economical procedur in internet business. The conclusion of the bachelor's work creates the statistics of announcements regarding the fraudulent manners on auctions servers.

Obsah

Úvod

Pro svoji bakalářskou práci jsem si zvolil téma „Využití internetu při páchání majetkové trestné činnosti.“ Toto téma je dle mého názoru vysoce aktuální v závislosti na prudkém nárůstu majetkové trestné činnosti v oblasti informačních a komunikačních technologií, ale také na změnách, které proběhaly v legislativě našeho státu.

Internet umožňuje rychlou a relativně anonymní výměnu informací a názorů. Tím slouží jak legálním účelům, tak zločincům, včetně teroristů.

V roce 2010 kriminalisté jihočeského policejního ředitelství vyšetřovali po celém kraji zhruba tři desítky případů, kde hrál hlavní roli při sjednání obchodu internet a jeho anonymita. Za první tři měsíce letošního roku již vyšetřují čtyři desítky případů. Nárůst této specifické trestné činnosti je tedy značný. Z velké části si nakupující problém přivolají sami, protože při internetových a tím vlastně i anonymních nákupech, nedodržují základní pravidla opatrnosti.

Lidská důvěřivost prostě nezná mezí. Pod vidinou ušetření několika set či tisíc korun nakupuje čím dál více lidí po internetu. Většina z nich, však nedodrží základní bezpečnostní pravidla. Mnoho později podvedených lidí si vybere výrobek například v internetových aukcích či internetových bazarech a pod vidinou výrazné slevy oproti kamennému obchodu pošle dopředu peníze naprosto neznámé a neprověřené osobě či společnosti. Jaký je pak „údiv“ když zboží nedorazí, prodejce na emailových adresách či uvedených mobilních telefonech není dostupný a peníze jsou pryč. Ve většině případů se pak od prvního poškozeného začne odvíjet celá řada dalších podvedených.

Cílem této bakalářské práce je analýza nejčastějších trestných činů souvisejících s tzv. informační kriminalitou s důrazem na majetkovou trestnou činnost. Výstupem práce je metodický profil postupů a činností, vedoucích k ochraně uživatelů internetového obchodování, nákupu, či prodeje věcí se specifikací konkrétních preventivních kroků.

Jelikož Policie ČR není schopna zmapovat veškerou kriminalitu na území České republiky, která se týká informační kriminality, rozhodl jsem se analyzovat nejčastější trestné činy v oblasti informačních a telekomunikačních technologií s důrazem na majetkovou trestnou činnost spáchané na území Jihočeského kraje.

Následující rady jsou určeny primárně těm, kteří jsou připojeni k síti Internet, ale využít jich mohou i ostatní uživatelé informačních a komunikačních technologií. V bakalářské práci

jsou shrnuty základy bezpečnosti na Internetu – základní rady a doporučení pro nejširší veřejnost.

Práce je rozdělena do sedmi kapitol. První kapitola objasňuje základní pojmy týkající se informační technologie. Ve druhé kapitole je popsán historický vývoj počítačové kriminality, její rozdělení a výčet základních skupin. Dále jsou v této kapitole charakterizovány typické způsoby páchání informační kriminality. Třetí kapitola se věnuje odhalování informační kriminality, bezpečnostní politikou ČR v boji proti počítačové a informační kriminalitě. Další část této kapitoly charakterizuje pachatele a trendy informační kriminality. Čtvrtá kapitola vymezuje znaky internetového obchodování, charakterizuje elektronický obchod a typy obchodů. V závěru této kapitoly jsou představena rizika obchodování na internetu. Pátá kapitola popisuje stávající situaci při obchodování na internetu, jsou zde charakterizovány čtyři hlavní představitelé internetových obchodů. Šestá kapitola přináší návod postupů a činností pro obchodování na internetu, zahrnující obecnou metodiku a program ochrany kupujících. Sedmá kapitola je věnována statistickému výzkumu, provedeném v rámci této bakalářské práce. Pro zjištění potřebných údajů, jsem použil Evidenci trestního řízení používanou u Policie ČR. Závěr této bakalářské práce přináší shrnutí rad pro obchodující na internetu, ale i pohled na možnosti boje proti informační kriminalitě ze strany policie.

1. VYMEZENÍ ZÁKLADNÍCH POJMŮ

1.1 HARDWARE A SOFTWARE POČÍTAČE

Počítačový hardware „computer hardware“ označuje veškeré fyzicky existující technické vybavení počítače na rozdíl od dat a programů (označovaných jako software). Hardware jsou součástky počítače, bez nichž by nebyl schopen pracovat. Jsou to elektronické součástky, které jsou na základové jednotce někdy nazývané základová deska, motherboard nebo mainboard. Základová deska je základní hardware většiny počítačů. Samotná hranice mezi softwarem a hardwarem však není nijak ostrá – existuje tzv. firmware, což je název pro programy napevno vestavěné v hardware. Zdroj, je hardware napájený z elektrické sítě, který vede proud do základové jednotky a jiných hardware součástí, které nejsou přímo zapojeny do některé ze sběrnic na základové jednotce, a potřebují k chodu proud.

Počítač se obvykle skládá z čistě elektronických zařízení (procesor, operační paměti, display) a elektromechanických dílů, vstupně-výstupních zařízení (klávesnice, tiskárna, diskety, disky, jednotky CD-ROM, páskové jednotky, reproduktory) pro vstup, výstup a ukládání dat.[1]

Software (též programové vybavení) je v informatice sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost. Software lze rozdělit na systémový software, který zajišťuje chod samotného počítače a jeho styk s okolím a na aplikační software, se kterým buď pracuje uživatel počítače, nebo zajišťuje řízení nějakého stroje.

Software je protiklad k hardwaru, který zahrnuje všechny fyzické součásti počítače (elektronické obvody, skříň…).

Mezi software zahrnujeme i data, která typicky není možné vykonat procesorem, protože neobsahují strojové instrukce pro procesor počítače, ale data popisují obrázek, textový dokument a podobně. Označení software se tak někdy vztahuje jen na programy, ale může se vztahovat i na data.[2]

[1] http://cs.wikipedia.org/wiki/Hardware 9. 10. 2011
[2] http://cs.wikipedia.org/wiki/Software 9. 10. 2011

2. INFORMAČNÍ KRIMINALITA

Informační kriminalita jako nový kriminální obor se rozvíjí stejně bouřlivě jako technický obor, s nímž souvisí. V roce 1990 byla na mezinárodním fóru zmíněna počítačová (informační) kriminalita jako jedna z nejnebezpečnějších forem kriminálních deliktů spolu s organizovaným zločinem a distribucí drog.[3] Pod tímto pojmem je třeba chápat páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení data nevyjímaje, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako movité věci, nebo jako nástroj trestné činnosti.[4]

Chmelík ve své knize Rukověť kriminalistiky popisuje informační (počítačovou) kriminalitu jako velmi specifickou a velmi sofistikovanou formu kriminality, která nemá vždy jen ekonomický rozměr. [5]

„Computer crime“ se jako všeobecně přijímaný a chápaný pojem objevuje v právní a kriminologické terminologii vyspělých zemí již v sedmdesátých letech.[6] V České republice se častěji užívá výraz „počítačová kriminalita“, kdy tento výraz je poměrně složitě definovatelný a existuje mnoho podob různých definic, podle toho z jakého hlediska na tuto problematiku její autoři nahlíží.

Informační kriminalita je specifická trestná činnost, která je páchána pouze s pomocí výpočetní techniky, kdy je také předmětem trestného činu nebo pachatelovým nástrojem. Pokud pachatel ke svému jednání užije výpočetní techniku a jeho jednání naplňuje znaky skutkové podstaty některého z trestných činů uvedených v trestním zákoně a nebezpečnost takového jednání dosahuje požadovaného stupně nebezpečnosti činu pro společnost, můžeme říct, že se jedná o informační kriminalitu.

Počítače v podstatě neumožňují páchat novou neetickou a trestnou činnost, poskytují jen novou technologii a nové způsoby páchání již známých trestných činů, jako sabotáž, krádež, neoprávněné užívání cizí věci, vydírání nebo špionáž.[7]

---

[3] Pravděpodobné modely organizované kriminality. 8. Konference OSN, Havana, 1990. Vydal Institut pro kriminologii a sociální prevenci, Praha 1994.
[4] SMEJKAL, V., SOKOL, T.,VLČEK, M. *Počítačové právo*. Praha : C.H. Beck: SEVT, 1995. s. 99
[5] CHMELÍK, J. a kol. *Rukověť kriminalistiky*. Vyd. Plzeň: Aleš Čeněk 2005. ISBN 80-86898-36-9.
[6] SMEJKAL, V. *Internet @ .§§§*. Vyd. 1. Praha: Grada, 1999. s. 168, ISBN 80-7169-765-6.
[7] POŽÁR, J. *Základy teorie informační bezpečnosti*. 1. Vyd. Policejní akademie České republiky v Praze, 2007. ISBN 978-80-7251-250-8.

Počítačová kriminalita má řadu významných charakteristik, které ji odlišují od kriminality klasické. Ve většině případů informační kriminality se neobjevují takové prvky, jako je násilí, použití zbraně, újma na zdraví osob apod. Zatímco u klasické kriminality se měří doba spáchání trestného činu na minuty, hodiny, dny, trestný čin v oblasti informační kriminality může být spáchán v několika tisícinách sekundy a pachatel ani nemusí být přímo na místě činu.

Další významnou charakteristikou pro informační kriminalitu jsou v důsledku značné ztráty, ať již přímo v podobě finančních částek, nebo v podobě zneužití získaných údajů.

Informační kriminalitu zároveň provází určitá diskrétnost trestné činnosti. Z uvedeného vyplývá, proč informační kriminalita bývá pro svou povahu označována jako kriminalita „bílých límečků".

Trestná činnost, která je spojena *s prostředím Internetu* se může rozdělit do dvou základních skupin:

1. *informační trestná činnost* - zpřístupňování informací, které mohou někomu způsobit újmu nebo založit spáchání trestného činu nebo naopak shromažďování informací o osobách za účelem jejich pozdějšího nelegálního využití,
2. *internetovská trestná činnost* - páchání trestné činnosti v internetovém prostředí.

Matějka ve své publikaci Počítačová kriminalita cituje definici informační kriminality vypracovanou Radou Evropy v roce 2000. „Trestný čin namířený buďto proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin v tradičním smyslu, při kterém je použito moderních informačních či telekomunikačních technologií".[8]

Dle nastíněných definicí není vymezení informační kriminality ostře vyhraněno, a to zřejmě z důvodu, že se překrývá i s jinými typy kriminality (např. hospodářskou kriminalitou, kriminalitou bílých límečků, organizovaným zločinem), k jejichž páchání není zapotřebí počítač.[9]

OSN ve svém Manuálu definuje informační kriminalitu takto: Informační kriminalitu představují jednak tradiční zločinné aktivity jako krádež, podvod nebo padělání, tedy činy,

[8] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002. s. 5
[9] MUSIL, S. *Počítačová kriminalita: Nástin problematiky: kompendium názorů specialistů*. Praha: Institut pro kriminologii a sociální prevenci, 2000. s. 13

které jsou trestné ve většině zemí. K tomu se přidružují nové způsoby zneužití počítačů, které jsou, nebo by měly být trestnými.[10]

Literatura většinou uvádí následující **základní kriminogenní faktory**, které mají vztah k informační kriminalitě, případně ji usnadňují:

1. Složitost informačních technologií a jejich provozu je pro značnou část uživatelů neproniknutelná. Z toho pramení vnímání světa počítačů jako čehosi neuchopitelného a již od základu podezřelého.
2. Důvěra uživatelů ve výstupy z informačních technologií. Například skutečnost, že málo koho napadne kontrolovat účet připravený počítačovým systémem v supermarketu, nebo ověřovat správnost výpočtu provedených počítačem v rámci firemního účetnictví. V důsledku toho může zůstat dlouho neodhalen pachatel počítačového podvodu či zpronevěry, který si z finančních toků procházejících systémem pravidelně odečítá mikroskopické částky pro vlastní obohacení apod.
3. Objem dat v prostředí, kde se pachatelé pohybují, je často enormní. Je technicky neproveditelné efektivně kontrolovat veškerá data procházející třeba sítí Internet.
4. Páchání trestné činnosti od obrazovky počítače je neporovnatelně snazší, než je tomu v reálném životě.
5. Obecně nízké právní vědomí populace, které se projevují i v jiných oblastech práva, je v případě informačních technologií (dále jen IT) ještě nižší.
6. Nedokonalost legislativy. Právní normy upravující oblast IT jsou mnohdy obtížně vyložitelné a jejich mezerovitost je značná.

Internetová encyklopedie Wikipedia označuje termínem informační (počítačová) kriminalita trestné činy zaměřené proti počítačům a trestné činy páchané pomocí počítače.[11]

Dokument zpracovaný odborem bezpečnostní politiky MVČR „Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení,“[12] který informační kriminalitu definuje jako: „Páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem

[10] Manuál OSN pro prevenci a kontrolu počítačového zločinu, OSN 1994
[11] http://sk.wikipedia.org/wiki/počítačová_kriminalita, 25.8.2011
[12] http://www.mvcr.cz, 25.8.2011

s výjimkou majetkové trestné činnosti, nebo jako nástroj trestné činnosti.“ Autor neoperuje jen s pojmem počítačová kriminalita, ale vzhledem k prolínání výpočetní techniky s komunikačními technologiemi je operováno s termínem informační kriminalita. Jak je dále zmíněn, „Tím dochází k vytváření kompaktnějšího systému, kdy se do informační kriminality zahrnuje oblast výpočetní techniky, komunikačních technologií a další technicky vyspělá odvětví jako například elektronické platební prostředky“.

Mezinárodní dokumenty, například COM (2000) 890 final, se snaží posouvat pojetí počítačové kriminality do oblasti informačních technologií. Dochází zde ke sjednocení pojmů jako „computer crime” “computer-related crime,” “high-tech crime” and “cybercrime”.[13]

Poslední zmíněný termín, „Cybercrime“, který já sám považuji za nejvýstižnější, je navíc zmíněn v oficiálním názvu Úmluvy o počítačové kriminalitě (Convention on Cybercrime).[14] Je tak zahrnuta i nová oblast související s počítačovou kriminalitou, a to trestná činnost mající souvislost s kyberprostorem. Kyberprostorem je míněna oblast počítačových systémů a sítí, v níž jsou ukládána data a v níž probíhá on-line komunikace. V podstatě jde o Síť, neidentifikovatelný prostor mezi zařízeními, neurčitý prostor kde se odehrává veškeré dění, tedy zábava, komunikace, obchod a samozřejmě i zločiny. Do této oblasti tudíž spadá i počítačová kriminalita páchaná v souvislosti s „Internetem“, potažmo s „World Wide Web“.

2.1 HISTORIE INFORMAČNÍ KRIMINALITY

K rozmachu informační kriminality v pravém slova smyslu došlo až na počátku 80. let 20. století s masivnějším rozšířením počítačů mezi jednotlivé uživatele. U informační kriminality tak můžeme sledovat určitá vývojová stádia související s vývojem počítačové technologie. Fenoménem informační kriminality se zabývají různé zdroje se svou vlastní etapizací vývoje. Dle mého názoru nejpřehlednější etapizaci uvádí Matějka ve své publikaci, kde dělí informační kriminalitu do tří etap:

- Pravěk – období do uvedení prvního PC na trh v roce 1981,
- Středověk – období od roku 1981 do případu Citibank v roce 1994,
- Novověk – období od 1994 dodnes. [15]

[13] http://eur-lex.europa.eu/LexUriServ/site/en/com/2000/com2000_0890en01.pdf, 23.8.2011
[14] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, 25.8.2011
[15] MATĚJKA, M.: Počítačová kriminalita. Praha: Vydavatelství Computer Press, 2002, s. 17

Počítačový pravěk

Je otázkou od kdy mluvit o informační kriminalitě v době kdy výpočetní technika nebyla mezi uživateli vůbec rozšířena. Přesto i v tomto období docházelo k jednáním, ve kterém lze již znaky „informační kriminality“ vysledovat. Zrod počítačového věku nastal v roce 1946, kdy byl sestrojen první elektronkový počítač ENIAC. Tehdejší počítače však zabíraly téměř celou místnost a vzhledem k nákladům na pořízení byly doménou opravdu velkých institucí a firem. Nelze tak mluvit o možnostech jejich kriminálního využití.

Tehdejší programátoři byli při práci se sálovými počítači nuceni pracovat s často nepříliš dobře fungujícími programy. Bylo tak nutné tyto programy upravovat svépomocí. Takovéto zásahy do programu s cílem lepší funkce se označovaly termínem „hack“. Odtud i programátoři upravující programy k lepší efektivitě byli nazýváni „hackeři“. Tento termín však postupem času získal jiný, negativní obsah. V současnosti jsou tak označováni pachatelé útoků proti počítači.

U nás je ze sedmdesátých let znám jeden z prvních případů informační kriminality, kdy nespokojený pracovník Úřadu důchodového zabezpečení poškozoval magnetem záznamy na magnetických páskách. Nikterak ojedinělé nebyly ani machinace s výpočetní technikou v mzdových účtárnách, či jiných pracovištích umožňujících manipulaci s penězi. V 80. letech bylo zaznamenáno 14 takových deliktů.[16]

Počítačový středověk

V roce 1981 byl na trh uveden první počítač typu IBM PC jeho velikost a stavebnicové uspořádání předznamenalo brzké rozšíření mezi běžné uživatele. Propojení počítačů pomocí modemů a telefonních linek do sítí na sebe nenechalo dlouho čekat a došlo tak k rozšíření předchůdce dnešního Internetu v podobě systému BBS.

Toto období bylo charakteristické změnou typického pachatele počítačového zločinu. Zpočátku se jednalo o počítačové fandy, pro něž představoval průnik do systému intelektuální výzvu. Cílem pachatelů nebyl již zisk slávy, ale zisk peněz.

„Středověk“ byl také charakteristický nástupem počítačových virů. Nejstarší infiltrací byli trojské koně. Svůj boom zažila i rozsáhlá oblast informační kriminality – počítačové pirátství. Prudký pokles cen CD-ROM mechanik a následně i CD-R mechanik tak dovolil téměř každému uživateli počítače stát se potenciálním počítačovým pirátem.

[16] SMEJKAL, V.: Informační a počítačová kriminalita v České republice, MV ČR 1999.

Počítačový novověk

Éru středověku ukončil asi nejznámější případ počítačové kriminality – připad Citibank. Ruská hackerská skupina pronikla do počítačů Citibank a na své účty postupně převedla částku kolem 10 miliónů dolarů.[17]

Pro období novověku bylo charakteristické masové rozšíření počítačů zejména na platformě PC s operačním systémem Microsoft Windows. Navíc docházelo k rozšíření sítí typu Internet. Z původní domény akademických kruhů se Internet stal komerčním nástrojem, kterým protéká množství peněz. Počítačoví nadšenci byli tak vystřídáni chladnými profesionály sledujícími jen dosažení zisku.

Počítačové pirátství v éře „novověku“ bylo dovedeno k dokonalosti. Může za to zcela nový přístup ke sdílení dat. Zatímco dřív byl Internet organizován hlavně na principu klient-server, kdy poskytovaná data musela existovat na konkrétním serveru, nově se dá připojit způsobem peer-to-peer (P2P), tedy přímo ke konkrétnímu uživateli nabízejícímu daný obsah. Na tomto principu pracoval program Napster určený ke sdílení hudby v digitálním formátu.

Mezi relativně mladou kriminální aktivitou jsou tzv. Denial of Service (odepření přístupu) toky. Na rozdíl od počítačového viru se zde ovšem pachatel nesnaží cílový počítač infikovat, ale sérií opakovaných požadavků ho zahltit, případně vyřadit z provozu.[18]

2.2 TYPICKÉ ZPŮSOBY PÁCHÁNÍ INFORMAČNÍ KRIMINALITY

Chmelík ve své publikaci uvádí následující formy zneužívání Internetu:

- zneužívání platebních karet (carding) - pachatel nelegálním způsobem získá potřebné údaje a zneužije je k platbě za zboží či služby pro svou osobu na úkor majitele platební karty,
- podvodné obchodování se zbožím a službami s požadavkem okamžitého placení elektronickou cestou,
- přesměrování telefonického spojení na dražší tarif – zejména při volání na stránky s pornografickým obsahem je uživateli sítě nainstalován tzv. dialer, který bez vědomí uživatele sítě veškeré další spojení přesměrovává na telefonní čísla s dražším tarifem,
- nabízení účasti v různých podvodných hrách, sázkách, loteriích,
- neoprávněné monitorování elektronické komunikace (sniffing),

[17] MATĚJKA, M.: Počítačová kriminalita. Praha: Vydavatelství Computer Press, 2002, s. 32
[18] MATĚJKA, M.: Počítačová kriminalita. Praha: Vydavatelství Computer Press, 2002, s. 35

- další aktivity mající charakter kriminality obecné, jako je šíření pornografie, terorismu či extremistických aktivit. [19]

2.3 ROZDĚLENÍ INFORMAČNÍ KRIMINALITY

V souvislosti se samotným vývojem informačních technologií se setkáváme s množstvím náhledů na třídění informační kriminality. Tříděním na trestnou činnost páchanou proti počítači a trestnou činnost páchanou s použitím počítače by si odborníci vystačili v dobách rozšiřování osobních počítačů v 80. a první polovině 90. let minulého století. Řada skutků by však z dnešního pohledu spadala do obou kategorií, nemluvě o jednáních, které jsou páchány proti počítači, ale jen jako objektu majetkové trestné činnosti.

Obecně lze říci, že pomocí počítače lze spáchat jakýkoli trestný čin, který nevyžaduje pachatelovu přítomnost na místě činu. Samozřejmě lze také využít informačních technologií k ostatním trestným činům, například ve stádiu přípravy, pro komunikaci mezi pachateli apod.

Požár člení informační kriminalitu na jednání **nová** oproti jednáním **tradičním.** Nová jednání se objevila až s nástupem informačních technologií, před tím o nich vůbec nemohla být řeč. Počítač/kyberprostor je jejich nutnou, podstatnou součástí. Oproti tomu tradiční jednání dříve nic takového ke spáchání nepotřebovala (podvod, padělání), avšak úspěšně se přizpůsobila podmínkám informační společnosti.[20]

Rozdělení trestné činnosti podle Úmluvy o počítačové kriminalitě (Convention on Cybercrime) přijaté v roce 2001 Radou Evropy (European Treaty Series No. 185), kterou ČR podepsala 9. 2. 2005, ale dosud neratifikovala (dále jen „Úmluva“). Dělí informační kriminalitu do čtyř oblastí:

1. **Trestné činy proti důvěřivosti, integritě a dostupnosti počítačových dat a systémů:** neoprávněný přístup, neoprávněné odposlouchávání, narušování dat, zasahování do informačních systémů, zneužití zařízení.
2. **Trestné činy se vztahem k počítači:** počítačové padělání, počítačový podvod.
3. **Trestné činy se vztahem k obsahu počítače:** dětská pornografie.
4. **Trestné činy související s porušováním autorského práva a práv s ním související.** [21]

---

[19] CHMELÍK, J. a kol. *Rukověť kriminalistiky*. Vyd. Plzeň: Aleš Čeněk 2005. ISBN 80-86898-36-9.
[20] POŽÁR, J. *Základy teorie informační bezpečnosti*. 1. Vyd. Policejní akademie České republiky v Praze, 2007. ISBN 978-80-7251-250-8.
[21] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, 25.8.2011.

Rozdělení podle kriminalisticko taktických hledisek:[22]

1. **Porušování autorského práva** – softwarové pirátství (§ 270 TZ),
2. **Poškození a zneužití záznamu na nosiči informací** (§ 230 TZ),
   - útok z vnějšku subjektu,
   - útok zevnitř subjektu,
   - útoky kombinované (z vnějšku i zevnitř),
3. **Ostatní počítačová a informační trestná činnost**
   - trestné činy, které IT využívají jako prostředek k páchání trestných činů, nikoliv jako přímý objekt zájmu pachatele, i když není vyloučeno, že objektem zájmu mohou být počítačová data.[23]

Smejkal dělí trestné činy v oblasti informatické kriminality (mezi předměty ochrany zahrnuje také telekomunikační systémy) do tří kategorií:

1. **Trestná činnost ve vztahu k hmotnému majetku** (tj. k počítači, jeho příslušenství, telekomunikačním prostředkům a jiným nosičům informací) – *majetková kriminalita*.
2. **Trestná činnost ve vztahu k nehmotnému majetku** (tj. k programům, databázím, datům, informacím zpracovávaným prostřednictvím informačních a telekomunikačních systémů) – *informatická kriminalita*. [24]
3. **Trestné činnosti, při nichž je počítač prostředkem k jejich páchání** (není vyloučen ani souběh s jednáními podle bodu 2.) – může se jednat např. o *hospodářskou kriminalitu* (např. podvody, zpronevěra) nebo o jinou trestnou činnost podle TZ (např. pomluva, podněcování a schvalování trestného činu).[25]

Pramenem právní úpravy informační kriminality v České republice je trestní zákoník. V současném Trestním zákoníku (dále jen TZ) je zakotvena řada trestných činů, které postihují různé druhy počítačové a informační kriminality. Jedná se zejména o skutkové podstaty trestných činů:[26]

---

[22] Dle analýzy Ministerstva vnitra České republiky

[23] Ministerstvo vnitra České republiky. *Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení* [online]. c2005. [cit. 2011-09-08]. Dostupné z WWW: <http://www.mvcr.cz/dokument/2006/informacni.doc>.

[24] SMEJKAL, V.: *Informační a počítačová kriminalita v České republice*. MV ČR 1999.

[25] SMEJKAL, V. *Právo informačních a telekomunikačních systémů*. 2., aktualiz. a rozš. vyd. Praha: C. H. Beck, 2004. s. 694

[26] ÚZ Úplné znění. Trestní zákoník 2010. vyd. Sagit,a.s. ISBN 987-80-7208-736-5.

1. **§ 180 Neoprávněné nakládání s osobními údaji.**

   (1) Kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají.

2. **§ 182 Porušování tajemství dopravovaných zpráv.**

   (1) Kdo úmyslně poruší tajemství a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením, b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovatelnému účastníku nebo uživateli, který zprávu přijímá, nebo c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data.

3. **§ 184 Pomluva.**

   (1) Kdo jinému sdělí nepravdivý údaj, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu.

4. **§ 191 Šíření pornografie.**

   (1) Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, v němž se projevuje násilí či neúcta k člověku, nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem.

5. **§ 192 Výroba a jiné nakládání s dětskou pornografií.**

   (1) Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak zneužívá dítě.

6. **§ 205 Krádež.**

   (1) Kdo si přisvojí cizí věc tím, že se jí zmocní, a a) způsobí tak na cizím majetku škodu nikoliv nepatrnou, b) čin spáchá vloupáním, c) bezprostředně po činu se pokusí uchovat si věc násilím nebo pohrůžkou bezprostředního násilí, d) čin spáchá na věci, kterou má jiný na sobě nebo při sobě.

7. **§ 206 Zpronevěra.**

   (1) Kdo si přisvojí cizí věc nebo jinou majetkovou hodnotu, která mu byla svěřena, a způsobí tak na cizím majetku škodu nikoli nepatrnou.

8. § 207 Neoprávněné užívání cizí věci.

(1) Kdo se zmocní cizí věci nikoli malé hodnoty nebo motorového vozidla v úmyslu je přechodně užívat, nebo kdo na cizím majetku způsobí škodu nikoliv malou tím, že neoprávněně takové věci, které mu byly svěřeny, přechodně užívá.

9. § 209 Podvod.

(1) Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu, nikoli nepatrnou.

10. § 230 Neoprávněný přístup k počítačovému systému a nosiči informací.

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části.

11. § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat.

(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části.

12. § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat, a tím způsobí na cizím majetku škodu.

13. § 234 Neoprávněné opatření, padělání a pozměnění platebního prostředku.

(1) Kdo sobě nebo jinému bez souhlasu oprávněného držitele opatří, zpřístupní, přijme nebo přechová platební prostředek jiného, zejména nepřenosnou platební kartu

identifikovatelnou podle jména nebo čísla, elektronické peníze, příkaz k zúčtování, cestovní šek nebo záruční šekovou kartu.

14. **§ 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi.**

    (1) Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi.

15. **§357 Šíření poplašné zprávy**

    (1) Kdo úmyslně způsobí nebezpečí vážného znepokojení alespoň části obyvatelstva nějakého místa tím, že rozšiřuje poplašnou zprávu, která je nepravdivá.

Jelikož je výše uvedená problematika z hlediska historie kriminality novým oborem a v oblasti IT dochází k neustálému vývoji a výskytu nových hrozeb a jevů, objevují se stále častěji případy, na které český právní řád neumí reagovat. Tyto nové fenomény lze pak jen velmi obtížně podřídit stávajícím skutkovým podstatám. Otázkou tedy zůstává, zda výše uvedené skutkové podstaty TZ skutečně pokryjí všechny páchané delikty v oblasti počítačové a informační kriminality.

2.4 ZÁKLADNÍ SKUPINY INFORMAČNÍ KRIMINALITY

V současné době nemá pojem „informační kriminalita“ žádný oficiálně definovaný obsah, ale existuje více různorodých pojetí podle toho, z jakého hlediska se autoři na problém dívají. Dle Požára lze informační kriminalitu dělit z hlediska postavení počítače při páchání trestné činnosti na tyto základní skupiny:

Trestná činnost ve vztahu k softwaru, datům, uloženým informacím, k počítači a jeho programovému vybavení a datům v něm jako cíl útoku, jako předmět trestného činu

a) Hacking

Hacking je považován odborníky za druhou nejvýraznější oblast informační kriminality ihned po porušování autorských práv. Ve své podstatě jde o průnik do systému jinou než standardní cestou a znamená obejití nebo prolomení ochrany.[27] Hackeři se vyvinuli

[27] POŽÁR, J. *Základy teorie informační bezpečnosti*. 1. Vyd. Policejní akademie České republiky v Praze, 2007. ISBN 978-80-7251-250-8.

z programátorů snažících se zjistit, jak systém funguje, případně odstranit chyby a něco nového se naučit. Postupem času tak vznikly dvě základní skupiny „hackerů“. První, která svou činností nemá v úmyslu cílový systém jakkoliv poškodit, a druhá, která sleduje jen materiální cíle (viz zmíněný případ Citibank). Politicky motivované napadání internetových stránek se nazývá hacktivismus. V posledních letech se stále více a více rozvíjí. Je pravděpodobné, že mimo jednotlivce a organizované skupiny se do této činnosti zapojují i profesionálové ze speciálních služeb.

Proniká-li hacker do systému za účelem krádeže osobních údajů, může se jednat o trestný čin neoprávněného nakládání s osobními údaji, je-li cílem odcizení peněz z bankovního účtu, může jít o trestný čin krádeže, apod. Naopak bez postihu bude hacker, jehož aktivita bude směřovat k testování bezpečnostního systému a bude prováděna na žádost jeho tvůrce. V tomto případě zde chybí trestněprávně relevantní následek, tedy porušení nebo ohrožení hodnot, které jsou objektem trestného činu. Hacking na žádost tak nemůže být označen jako trestný čin, neboť žádné ohrožení nepůsobí, naopak případné ohrožení eliminuje.

b) Narušování systému

Do této skupiny jednání řadíme některé druhy kybernetických útoků, u nichž dochází k závažnému narušení nebo přerušení fungování softwaru, respektive počítače. Konkrétní případy zahrnují především DoS (Denial of Service) útoky. Rozumí se jím takový neoprávněný zásah do počítače, který způsobí jeho vyřazení z činnosti nebo snížení výkonu, ať už zahlcením počítače záplavou nesmyslných požadavků, nebo zahlcením spojovací cesty daty, čímž je oprávněným uživatelům znemožněno počítač využívat.[28] Varianty DoS útoků: Mass mailing list, E-mail bombs, Fork bomb.

c) Prolamování ochrany systémů (cracking)

Prolamovače hesel jsou programy používané k prolomení ochrany nebo autorizace, která je prováděna (statickým) heslem. Prolamovačů využívají oprávnění uživatelé, kteří zapomněli heslo k systému nebo jednotlivému dokumentu, systémoví administrátoři, kteří jimi kontrolují, zda si uživatelé nevolí nevhodná hesla, ale i hackeři k získání protiprávního přístupu nebo dešifrování cizích dat. Na Internetu je volně dostupných několik prolamovačů. Výroba prolamovače hesel není v současnosti trestná.

[28] http://cs.wikipedia.org/wiki/Denial_of_Service, 20.8.2011

Malware je společný název pro škodlivý kód, tedy software nebo jiná data, jejichž účelem je uškodit počítači nebo jeho obsahu nebo je jinak zneužít. Někteří sem řadí i programy, které pouze umí infiltrovat počítač bez souhlasu jeho uživatele. Pro hrubou představu uvádím základní druhy malwaru (kategorie nejsou vzájemně uzavřené a definice volné):

Viry jsou programy, které se umí samy šířit bez vědomí a obvykle proti vůli uživatele počítače. Své jméno dostaly podle toho, že jsou vždy součástí hostitelského souboru. Jejich účinky se pohybují od prostého zabírání paměti a možných výpadků v důsledku chyb (*bugs*) v nich obsažených až po ztrátu dat a nutnost reinstalace operačního systému. Existují viry se schopností měnit svůj „tvar" po každém přenosu na dalšího hostitele (polymorfní viry).

Trojský kůň je neškodně nebo přitažlivě vypadající program, například hra, který po spuštění vypustí svůj „náklad", obvykle vir nebo spyware. Může také otevírat porty (viz port scannery), čímž umožní nebo usnadní útok hackerovi. Počty nových trojských koní zůstávají od roku 2003 na vysokých hodnotách.

Spyware je software, který bez vědomí uživatele počítače odesílá skrz Internet důvěrné informace, například jaké webové stránky uživatel navštěvuje. Počet nového spywaru od roku 2002 strmě narůstá.

Dialer přesměruje vytáčené připojení k Internetu na draze placenou linku, přičemž takto získané prostředky plynou do kapsy tvůrce dialeru.

Nepříjemným a relativně novým malwarem je tzv. rootkit.[29] Obecně se jím míní jakýkoli program, který „zametá stopy" po nekalé činnosti jiného malwaru, a tím, že je součástí operačního systému, se stává prakticky neodhalitelným.

Spamming znamená rozesílání nevyžádaných zpráv elektronickou poštou s reklamním či propagačním obsahem. Díky spammingu může docházet jednak k zahlcení mail-serverů nebo k narušení řádného fungování interaktivních sítí.[30]

Trestné činnosti, při nichž je počítač prostředkem k jejich páchání

Nejčastějším případem jsou podvody realizované formou neoprávněného převodu finančních prostředků na účet, který byl k tomu zvlášť založený. Hlavními cíli útoků jsou velké

[29] http://en.wikipedia.org/wiki/Rootkit, 25.8.2011

[30] OTEVŘEL, P. *Spamming a některé otázky šíření obchodních sdělení* [online]. 2006. [cit. 2011-09-08]. Dostupné z WWW: <http://www.pravoit.cz/view.php?nazevclanku=spamming-a-nektere-otazky-sireni-obchodnich-sdeleni&cisloclanku=2005120001>.

banky, telekomunikační společnosti a další. Zhruba 70 % narušení systémů má souvislost se zaměstnanci postižených firem.[31]

Sociální inženýrství (social engineering) je souhrnný pojem pro metody zneužití lidského faktoru při páchání informační kriminality (např. phishing, pharming). Jedná se o velmi dostupný a jednoduchý nástroj, který je však také velmi efektivním nástrojem podvodu. Autoři phishingových zpráv velmi výrazně využívají právě důvěřivost uživatelů. Americké studie zjistily, že v jednotlivých kampaních bývá až 5 % napálených uživatelů. V některých případech bývá jejich počet dokonce i vyšší. Těžištěm zájmu přestávají být čísla telefonních karet, ale citlivé údaje o platební kartě, krádež přístupového jména a hesla. S takovými údaji lze potom snadno manipulovat s bankovními konty uživatelů platebních karet. Tyto uvedené podrobnosti o bankovních účtech získávají pachatelé tak, že vytvoří falešné webové stránky a následně rozešlou falešné e-maily, jejichž prostřednictvím vylákají od klientů čísla z jejich účtů. Po získání přístupu následuje zneužití nebo vykradení účtu oběti.

a) Phishing

Phishing, někdy překládaný do češtiny jako „rhybaření“ spočívá v získávání důvěrných a citlivých informací (hesla, detaily o kreditních kartách) za účelem získání přístupu a následném obohacení se z cizích zdrojů. Nejčastější a nejznámější formou je zasílání podvodných emailových zpráv. [32]

Jak vyplývá ze studie společnosti McAfee o virtuální kriminalitě, začaly phishingové útoky v USA v prosinci 2003 a od té doby rapidně stoupá jejich nárůst o 50 % měsíčně. V následujícím roce 2004 se tyto útoky objevily ve Velké Británii a Austrálii, v červenci v Brazílii a Německu a v srpnu ve Francii. V této době se také objevily na Internetu návody pro drobné hackery, jak phishingový útok provést.[33]

Podle výše uvedeného zdroje dvě třetiny všech webových stránek, které využívají phishing, se nacházely na serverech v USA, Jižní Koreji a v Číně. Okolo 15 % phishingových útoků bylo provedeno v Evropě, zejména v Nizozemí, v Turecku, Chorvatsku, ale také Polsku, Portugalsku, Španělsku, Švédsku a Velké Británii.

Výjimkou ovšem není ani Česká republika. V roce 2006 došlo k napadení hned několika bankovních institucí, a to opakovaně. Banky na tuto situaci reagovaly přijetím

---

[31] HOUDEK, S. *Světem informačních technologií se šíří vlna kriminality*. Dostupné na WWW.ihned.cz

[32] BAUDIŠ, P.: Rhybaření. Chip, 2006, č.04, s.14

[33] McAfee. *Zpráva společnosti McAfee o virtuální kriminalitě: první celoevropská studie o organizovaném zločinu a internetu* [online]. 2004 [cit. 2011-09-08].
Dostupné z WWW: <http://www.fi.muni.cz/~xbitto/McAfee_kriminalita.pdf>.

opatření, které má za úkol zvýšit zabezpečení klientů daných institucí při dálkové správě jejich účtů.[34]

První česky psaný phishingový email byl rozeslán klientům bankovního ústavu CitiBank v roce 2006. Jeden z posledních phishingových útoků byl zaznamenán 15. 3. 2007 v podobě napadení internetového bankovnictví České spořitelny.[35] V příloze 1 uvádím příklad phishingového dopisu.

b) Pharming

Pharming představuje daleko nebezpečnější způsob útoku. Pachatel při něm nejprve hackuje DNS server odpovědný za přiřazování doménových jmen IP adresám tak, aby odkazoval na podvržené stránky. Oběť tak v podstatě nemá o podvrhu žádné podezření. Pharming má následně stejný průběh jako Phishing, od nějž se liší právě pouze nutností hacknutí DNS serveru.

Samotný Phishing a Pharming lze kvalifikovat jako přípravu krádeže podle ustanovení § 20 odst. 1 TZ. Následné vykradení účtu pak jako krádež podle § 205 odst. 1 TZ a spadají pod majetkovou trestnou činnost.

c) Cyberstalking a kyberšikana

Kyberšikana je druh šikany, který využívá elektronické prostředky, jako jsou mobilní telefony, e-maily, pagery, Internet, blogy a podobně. Řada jejích projevů může spadat do oblasti kriminálních činů. Její nejobvyklejší projevy představuje zasílání obtěžujících, urážejících či útočných e-mailů a SMS, popřípadě může kyberšikana sloužit k posilování klasických forem šikany, nejčastěji prostřednictvím nahrání scény na mobilní telefon a jejího následného rozeslání známým dotyčného, popřípadě vystavení na Internetu.

d) Hoaxes

Škodlivé šíření informací, nepravdivých varování. Je to nevyžádaná e-mailová, nebo ICQ zpráva, která uživatele varuje před nějakým virem, prosí o pomoc, informuje o nebezpečí, snaží se ho pobavit apod. Běžní uživatelé se mohou na Hoax nachytat a nevědomky a v dobré

[34] Ministerstvo vnitra České republiky. *Zpráva o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území ČR v roce 2010: (ve srovnání s rokem 2009)* [online]. 2007 [cit. 2011-09-08]. Dostupné z WWW : <http://www.mvcr.cz/dokument/2007/verejnyporadek/zprava06.pdf>.

[35] ZÁMEČNÍK, P. Podvodná stránka České spořitelny. *Měšec.cz* [online]. 19.3.2007. [cit. 2011-09-08]. Dostupné z WWW: <http://www.mesec.cz/clanky/podvodna-stranka-ceske-sporitelny/>.

víře jej následně posílat dál. Správně napsaná falešná zpráva dokáže ovlivnit chování lidí, vzbudit v nich pocity úzkosti, strachu, nebo je přesvědčit o nějaké mystifikační události.

e) Carding – zneužívání platebních karet

Ke zneužívání platebních karet dochází různými způsoby. Tím nejjednodušším způsobem je krádež karty samotné. V minulosti docházelo také často k využívání tzv. generátorů (programů), které dokázaly vygenerovat číslo kreditní karty na základě odcizeného algoritmu.

f) Pornografie

Šíření pornografie (dříve za pomocí časopisů, fotografií, filmů, videonahrávek; od konce osmdesátých let z velké části za pomocí počítačových sítí a Internetu) nabývá na síle. Internet je využíván jednak ke snadné výměně informací, k obchodu s fotografiemi či videonahrávkami obsahujícími pornografii, popř. k peněžním transakcím. Právě díky Internetu a jeho globální povaze nastává problém s postihem tohoto jednání. V některých zemích není šíření pornografie vůbec kvalifikováno jako trestný čin, a v těch zemích ve kterých ano, jsou webové stránky s nelegálním obsahem stejně viditelné.[36]

Pokud jsme vyslovili tezi, že rozvoj informačních technologií a Internetu umožnil rychlejší rozvoj i v jiných oblastech trestné činnosti, musíme zmínit šíření závadného obsahu. Zejména to platí o šíření pornografie, potažmo dětské pornografie. Ta se sice šířila i v dobách před tím, ale možnosti rozšiřování byly dosti omezené. Teprve kybernetický věk přinesl nové možnosti, čehož právě porno průmysl využil snad bezezbytku.

Z mezinárodního hlediska je problematika zmíněna v článku 9 Úmluvy o počítačové kriminalitě, která stranám postihuje nabízení, zpřístupňování, šíření, posílání dětské pornografie skrze počítačový systém a výrobu dětské pornografie za tímto účelem a konečně také získávání a držení. Vzápětí se však v úmluvě vyhrazuje stranám právo neužít ustanovení o získávání a držení dětské pornografie pro vlastní potřebu uživatele, stejně jako výhradu, že za dětskou pornografii nebudou považovat zobrazení osoby, která se pouze jeví být dítětem, ani realistické znázornění (neexistujícího) dítěte.

[36] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002.

g) Extremismus

Neméně závažným problémem je na Internetu také šíření extremismu. Snad veškeré myslitelné extremistické skupiny se snaží prezentovat svoje názory právě na síti Internet. Informační technologie v tomto směru odstranily mnohé komunikační těžkosti a jsou masově využívány i ke komunikaci mezi jednotlivými částmi organizací. Internet bývá také díky jeho snadné přístupnosti a globální povaze zneužíván k šíření neonacistických, rasistických a jiných xenofobních idejí. Velkou výhodou Internetu pro tyto organizace je také samozřejmě možnost snadné ilegální komunikace mezi jejími jednotlivými členy.[37]

Jak vyplývá ze samostatné přílohy *Zprávy o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území České republiky v roce 2005,* ubyly oproti minulým letům extremistické publikace zejména v tištěné podobě. [38] Naopak stále častěji je různá rasistická, antisemitská a další nenávistná propaganda obsažena a nabízena v elektronických časopisech a brožurách prostřednictvím Internetu.

K ochraně před odhalením používají autoři nelegálních webových stránek různé metody k utajení své identity, jako je např. kryptografie[39] nebo anonymizéry.[40]

Zajímavé je, že extremismus na Internetu je v každé zemi pojímán odlišně. Matějka udává, že zatímco anglosaské pojetí trestá zásadně skutky a nikoli slova, kontinentální Evropa posuzuje např. i tzv. verbální delikty, které je možné spáchat slovem

h) Vydírání a elektronické výpalné

Majitelé systémů připojených k Internetu jsou zastrašováni hrozbami průniků do systému, zničení či zneužití dat atd. Jelikož žádný systém si nemůže být jist dokonalým zabezpečením, mnohé instituce raději zaplatí elektronické výpalné za ochranu.

i) Podvody a zpronevěra

Do této skupiny spadají bankovní podvody, počítačová zpronevěra, ke které dochází zneužitím pravomoci od zaměstnanců bank, nebo administrátorů vlastnících přístupová práva.

---

[37] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha : Computer Press, 2002. s. 67

[38] Ministerstvo vnitra České republiky. *Informace o problematice extremismu na území České republiky v roce 2005* [online]. c2006. [cit. 2011-12-21]. Dostupné z WWW: < http://www.mvcr.cz/dokument/2006/extrem05.pdf>.

[39] *„Kryptografie neboli šifrování je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí.* viz Wikipedie: Otevřená encyklopedie. *Kryptografie* [online] . [cit. 2011-10-25]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Kryptografie>.

[40] Anonymizer je jednoduchá aplikace, která dokáže skrýt např. reálnou IP adresu PC, nebo stát, ve kterém se uživatel Internetu pohybuje.

Zaměstnanec, který má přístup k finančním prostředkům, je v tomto případě použije ke svému obohacení, a to za pomoci počítače.

Kromě klasického pirátství a hackingu zaznamenala Česká republika za dobu své porevoluční existence několik dalších případů, například provozování her typu letadlo s použitím počítače, či Internetu. Známá je především činnost tzv. Kyjovské buňky z počátku 90. let, kdy se jednalo o letadla organizovaná především na jižní Moravě, do kterých se tehdy zapojilo zhruba 10 000 občanů, přičemž zisk v průměru okolo 150 000 Kč na hlavu si mezi sebou rozdělilo pouze prvních 15 - 20 účastníků - organizátorů hry. Všichni organizátoři byli stíháni pro podvod.

Mezi nové druhy online podvodů se řadí nákup prostřednictvím Internetu. Falešné webové stránky, které nabízejí nejrůznější zboží, slouží také k odcizení informací z kreditních karet důvěřivých jedinců. Uživatel falešného e-shopu se tak může stát obětí hned dvakrát. V prvním případě při platbě kreditní kartou (falešná webová stránka oznámí, že transakce nebyla provedena), ve druhém případě, když zaplatí poštovní poukázkou za neexistující zboží.[41]

Také se může jednat např. o nabídky sexuálních služeb, které jsou vystaveny na webových stránkách – tzv. freewebech,[42] nebo formou inzerátů v „seznamkách“. Tyto služby pak bývají nabízeny za poslání čísla dobíjecího kuponu předplacené karty pro síť GSM.

Známé jsou také případy podvodných finančníků, kteří se snaží nalákat důvěřivé jedince na vysoké zisky různých obchodů s cennými papíry nebo měnami. Ke své prezentaci používají tito podvodníci taktéž freeweby; adresy mají registrované na free-mailech a velmi vysoká hodnocení od agentur bývají povětšinou vymyšlená.

Trestná činnost ve vztahu k počítači (hardwaru)

Podle odborníků se výše uvedená problematika týká počítačové a informační kriminality pouze rámcově, zejména pokud se jedná např. o krádež počítače s cílem získat hardware.

---

[41] JÍROVEC, J. Nový druh podvodů na Internetu. *Počítač pro každého: Nejprodávanější počítačový časopis v ČR* [online]. c2005. [cit. 2011-10-25].
Dostupné z WWW: <http://www.ppk.cz/novinky/?clanek=145>.

[42] Freeweby – servery, které poskytují provozování a ukládání webstránek zdarma (freewebhosting). Např. www.webzdarma.cz, www.ic.cz, www.webpark.cz, www.php5.cz atd.

Trestná činnost ve vztahu k programu jako autorskému dílu

Svou charakteristikou by tyto delikty mohly patřit do druhé kategorie trestných činů, vzhledem k jejich četnosti výskytu jsou zařazeny v samostatné skupině.

Toto možné legislativní dělení počítačové kriminality není samozřejmě konečné a uzavřené. V průběhu technického rozvoje se budou vyskytovat další nové útoky na data a bude nutné tyto skutky kodifikovat.

a) Porušování autorských práv počítačové pirátství

Do kategorie porušování autorských práv spadá softwarové (počítačové) pirátství, které patří mezi nejrozšířenější protiprávní činnost počítačové a informační kriminality vůbec.

V 99 % případů si pod pojmem počítačová kriminalita představíme právě počítačové pirátství. Nové možnosti, které sebou přinesl internet a jeho rychlá přenosová kapacita, daly vzniknout fenoménu Warezu. Jde o šíření nelegálního softwaru pomocí vypálených CD nebo sdílení na FTP serverech a Peer-to-Peer sítích. Vývojem v oblasti informačních technologií, hlavně v oblasti komprimace dat, došlo k integraci pirátství v oblasti software a hudebních a filmových nahrávek. Na WWW stránkách warezových skupin tak najdeme jak nelegální software, tak i MP3 nahrávky, ale i filmy, často s pornografickým obsahem.

Motivem počítačových pirátů je jako vždy finanční prospěch generovaný distribucí nelegálních kopií na CD a DVD, většinou se tvářících jako originální nosiče. Naproti tomu Warezové skupiny svým jednáním zpřístupňují software a audio a videonahrávky zdarma, financování na své projekty získávají prodejem reklamy na svých WWW stránkách a symbiózou s online pornoprůmyslem.

b) Cybersquatting

Neboli doménové pirátství je spekulace s doménami za účelem zisku. Stává se, že konkurent užívá výrobky či služby označené doménovým jménem, které lze snadno zaměnit s doménou jiného subjektu; užívá doménové jméno, které je již vžité v souvislosti s konkrétním podnikatelem; nebo si zaregistruje doménu známého subjektu s cílem ji dotyčnému subjektu se ziskem prodat.[43] Existují už i aukční servery, kde lze snadno prodat

[43] KOMÁROVÁ, L. *Cybersquotting? Červená spekulantům (2. díl)* [online]. 2011. [cit. 2011-09-08]. Dostupné z WWW:< http://www.pravoit.cz/view.php?nazevclanku=cybersquatting-?-cervena-spekulantum-2-dil&cisloclanku=2007030004 >.

název domény nejvyšší nabídce. Případy cybersquattingu, se v poslední době vyskytují ve stále větší míře a stávají se používanější praktikou informační kriminality.

3. ODHALOVÁNÍ INFORMAČNÍ KRIMINALITY

Pro postihování informační kriminality lze najít ustanovení v celém Trestním zákoníku platném od 1. 1. 2010. Možná by stálo za úvahu při příští novele trestního zákoníku zvážit použití vyšší trestní sazby. V rekodifikovaném trestním zákoníku došlo k zařazením zvláštních skutkových podstat souvisejících s počítačovou kriminalitou (Trestné činy proti majetku - § 230, § 231, § 232 viz kap. 2.3). *Zatím je přísněji kvalifikováno, pokud je trestný čin spáchán se zbraní nebo v organizované skupině, ale to, že čin byl spáchán za pomoci počítače, nebezpečnost pachatelova jednání v očích trestního zákoníku nijak nezvyšuje.*

Boj proti informační kriminalitě si zaslouží daleko větší a koordinovanou pozornost, než jí dosud věnují zákonodárci, policejní orgány i uživatelé počítačů. Škody vzniklé v důsledku informační kriminality mají stále vzestupnou tendenci, přičemž používané metody a prostředky pachatelů jsou na velmi vysoké technické a intelektuální úrovni. Jako tomu je ve všech ostatních oblastech trestné činnosti, zločinci mají vždy náskok před ostatními. Mají motiv (touhu po zisku), prostředky a lidi (které si zaplatí většinou lépe než banka nebo stát). Mají výhodu volby času a způsobu.

Úkol orgánů činných v trestním řízení tedy v tomto případě především policie, spočívá v tom, aby zajistili takové množství důkazního materiálu, aby mohl být obžalovaný nad veškerou pochybnost usvědčen, shledán vinným a odsouzen. Bohužel ve virtuálním světě je právě tento požadavek klíčovým problémem dokazování počítačového zločinu.[44]

Vyhledávání forenzních důkazů v kybernetickém prostředí je velmi obtížné, mnohdy zcela nemožné. Prioritní otázkou je čas, který uběhl mezi útokem a začátkem objasňování. Vzhledem k technologiím internetu dochází k velmi rychlému ničení veškerých stop, které mohou vést k objasnění trestného činu. Protože se vždy jedná o neznámého pachatele, je zjištění IP adresy nejdůležitějším prvotním úkolem policejního orgánu či vyšetřovatele. Jedná se o vysoce odbornou práci vyžadující značnou znalost výpočetní techniky a technického vybavení.

Odborníci působící v oblasti prevence a represe proti informační kriminalitě budou muset mnohem více disponovat mezioborovými znalostmi (od informačních technologií přes bezpečnost informačních systémů až po právní disciplíny).

[44] MATĚJKA, M.: Počítačová kriminalita. Praha: Vydavatelství Computer Press, 2002, s. 83.

Jak vyplývá ze sborníku *Přítomnost a budoucnost krizového řízení*,[45] potýká se problematika informační bezpečnosti s řadou následujících jevů:

- Nedostačující vybavení specializovanou technikou (např. certifikovaný software, specializovaný hardware, atd.).
- Nedostačující odborné vzdělání příslušníků Policie České republiky v oblasti ICT.
- Neochota veřejné sféry vnímat investice do bezpečnosti kyberprostoru jako prioritní.
- Nedostačující vzájemné propojení mezi jednotlivými relevantními subjekty v rámci bezpečnostní komunity (roztříštěnost jednotlivých pracovišť).
- Neexistence důvěryhodného „neutrálního" subjektu, který by zastřešoval a zajišťoval vhodné podmínky pro bezpečnostní experty (servis, metodika, školení, zpětná vazba).
- Neschopnost bezpečnostních složek profesionálně úkolovat existující forenzní pracoviště.

Podle mého názoru je třeba daleko více sil přesunout do oblasti prevence, obrany počítačů a informačních systému, neboť jedině tak lze účinně bojovat proti tomuto druhu trestné činnosti, patřícímu do stále sílícího objemu kriminality bílých límečků a organizovaného zločinu. Důležité je též vytvořit systém právní výchovy a propagace v boji proti informační a počítačové kriminalitě, která zahrnuje celou veřejnost od žáků a studentů až po podnikatele.

3.1 BEZPEČNOSTNÍ POLITIKA ČR V BOJI PROTI POČÍTAČOVÉ A INFORMAČNÍ KRIMINALITĚ

Mezi aktuální bezpečnostní výzvy našeho státu patří oblast prevence a boje proti počítačové a informační kriminalitě. S rychlostí a anonymitou útoků na informační a komunikační systémy není snadné rozlišit, zda se jedná o teroristickou, kriminální či náhodnou trestnou činnost. Proto je velmi důležité správné fungování a nastavení pravidel informační bezpečnosti.

Jak vyplývá ze Zprávy o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území ČR v roce 2010: (ve srovnání s rokem 2009),[46] jsou poměry v oblasti počítačové

[45] JIROVSKÝ, V.– HNÍK, V. – KRULÍK, O. Kybernetické hrozby : Výzva pro moderní společnost. In *Přítomnost a budoucnost krizového řízení* [online]. Praha: T-Soft, 2006 [cit. 2011-09-08]. Dostupné z WWW: <http://www.mvcr.cz/bezpecnost/informacni/kyberneticke_hrozby.pdf>.

[46] více Ministerstvo vnitra České republiky. *Zpráva o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území ČR v roce 2010 : (ve srovnání s rokem 2009)* [online]. 2011 [cit. 2011-09-11]. Dostupné z WWW: http://www.mvcr.cz/soubor/iii-zprava2010-pdf.aspx

a informační kriminality v České republice hodnoceny jako zhoršující se. Nejčetnější útoky byly zaznamenány zejména v prostředí výměnných sítí, kde dochází ke sdílení digitalizovaných materiálů (porušování autorských práv), sdílení zakázaných pornografických materiálů a šíření extremistických materiálů.

3.2 PACHATELÉ A TRENDY INFORMAČNÍ KRIMINALITY

Pachateli informační kriminality jsou ve většině případů kvalifikované osoby, které důkladně rozumí dané problematice, mají možnost přístupu k informační a komunikační technice a zařízením, případně mají svou vlastní dokonalou výpočetní techniku. Metody na zakrývání jejich činnosti jsou obvykle složité a komplikované. Jsou to převážně studenti vysokých škol, kteří mají dobré technické a praktické zkušenosti. Dále jsou to podnikatelé, kteří v předmětu podnikání mají nákup a prodej výpočetní techniky.

Jak uvádí Chmelík většinou zaměstnanec dané firmy, si vytváří programy, jejichž pomocí vyvádí peníze z finančního ústavu či firmy na své účty zřízené u jiné banky. Nejčastěji dochází k pronikání do počítačových systémů (hacking) a krádež osobních údajů či jiných dat na počítači.[47]

Informační kriminalitu v současné době rozvíjejí ti, kteří v ní hledají zdroj obživy, což vede k narůstajícímu zapojení organizovaného zločinu. Dnešní firmy, organizace a státní instituce jsou na počítačích, počítačových sítích a obzvláště na internetu silně závislé. Bohužel internetový protokol TCP/IP je velice málo zabezpečený proti útokům zvenčí.

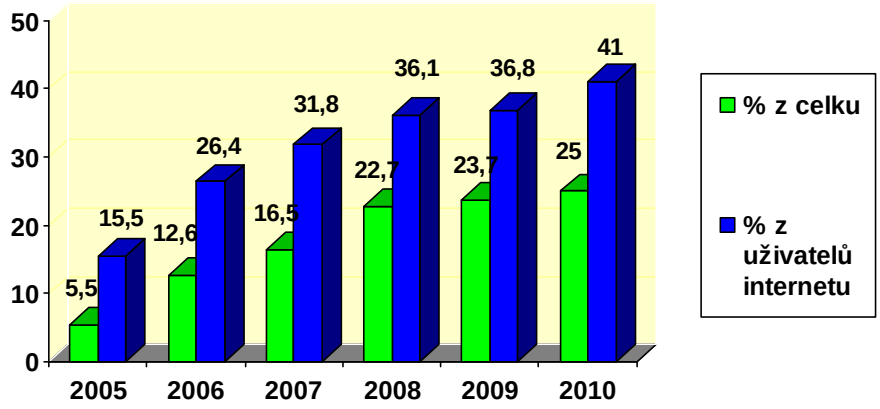
[47] CHMELÍK, J. a kol. *Rukověť kriminalistiky*. Vyd. Plzeň: Aleš Čeněk 2005. ISBN 80-86898-36-9.

4. INTERNETOVÉ OBCHODOVÁNÍ

V této kapitole bych v krátkosti objasnil pojem elektronický obchod a uvedl jednotlivé druhy.

Internetové obchodování je dynamicky se rozvíjejícím prvkem internetu, který si získává stále více příznivců. Západní Evropa má v nakupování na internetu sice náskok, avšak i uživatelé v České republice si na nákupy v e-shopech stále více zvykají. Podle údajů Českého statistického úřadu nakupovalo v roce 2005 přes internet pouze 6 % jednotlivců starších šestnácti let (17 % uživatelů internetu), v roce 2008 to bylo 21 % jednotlivců starších šestnácti let (39 % uživatelů internetu) v roce 2010 to bylo již 41 % jednotlivců starších šestnácti let (25,4 % uživatelů internetu). Nárůst uživatelů internetového nakupování je tedy opravdu výrazný. (viz Graf 1) Největší zájem je podle Českého statistického úřadu o vstupenky, elektroniku, oblečení, kosmetiku, knihy, atd.[48]

Graf 1 Uskutečněné nákupy přes internet



Zdroj: *Český statistický úřad*. Graf vlastní.

4.1 ELEKTRONICKÝ OBCHOD

V literatuře se můžeme setkat s více definicemi elektronického obchodu. Jedna z nich říká, že e-obchod je jakákoliv forma obchodování prováděná elektronicky, tzn. pomocí

[48] Jaké jsou nejčastější činnosti prováděné jednotlivci na internetu? *Český statistický úřad* [online]. 2009 [Cit. 2011-09-08]. Dostupný z: http://www.czso.cz/csu/redakce.nsf/i/domacnosti_a_jednotlivci

telekomunikačních sítí. Jiná definice chápe elektronické obchodování jako výměnu informací po elektronickém médiu za účelem uzavření obchodu nebo k jeho podpoře. [49]

Elektronický obchod nebo také E-commerce se soustřeďuje na nákup a prodej zboží a služeb. Jedná se o zajištění obchodních aktivit prostřednictvím informačních technologií. Zákazník si například vybere zboží prostřednictvím WWW stránek a okamžitě si je koupí a zaplatí. Všechny tři fáze výběr, nákup a platba se odehrávají bez jediného kontaktu s prodejcem. Komunikace mezi účastníky při tomto obchodu probíhá zčásti nebo zcela s využitím elektronických médií, počítačových sítí a telekomunikací pro potřeby obchodování.

Na internetu rozlišujeme podle jednotlivých subjektů, které se účastní nákupního procesu obchodní transakce:[50]

- **B2B** - Business-to-Business - obchodování mezi podniky navzájem. Jedná se o marketingové transakce mezi firmou a firmou, které zboží nebo služby nakupují převážně za účelem jejich dalšího prodeje nebo zpracování.
- **B2C** - Business-to-Consumer – označuje marketingové a komerční aktivity či transakce mezi firmou a konečným spotřebitelem zboží nebo služby.
- **C2C** - Consumer-to-Consumer - jde o obchod mezi dvěma neobchodníky. Např. prostřednictvím aukce mezi sebou prodávají a nakupují koncoví zákazníci.

4.2 TYPY OBCHODŮ

Mezi nejčastější typy internetových obchodů patří internetový obchod (e-shop), e-aukce a e-tržiště. Jednotlivé typy krátce definuji a ke každému z nich uvádím zástupce.

Internetový obchod

Nebo také e-shop, je počítačovou aplikací používanou v B2B nebo v B2C komerci v prostředí internetu spadající pod e-commerci, prostřednictvím níž dochází k prodeji fyzického zboží, v menší míře služeb. E-shop slouží především k nabízení a vyhledávání zboží nebo též služeb s možností si je na dálku objednat, k přijímání objednávek od zákazníků, k poskytování

[49] STEINOVÁ, M; HLUCHNÍKOVÁ, M; PŘÁDKA, M. *E-marketing II.: marketingová komunikace na internetu: elektronické obchodování.* 1. vyd. Ostrava: Vysoká škola báňská - Technická univerzita, 2003. 107 s. ISBN: 80-248-0351-8.

[50] STUCHLÍK, P; DVOŘÁČEK, M. *Marketing na Internetu*. 1. vyd. Praha: Grada, 2000. s. 50-62. ISBN: 80-7169-957-8.

informací o nabízeném zboží, ke zprostředkovávání plateb, k zajištění komunikace mezi prodejcem a nakupujícím a také k vyřizování reklamací.[51]

E-shopy jsou nejčastějším typem internetových obchodů. Mezi nejznámější patří např. Amazon.com, Buy.com, z českých např. Mall.cz, Alza.cz, Kasa.cz a mnoho dalších.

Typický obchod je tvořen katalogem, v němž je možné si vybírat jednotlivé položky. Tedy vybrat si určité zboží, nabízené pod určitou adresou (na určité nástěnce) včetně jeho popisu či fotografie nebo audio-vizuální prezentace.[52] Každá z nich obsahuje detaily. Když si zákazník vybere to, co chce koupit, nastane placení. Ve většině případů je při nakupování vyžadována registrace pro zjednodušení komunikace s obchodem, tak aby kupující nemusel vícekrát zadávat údaje a pro ověření identity zákazníka. Nákupní košík, který se často objevuje, je vlastně souhrnná objednávka vybraného zboží. Ta se pak u virtuální pokladny potvrdí a pokud obchod podporuje přímou komunikaci s bankou, respektive její aplikací přímého bankovnictví, zaplatí. Jsou ale možné i jiné způsoby placení. Objednané zboží je zasláno na dobírku poštou, nebo kurýrní službou, nebo je zákazník inkasován při potvrzení objednávky pomocí přímé platby. Druhá metoda je pro uživatele výhodná tehdy, když si kupuje službu, kterou může začít ihned využívat.

Internetové aukce

Elektronické aukce (e-aukce) jsou dnes hojně používané nástroje pro nakupování a prodej prostřednictvím internetu. Internetová aukce používá virtuálního prostředí Internetu s jeho výhodami a nevýhodami, kterými může být rychlost umístění nabídky a provedení aukce, možnost neustálého přístupu různých uživatelů k aukci. Na druhé straně dražený předmět může být pouze ve formě fotografie nebo prezentačního videa.

Jejich princip je stejný jako u obchodování na klasických aukcích, například těmi s uměleckými předměty nebo s akciovými podíly na burze cenných papírů. Na jednom místě se zde střetává nabídka na koupi a prodej a po uplynutí určitého časového limitu nejvyšší nabídka v aukci vítězí.[53]

Internetová aukce je online systém fungující na infrastruktuře Internetu, kdy uživatel může prodat položky, které vlastní, a může koupit položky nabízené jinými uživateli. Všechny

---

[51] Internetový obchod. *Wikipedie: otevřená encyklopedie.* [online]. 2011 [Cit. 2011-09-08]. Dostupný z: <http://cs.wikipedia.org/wiki/Internetov%C3%BD_obchod>.
[52] SMEJKAL, V. *Internet @ .§§§*. Vyd. 1. Praha: Grada, 1999. S. 168, ISBN 80-7169-765-6.
[53] E-tržiště. *B2B Centrum* [online]. c2011 [Cit. 2011-09-08]. Dostupný z: <http://www.b2bcentrum.cz/cs/e_marketplace>.

tyto služby lze provádět bez fyzické účasti obou aktérů. V těchto systémech kupec zpravidla nezná prodávajícího a naopak.[54]

Aukční servery fungují jako kombinace aukce a bazaru. Aukce zde neřídí vyvolávač jako u klasické aukce, ale robot, který kontroluje přihazování. Cenu zboží lze stanovit aukčním způsobem, kdy se zadá minimální cena jako vyvolávací a uživatelé k ní mohou přihazovat do vypršení časového limitu aukce. Zboží získá ten, kdo nabídne nejvyšší částku (anglická aukce). Druhou možností je pak stanovení bazarové ceny, která je stanovena pevně jako v obchodě či bazaru a zájemce tak má možnost koupit si vybrané zboží přímo. Třetí možností je aukce holandská, kdy je stanovena počáteční vysoká vyvolávací cena, která je potom licitátorem snižována až do chvíle, kdy je některý z účastníků ochoten určitou cenu po snížení zaplatit. Holandská aukce se v elektronické aukci vyskytuje zejména, pokud obchodník má více zboží jednoho druhu a prodává více zájemcům.

Riziku, které s sebou nakupování a prodej na aukcích přináší, se snaží provozovatelé aukčních serverů předcházet různými opatřeními. Jedná se například o aktivaci účtů či hodnocení uživatelů, které si nakupující i prodejci udělují po každém uskutečněném obchodu. Při nedodržení pravidel stanovených aukčním serverem, mohou provozovatelé uživateli, který se provinil, zrušit účet.[55]

Nakupování i prodej na aukcích si ve světě i u nás získává stále více příznivců. Původní snaha něco koupit nebo prodat se tak u mnoha uživatelů může snadno změnit ve vášeň a určitý druh sportu. Mezi nejznámější aukční servery patří eBay, Alegro, u nás je to především Aukro.cz, Odklepnuto.cz, iKup.cz atd.

E-tržiště

Elektronická tržiště jsou jednou ze součástí moderního obchodu v prostředí Internetu. Spadají do kategorie obchodování B2B, neboli obchodování firmy s firmou. Elektronická tržiště by se dala definovat jako virtuální místo, kde se střetává poptávka mnoha odběratelů s nabídkou mnoha dodavatelů. Dochází tu stejně jako na tržištích klasických k nejrůznějším jednáním mezi dodavateli a odběrateli, která potom vedou k uzavírání konkrétních obchodů.

---

[54] BERÁNEK, L. *Modelování důvěry a reputace se zaměřením na C2C systémy*. České Budějovice: Kopp, 2009. 182 s. ISBN 978-80-7232-387-6.

[55] KOČIČKA, P. Jak se nenechat napálit v internetových aukcích. *Technet.cz* [online]. 2011 [Cit. 2011-09-08]. Dostupný z: <http://technet.idnes.cz/jak-se-nenechat-napalit-v-internetovych-aukcich-f5a-/sw_internet.asp?c=A080114_210515_sw_internet_vse>.

Jinou zajímavou možností v této oblasti jsou internetová tržiště, která neslouží samotnému uzavření obchodu, ale spíše k rychlému zprostředkování nabídek.[56]

Přínos elektronických tržišť spočívá především v úsporách, které přináší optimalizovaný a automatizovaný obchodní proces. Pro odběratele je přínosem nabídka několika konkurenčních dodavatelů na jednom místě a rychlý přístup k informacím o zboží. Další výhodou je pohodlný a vcelku jednoduchý způsob objednání zboží s minimálními náklady. Pro dodavatele znamenají tržiště možnost, jak získat řadu nových zákazníků, které mohou tímto způsobem oslovit.

4.3 PŘEDSTAVENÍ RIZIK PRO INTERNETOVÉ AUKCE

Z pohledu kupujících:[57]

1) Prodávající odmítá odeslat zboží.
2) Popis předmětu z aukce není přesný.
3) Prodejce nabádá využít mimoburzovního systému, než jím je oficiálně povolen aukčním serverem.
4) Předmět aukce je jiný než jsme žádali.
5) Aukční položka je padělek.
6) Prodávající pobídne své známé, či využije fiktivního účtu pro zvýšení aktuální ceny.

Z pohledu prodávajícího:[58]

1) Kupující nezaplatil za zboží.
2) Kupující neoprávněně nahlásil vadu, která nevznikla.
3) Kupující záměrně nahlásil, že položka z aukce nedošla.

---

[56] E-tržiště. *B2B Centrum* [online]. c2011 [Cit. 2011-09-08]. Dostupné z: <http://www.b2bcentrum.cz/cs/e_marketplace>.

[57] ŠEBESTA, M. Risks and problems of contemporary electronic C2C auction systems. *Systémová integrace*[online]. 2009, č. 1, [cit. 2011-09-09]. Dostupný z WWW: <http://www.cssi.cz/cssi/risks-and-problems-of-contemporary-electronic-c2c-auction-systems>. ISSN 1210-9479.

[58] ŠEBESTA, M. Risks and problems of contemporary electronic C2C auction systems. *Systémová integrace*[online]. 2009, č. 1, [cit. 2011-09-09]. Dostupný z WWW: <http://www.cssi.cz/cssi/risks-and-problems-of-contemporary-electronic-c2c-auction-systems>. ISSN 1210-9479.

Rizika, které platí jak pro kupujícího tak prodávajícího:[59]

1) Kupující se rozhodne, že podvede prodávajícího tím, že si zřídí dvě identity. Jednou identitou nabídne za položku nízkou cenu a na druhé to převýší nereálně vysokou cenou. Kupující pak ve druhém případě nebude reagovat na výzvy a tím automaticky vyhrává druhá nejvyšší cena, kterou získá ta první identita. Riziko pro jiného kupujícího je to, že nebude schopen přebýt tuto vysokou cenu.
2) Modifikací výše zmíněné praktiky jsou kupující se třemi identity. Zde je maskovací manévr ještě sofistikovanější. S první identitou nabídne nízkou cenu, s druhou nabídne vysokou cenu a ve třetím ještě větší. Následně odvolá třetí a druhou nabídku, a získává tak předmět za nízkou cenu.
3) Nákup či platba se neuskuteční. Musí se stáhnout z oběhu.

[59] ŠEBESTA, M. Risks and problems of contemporary electronic C2C auction systems. *Systémová integrace*[online]. 2009, č. 1, [cit. 2011-09-09]. Dostupný z WWW: <http://www.cssi.cz/cssi/risks-and-problems-of-contemporary-electronic-c2c-auction-systems>. ISSN 1210-9479.Tamtéž.

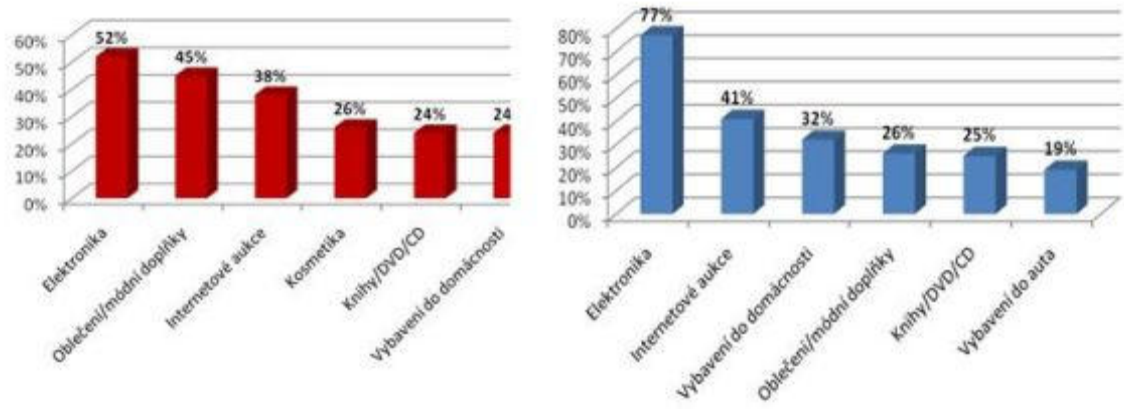
5. VÝZKUM

5.1 SOUČASNOST OBCHODOVÁNÍ NA INTERNETU

Podle průzkumu MasterIndex považuje internetové nákupy více jak polovina Čechů (53 %) za bezpečné. Nejčastěji si to myslí právě ti, kteří nakupují na internetu frekventovaně (81 %). Ve srovnání se Slováky je přístup k bezpečnosti téměř srovnatelný (56 %).[60]

Nejčastěji se v České republice na internetu nakupuje elektronika (65 %). Dále se Češi rádi účastní internetových aukcí (40 %) nebo si pořizují oblečení (36 %). České ženy na internetu nakupují nejčastěji elektroniku (52 %) či oblečení (45 %). Muži kromě elektroniky (77 %) a internetových aukcí (41 %) upřednostňují nákup vybavení do domácnosti (32%).[61]

Graf 2 Nejčastější nákupy žen a mužů na internetu



Zdroj: MasterIndex 2011, Česká republika, červen 2011, n = 902

5.2 AUKRO

Je největší obchodní platformou na českém internetu a lídrem trhu v elektronickém obchodování. Aukční server Aukro.cz byl založen v srpnu 2003 a od svých počátků je součástí polské skupiny Allegro, jedné z nejvýznamnější internetových společností na světě. V roce

[60] BUBÁK, Z. Češi se nákupů na internetu nebojí. 4.10.2011[online]. [Cit. 2011-09-10]. Dostupný z: http://www.finparada.cz/clanek.aspx

[61] Společnost MasterCard provádí spotřebitelský průzkum MasterIndex. Výzkum byl realizován jako Usage & Attitude studie klientů bank v České republice. Cílová skupina česká populace ve věku 18-69 let využívající služeb bank. Dotazování proběhlo ve všech regionech České republiky od 6. do 20. června 2011 a celkem bylo provedeno 965 kompletních rozhovorů.

2011 se stalo členem skupiny Allegro Group Česká republika a Slovensko, která vznikla jako holding polské skupiny Allegro. Kromě Aukra provozuje téměř dvacet dalších internetových platforem, mezi které patří například Heureka.cz, AukroCity.cz nebo otomoto.cz. Aukro má téměř sto zaměstnanců.[62]

Počet registrovaných uživatelů Aukro.cz, neustále roste. V prosinci 2010 jejich počet dosáhl 2 milionů. Pro srovnání v roce 2008 bylo přes milión registrovaných uživatelů.

Historie

2010

- Spuštěn projekt hromadných nákupů Úlovek týdne.
- Spuštěn charitativní program Aukro Přes překážky (sociálně odpovědná firma).
- Spuštěny nové kategorie Potraviny, Erotika, Šperky a hodinky.
- Nová sekce Moda.aukro, Deti.aukro a Cestuj.aukro.
- Aukro získalo ocenění Křišťálová lupa v kategorii Internetové obchodování.
- Povoleno obchodování uživatelům bez aktivace.
- Spuštěny Junior účty, které umožňují legálně obchodovat nezletilým starších 15 let.
- Nový platební systém PayU.
- Nová služba Přepravní centrum, spolupráce s DPD a Top Trans.
- Nový nástroj na správu aukcí – Aloader.
- Wikireality.cz - nový člen rodiny služeb.

2009

- Vznik podnikatelských účtů.
- Spuštěna nová služba Aukro Shopy.
- Propojení s realitním tržištěm bezrealitky.cz.
- Aukro vstupuje do Hotel.cz.
- Ocenění Obchodník roku, první příčka mezi internetovými obchody.

2008

- Spuštěn Program ochrany Kupujících.
- Odvysílána první televizní reklama.
- 1 000 000 registrovaných uživatelů.
- Křišťálová lupa v kategorii Eshop.
- Spuštění motoristické inzerce otomoto.cz.

[62] http://aukro.cz/country_pages/56/0/marketing/about.php [online]. 2011 [Cit. 2011-09-08].

Během posledních let se jeho prostřednictvím obchoduje stále více s novým zbožím za pevné ceny. V současné době je na Aukro.cz registrováno 2,3 milionu uživatelů a patří mu čtvrtá příčka mezi nejnavštěvovanějšími stránkami českého internetu. Aukro si za osm let působení na českém internetu vydobylo výsadní pozici. Z marketingového výzkumu vyplývá, že Aukro je nejznámější ze všech českých obchodních portálů. Zná ho 76% dotázaných.[63]

Během prvního půl roku (2011) se na Aukru prodalo 6,3 milionů produktů. Oproti minulému roku (2010) se tak prodalo o 200 tisíc produktů více. Největší zájem byl o vybavení domu a zahrady a v druhé řadě o oblečení.[64] Množství prodaného zboží se tak meziročně zvýšilo o 26 %. Podle odhadů se tržby e-shopů v loňském roce pohybovaly kolem 33 miliard Kč. Pro srovnání například v lednu 2007 se prodalo 150 tisíc položek, v prosinci to byl již dvojnásobek. Celkově se v roce 2007 na serveru Aukro prodalo více než 2,8 milionu položek za částku asi 1,2 miliardy korun.[65]

Od roku 2009 není většina zboží nabízena formou aukce, jak bylo zvykem, ale až 72 % předmětů je prodáváno za pevnou cenu. Aukce převažují v kategoriích typů sběratelství či starožitnosti a umění, kdy může cena dosáhnout vyšších částek. Denně jsou na Aukro.cz vystaveny přibližně 4 miliony aktivních položek.

Profesionální prodejci nabízejí na Aukro.cz nové zboží se zákonnou zárukou, kteří prodejem na Aukro.cz mnohdy nahrazují své vlastní e-shopy.

5.3 KASA.CZ

Jako jeden z předních představitelů e-shopů v ČR nabízí svým zákazníkům kompletní sortiment audio-video, bílého zboží, spotřební elektroniky, foto a výpočetní techniky, sportovního zboží, zahradní a auto-moto techniky, kosmetiky, dětského vybavení a hraček, nábytku i doplňků pro volný čas a zábavu. Jedná se o sortiment zahrnující více než 1000 světových značek.

Historie

2011 - sjednocení obchodů Holdingu KASA.cz a Obchodní-dům.cz pod Internet Retail a.s.

2010 - obrat Holdingu KASA.cz a Obchodní-dům.cz dosáhl 2,05 mld. Korun

---

[63] http://aukro.cz/country_pages/56/0/marketing/about.php [online]. 2011 [Cit. 2011-09-08].
[64] http://aukro.cz/country_pages/56/0/marketing/about.php [online]. 2011 [Cit. 2011-09-08].
[65] KOČIČKA, P. Jak se nenechat napálit v internetových aukcích. *Technet.cz* [online]. 2011 [Cit. 2011-09-08]. Dostupný z: <http://technet.idnes.cz/jak-se-nenechat-napalit-v-internetovych-aukcich-f5a-/sw_internet.asp?c=A080114_210515_sw_internet_vse>.

2009 - spuštění inovativního zákaznického systému

- spojení s internetovým obchodem Obchodní-dům.cz a založení pobočky v Maďarsku

2008 - 99. místo mezi nejrychleji rostoucími firmami v Evropě - Deloitte Technology Fast 500

- 2. místo mezi nejrychleji rostoucími firmami v ČR- Deloitte Technology Fast 50
- obrat Holdingu KASA.cz a Obchodní-dům.cz dosáhl 2,2 mld. korun

2007 - ocenění za inovativní přístup ve výběru příspěvků pro sbírku Pomozte dětem

- obrat skupiny obchodů KASA.cz činil v roce 2007 1,28 mld. korun

2006 - KASA.cz - jeden ze členů Záchranného kruhu, Klubu přátel sbírky Pomozte dětem

2005 - založení poboček v Německu, Polsku

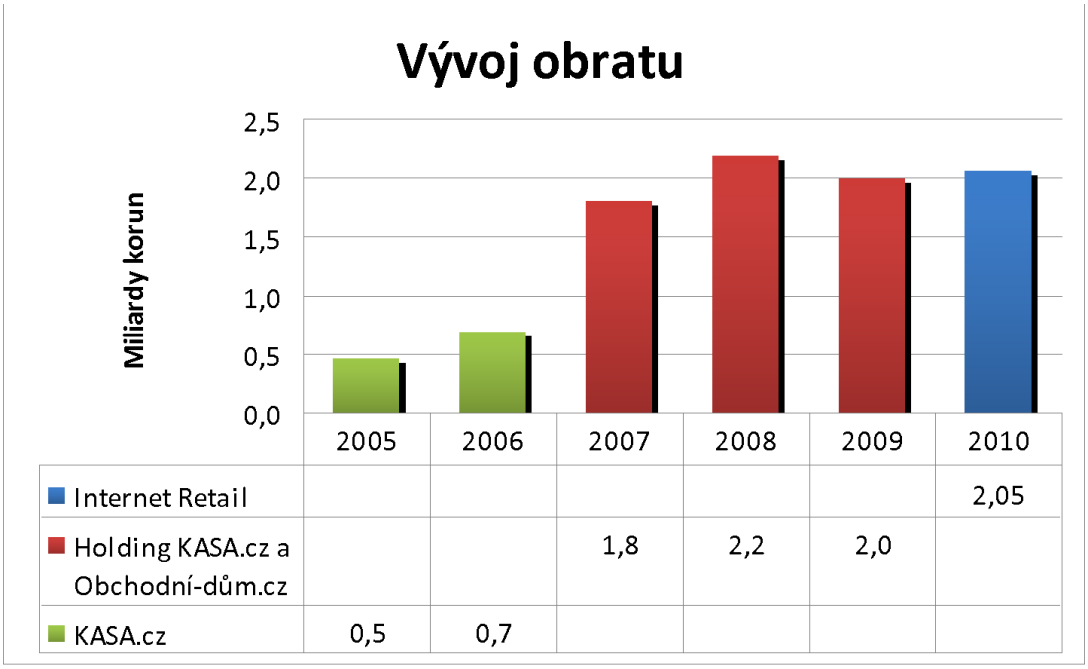
2004 - spuštění logistického a skladového centra v Kutné Hoře

2003 - otevření první zahraniční pobočky na Slovensku

2000 - otevření prvního kamenného obchodu v Praze

1999 - první prodej realizovaný přes internet[66]

Graf 3 Vývoj obratu internetového obchodu Kasa.cz



Zdroj: Kasa.cz

[66] O firmě. Kasa.cz [online]. 2011 [Cit. 2011-09-08]Dostupný z: http://www.kasa.cz/o-firme/?session

5.4 ALZA.CZ

Zabývá se prodejem výpočetní techniky a elektroniky od roku 1994 a dlouhodobě je lídrem českého internetového trhu. Jedničkou na trhu je Alza.cz zejména díky bezkonkurenční skladové dostupnosti zboží, široké nabídce produktů a nadstandardním službám, které doprovázejí samotný prodej i poprodejní služby.

Historie

2010 - ocenění Shop Roku.

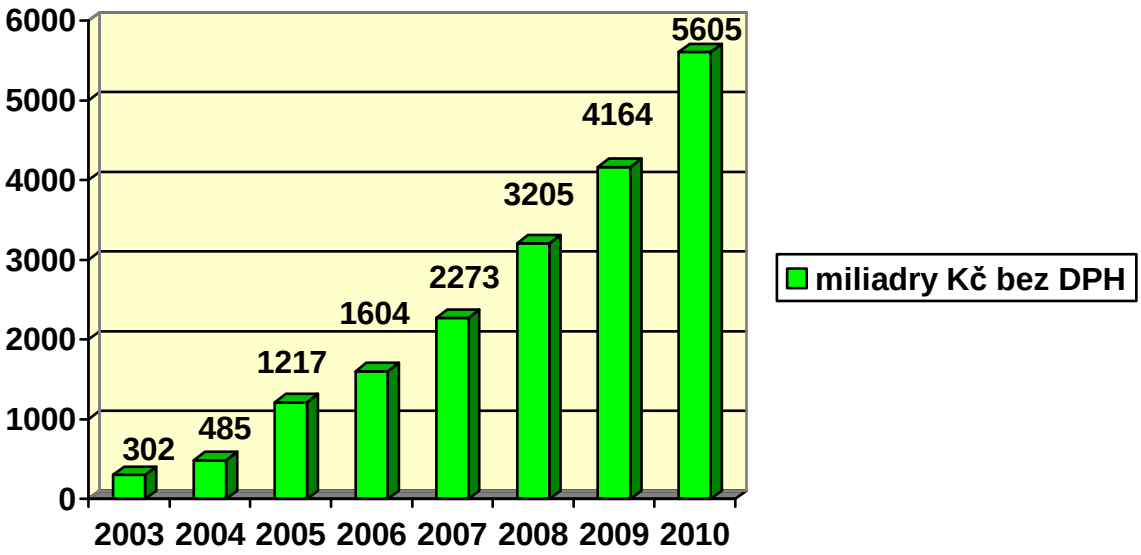
2009 - HP Partner roku za 1. místo v kategorii Dosažený obrat v prodeji notebooků.

2008 - GE Money Multiservis Obchodník roku.

Společnost Alza.cz a.s. dosáhla v uplynulém roce (2010) celkového obratu 5,608 miliardy Kč. Meziročně tak obrat společnosti vzrostl o 34%. Alza.cz a.s. má nulové zadlužení a její finanční kondice je zárukou jistoty nejen pro zákazníky a obchodní partnery, ale i pro vlastní zaměstnance.

Internetový obchod Alza.cz nabízí v současné době více než 35 000 různých produktů od 1000 světových značek v 3 600 kategoriích. V roce 2010 bylo vyřízeno 1 859 156 objednávek, což je oproti roku 2009, kdy to bylo 1 141 280 objednávek, nárůst o 62%.[67]

Graf 4 Roční obrat Alza.cz



Zdroj: Alza.cz 2011

[67] O společnosti Alza. [online]. 2011 [Cit. 2011-09-08]Dostupný z:. http://www.alza.cz/article

6. NÁVOD POSTUPŮ A ČINNOSTÍ PRO OBCHODOVÁNÍ NA INTERNETU

6.1 BEZPEČNÉ OBCHODOVÁNÍ NA INTERNETU

Tuto kapitolu považuji za výstup mé bakalářské práce. V kapitole uvádím typy a rady jak předejít nebezpečnému obchodování na Internetu. Bezpečný obchod nebo bezpečné internetové bankovnictví provozovat lze, ovšem investice na vybudování takového bezpečného prostředí jsou vysoké a náročné. Dle mého názoru nemusí kupující při dodržování určitých (následujících) pravidel vynakládat žádné finanční investice pro bezpečné obchodování na internetu.

Při skutečně plnohodnotném internetovém obchodování vzniká několik problémů:

- ověření totožnosti obou stran,
- skutečné provedení úhrady,
- doručení úhrady skutečnému prodávajícímu,
- dodání zboží (služby) skutečnému kupujícímu.

Jak poznat podvodný inzerát?

- Text bývá psaný špatnou češtinou a může vycházet i z nějakého internetového překladače.
- Cena je vždy neúměrně nízká typu a stavu zboží.
- Autor odůvodňuje nízkou cenu nutným stěhováním, často do jiného státu.
- Není uveden telefonický kontakt.
- Odpověď na inzerát je preferována v cizím jazyce.
- Pokud na inzerát odpovíte, pak je požadováno zaslání zálohy.

Ověření totožnosti stran

Prvním předpokladem úspěšného a bezpečného obchodování je ověření totožnosti obou stran, tj. prodávajícího a kupujícího. Na druhou stranu totožnost nemusí být absolutní; při nákupu v obchodě se rovněž nepředstavujeme, víme ale, ve kterém obchodě jsme nakupovali, máme o nákupu doklad apod. Prodávajícího nezajímá, kdo jsme, ale obsah naší peněženky. Jde tedy o autentizaci obou stran, neboli aby prodávající věděl (s dostatečnou jistotou), kdo je

kupujícím, resp. zda disponuje prostředky k úhradě, a naopak kupující by rád věděl, kdo mu zboží opravdu prodává a zda zboží skutečně existuje.[68]

Prokázání totožnosti prodávajícího se na Internetu provádí obvykle zvolením jeho webové stránky, kde se objeví určitá nabídka, a je na kupujícím, zda ji bude dále akceptovat. Zde vzniká první - spíše bezpečnostní nežli právní - problém. Kdo však zaručí, že se jedná skutečně o stránku velkoobchodu a nikoliv o hackera, který přesměroval volání pod výše uvedeným jménem na stránku svoji, se svým číslem účtu?[69]

V případě nákupu, kdy uživatel posílá někam své peníze na základě informací získaných z veřejně přístupných nástěnek na nějakém serveru, musíme konstatovat, že nemá dostatečnou jistotu, že odesílá peníze skutečně tomu, kdo byl jako prodávající na stránkách uveden.

Prodávající nepotřebuje příliš pátrat po skutečné totožnosti kupujícího, pokud si v klidu počká, až k němu dorazí platba, a pak zboží pošle na adresu uvedenou kupujícím.

V případě bankovního styku přes Internet je vzájemný vztah složitější. Banka potřebuje vědět, že klient je skutečně klient, a klient se z důvodu bezpečnosti neobejde bez potvrzení, že banka je opravdu banka. Jen tak je totiž zaručeno, že někdo jiný, vydávající se za banku, si zjistí přístupová pravidla simulací banky a potom se sám nepřihlásí a simuluje klienta.

Nákupní rádci

Podle výzkumů společnosti Forrester je přes 75% prodeje přes internet ovlivněno právě radami z nákupních rádců. Tento fakt přispívá k tomu, že se nákupní rádci stávají nepřehlédnutelným trendem v oblasti elektronického nakupování. Nákupní rádci na jednom místě poskytují databázi produktů, která se skládá z popisů zboží a uživatelských recenzí. Na základě těchto informací dávají uživateli možnost srovnat si zboží, které ho zajímá podle daných vlastností a zároveň mu poradit, kde ho může nakoupit nejvýhodněji. Na rozdíl od internetových stránek, zabývajících se srovnáváním cen, nabízejí nákupní rádci širší nabídku služeb.[70]

Příkladem nákupního rádce je **Heureka.cz,** která je v současnosti jedním z nejznámějších českých internetových nákupních rádců. Cílem tohoto internetového rádce je provést návštěvníka celým procesem nakupování. Poskytuje rady, pomáhá s výběrem produktu

---

[68] SMEJKAL, V. *Internet @ .§§§*. Vyd. 1. Praha: Grada, 1999. s. 168, ISBN 80-7169-765-6.
[69] SMEJKAL, V. *Internet @ .§§§*. Vyd. 1. Praha: Grada, 1999. S. 168, ISBN 80-7169-765-6.
[70] HODBOĎ, T. Internetové obchody tak jak je známe, zahynou. *Lupa: server o českém internetu* [online]. 2008 [Cit. 2011-09-08]. Dostupný z: <http://www.lupa.cz/clanky/internetove-obchody-tak-jak-je-zname-zahynou/>.

a snaží se doporučit uživateli ten nejvhodnější obchod k nákupu vybraného druhu zboží. Heureka se liší od vyhledávačů zboží a katalogů internetových obchodů poskytováním recenzí a hodnocením zboží i jednotlivých internetových obchodů. Uživatelé Heureky se tak mohou seznámit se zkušenostmi ostatních uživatelů s jednotlivými produkty. Heureka by se dala díky své komunitě uživatelů, kteří mezi sebou sdílejí recenze a názory na produkty, zařadit do kategorie spadající pod pojem komunitní nakupování – tedy social shopping.

Kromě recenzí zboží se na Heurece vyskytuje i hodnocení jednotlivých obchodů. Nákupní rádce Heureka není s žádným internetovým obchodem provázaný, a tak by tím neměla být nabídka obchodů ovlivněna. Celkem je v databázi Heureky přes 2500 obchodů.[71]

Podobné funkce jako Heureka mají i další vyhledávače zboží, k těm zajímavějším patří například seznamzbozi.cz, kde mohou uživatelé kromě recenzí a hodnocení vkládat také uživatelská videa daného zboží ze serveru YouTube. Tento server propojuje jednotlivé výrobky s aukcemi probíhajícími na serveru Aukro.

Hodnocení a recenze

Možnost hodnocení zboží pomáhá budovat vztah se zákazníky a vytvářet tak komunitu. Zákazníci oceňují, když se u produktu, který chtějí zakoupit, dozví názory a hodnocení ostatních uživatelů. Nejpoužívanější formou hodnocení zboží u e-shopů bývá bodování na stupnici, většinou na škále od 1 do 5, nejčastěji formou hvězdiček či přidáváním komentářů uživatelů ke zboží. Rozdíl v možnostech hodnocení může být například v tom, kdo má možnost hodnotit. Některé obchody umožňují hodnotit zboží jen zákazníkům, kteří si dané zboží u nich zakoupili (např. Mall.cz), jiné pouze zaregistrovaným uživatelům (např. Electroworld.cz). Tímto způsobem si obchody zajišťují objektivnost hodnocení a zabraňují tak zneužívání např. konkurencí.

Pro obchody, které chtějí zveřejňovat uživatelské recenze, je důležité motivovat uživatele k jejich psaní. Obzvláště důležitá je motivace uživatelů u internetových rádců, pro které je množství hodnocení a recenzí uživatelů klíčové.

[71] KLEGA, V. Povedený nákupní rádce. *Chip.cz* [online]. 2011 [Cit. 2011-09-08]. Dostupný z: <http://www.chip.cz/cs/novinky-ze-sveta-it/povedeny-nakupni-radce.html>.

6.2 OBECNÁ METODIKA NÁKUPU NA INTERNETU

1. Věnujte velkou pozornost výběru správného obchodu, ne vždy znamená nejnižší cena nebo líbivý vzhled nejlepší volbu. Může se jednat o zboží z tzv. šedého dovozu (není určeno pro český trh), o použité zboží či zboží s vadou. Proto si také důkladně pročtěte obchodní podmínky, jestli v nich není tato skutečnost poznamenána, prodejce by však měl spotřebitele s touto podstatnou informací seznámit přímo u popisu parametrů výrobku.
2. Pokud nemáte s vybraným obchodem zkušenosti, zjistěte si na internetu nebo od známých pozitivní reference. Zajímejte se o to, zda obchod pomáhá zákazníkům při výběru zboží například umožněním komentářů či hodnocení u zboží.
3. Hledejte na stránkách obchodu logo certifikace APEK či SAOP, nákup je pak bezpečnější. Můžete využít například katalogu certifikovaných obchodů www.certifikovany-obchod.cz nebo se přímo obrátit na SOS-Sdružení obrany spotřebitelů. Obchody, které k certifikaci přistoupily, dávají najevo, že znají práva spotřebitelů a tato práva dodržují. Certifikace znamená pro spotřebitele větší jistotu při nakupování a dovolání se práv.
4. Zjistěte, zdali obchodník na www stránkách poskytuje své identifikační údaje a uvádí nákupní řád, obchodní a reklamační podmínky, ze zákona je tak povinen. Nepodceňujte obsah nákupního řádu či obchodních a reklamačních podmínek, čtěte je! Občanský zákoník uvádí údaje, které musí obchodník při uzavírání smlouvy na dálku spotřebiteli poskytnout. Jsou mezi nimi zejména obchodní firma či jméno a příjmení fyzické osoby, identifikační číslo prodejce, sídlo právnické osoby a bydliště fyzické osoby a dále údaj o zápise v obchodním rejstříku či jiné obdobné evidenci. Přečtením obchodních a reklamačních podmínek si můžete ušetřit čas při řešení případné reklamace. Zjistíte z nich způsob platby, dodání zboží, jak uplatnit reklamaci a vaše nároky při výskytu vady. [72]
5. Z kontaktních informací si ověřte, zda má obchodník dostatečně kvalitní zázemí pro vyřízení vaší objednávky. Spolehlivé internetové obchody uvádí v kontaktech vždy i provozovatele.
6. Buďte pečliví při vyplňování objednávky a při zadávání bezhotovostní platby (převodem, SMS, on-line). Uschovejte si potvrzení o objednávce, předejdete komplikacím při tvrzení obchodníka, že jste si zboží objednali za jinou (vyšší cenu). Pokud podáte objednávku prostředkem komunikace na dálku (kromě objednávky elektronickou poštou) je obchodník

[72] Jak bezpečně nakupovat na internetu. 2011 [Cit. 2011-09-08]. Dostupný z: <http: http://www.bezpecnynakup.cz/

povinen neprodleně potvrdit její obdržení. Kartou plaťte pouze u prověřených obchodníků, kteří na trhu působí již dlouhou dobu. V jiných případech raději volte dobírku. Vždy si uchovávejte doklady o provedené transakci.

7. Při převzetí zásilky od dopravce zkontrolujte neporušenost obalu zásilky. Porušenou zásilku nepřebírejte, sepište protokol s dopravcem a kontaktujte obchodníka. Cena za zásilku musí odpovídat té, kterou vám obchodník potvrdil. Doporučuje se, zásilku za vyšší cenu, než za kterou jste si zboží objednali, nepřebírat a neprodleně kontaktovat obchodníka, aby sjednal nápravu.
8. Při nákupu přes internet máte ze zákona právo u většiny zboží od smlouvy odstoupit do 14 dnů od jeho převzetí. Toto právo nemůže spotřebitel využít např. u zboží upraveného podle jeho přání, u zboží, které podléhá rychlé zkáze, opotřebení či zastarání, na dodávku audio, video nahrávek a počítačových programů, jestliže spotřebitel porušil jejich originální obal, na dodávku novin, periodik a časopisů. Jestliže se rozhodnete odstoupit od smlouvy, učiňte tak v zájmu právní jistoty písemně, na adresu prodejce. Nemusíte udávat důvod odstoupení. Odstoupení musí být doručeno obchodníkovi ve lhůtě. Je povinností obchodníka Vás o tomto právu informovat. Pokud tak neučiní, prodlužuje se lhůta na tři měsíce od převzetí plnění.
9. Reklamaci je povinen obchodník vyřídit nejpozději do 30 dnů. Pokud je to možné, vyřizujte reklamaci osobně přímo na prodejně obchodu. Celý proces tím ještě urychlíte. Zákon o ochraně spotřebitele § 19 odst. 3 stanoví, že prodejce je povinen o reklamaci rozhodnout ihned, ve složitých případech do tří pracovních dnů. Reklamace, včetně odstranění vady (či odůvodněné zamítnutí) musí být vyřízena do 30 dnů od jejího uplatnění. Pokud tak prodejce neučiní, má spotřebitel stejná práva, jako by se jednalo o vadu, kterou nelze odstranit. Při neodstranitelné závadě má spotřebitel právo na odstoupení od smlouvy, výměnu výrobku či přiměřenou slevu z kupní ceny. Volba je na spotřebiteli.[73]
10. Pokud nakupujete opakovaně, snažte se využívat služeb obchodů, se kterými jste byli v minulosti spokojeni. Využívejte možnosti nákupu v kamenné prodejně, pokud ji daný internetový obchod vlastní.

[73]Jak bezpečně nakupovat na internetu. 2011 [Cit. 2011-09-08]. Dostupný z: <http: http://www.bezpecnynakup.cz/

6.3 PROGRAM OCHRANY KUPUJÍCÍCH (POK)

Aukční portál Aukro.cz poskytuje unikátní službu, a to Program ochrany Kupujících. Ten umožňuje kupujícímu získat finanční náhradu do výše 20 000 Kč v případě, že:

- zaplatil za vydraženou věc, ale neobdržel ji;
- obdržel věc, která se podstatně liší od popisu aukce.

Jednou z nejdůležitějších podmínek poskytnutí finančního plnění z Programu ochrany Kupujících je **oznámení** pro podezření ze spáchání přestupku či trestného činu prodávajícím na **Policii ČR** a odeslání kopie stejnopisu (ve kterém bude uvedeno číslo jednací a všechny skutkové okolnosti v této věci) tohoto oznámení spolu s ostatními požadovanými dokumenty na adresu společnosti Aukro.cz.[74]

Uchovávané informace o aukcích a uživatelích

- veškerá data související s uživatelským účtem včetně všech provedených změn;
- přihlašovací historie - IP adresy, kompletní historie;
- archiv veškerých ukončených aukcí (aukce starší 2 měsíců jsou zálohovány bez fotografií);
- historie aktivit uživatele (příhozy na aukce);
- údaje o obchodních partnerech (kupující, prodejci);
- vazby mezi jednotlivými uživatelskými účty (shodné bankovní účty, IP adresy, kontaktní údaje).[75]

Problémy oznamované na Policii ČR uživateli Aukro.cz

- podvod peníze byly odeslány prodejci předem, zboží však nedorazilo;
- zneužití uživatelského účtu - prolomení uživatelského hesla;
- zneužití osobních údajů pro páchání trestné činnosti - účet je zaregistrován např. na osobu blízkou;
- zboží pocházející z trestné činnosti nabízené na Aukro.cz.[76]

[74] http://aukro.cz/country_pages/56/0/marketing/about.php [online]. 2011 [Cit. 2011-09-08].
[75] http://aukro.cz/country_pages/56/0/marketing/about.php [online]. 2011 [Cit. 2011-09-08].
[76] http://aukro.cz/country_pages/56/0/marketing/about.php [online]. 2011 [Cit. 2011-09-08].

Informace od poškozených při přijetí oznámení na PČR

- uživatelské jméno prodávajícího a kupujícího;
- čísla aukcí;
- číslo bankovního účtu, kam byla zaslána platba za zboží;
- historie korespondence mezi uživateli včetně emailových adres;
- telefonní čísla, další údaje o možném pachateli;
- další okolnosti případu.

Obecné náležitosti dokumentu zaslaného společnosti Aukro s.r.o.

- zákonná ustanovení, na základě kterých jsou požadovány informace (§ 66 odst. 1 zákona č. 273/2008 Sb., § 8 odst. 1 tr. řádu);
- přesné údaje o policejním oddělení, včetně adresy, PSČ;
- jméno, příjmení a kontaktní telefon na zpracovatele nebo vyšetřovatele; číslo jednací;
- krátké vysvětlení problému;
- číslo aukce, uživatelské jméno prodejce a kupujícího;
- číslo bankovního účtu, na které byly zaslány finanční prostředky v případě podvodu; další zjištěné nebo oznámené informace kupujícím.[77]

Boj s phishingem

Tuto kapitolu zařazuji z důvodu počínajícího nárůstu výskytu phishingu v celé ČR. Dalším důvodem je, že při takovém útoku dochází k větším finančním ztrátám, než při nákupech prostřednictvím internetu, ztrátám většího obnosu peněz.

Existuje několik úrovní boje s phishingem: na uživatelské úrovni zejména osvěta a dodržování bezpečnostních pravidel, na softwarové úrovni je možno používat specializované nástroje, které phishingové útoky umožňují detekovat a upozorňovat na ně. Také existují organizace, které se bojem s phishingem zabývají cíleně a stránky využívané k těmto útokům odstraňují. Některé státy už dokonce vytvořily specializovanou legislativu zaměřenou na phishing. Ukázku podvodné webové stránky uvádím v příloze.

[77] http://aukro.cz/country_pages/56/0/marketing/about.php [online]. 2011 [Cit. 2011-09-08].

Jak se chránit před online útoky phishingu:

1. Chraňte své osobní údaje.
2. Na důvěryhodné weby přecházejte *zadáním webové adresy* přímo na panel Adresa.
3. Nikdy *neposkytujte své osobní údaje v e-mailu*, rychlé zprávě nebo automaticky otevíraném okně.
4. *Neklikejte na odkazy v e-mailech a rychlých zprávách* od neznámých osob nebo na jakýkoli podezřele vypadající odkaz. Protože mohou být i zprávy od přátel a rodiny falešné, ujistěte se u odesílatele, zda skutečně zprávu odeslal.
5. Používejte pouze *weby, poskytující prohlášení o ochraně osobních údajů* nebo informace o tom, jak nakládají s vašimi osobními údaji.
6. Pravidelně kontrolujte své finanční výpisy a historii kreditů a jakoukoli podezřelou činnost oznamte.

Filtr SmartScreen [78]

Filtr SmartScreen je funkce aplikace Internet Explorer, která pomáhá zjišťovat weby útoku phishing. Filtr SmartScreen může chránit proti instalaci škodlivého softwaru nebo malwaru. Filtr SmartScreen pomáhá chránit třemi způsoby:

1. Běží na pozadí, když procházíte web, analyzuje webové stránky a určuje, zda mají vlastnosti, které by mohly být podezřelé. Pokud zjistí podezřelé webové stránky, SmartScreen zobrazí zprávu nabízející možnost uvést váš názor. Rovněž doporučí, abyste postupovali opatrně.
2. Kontroluje navštěvované weby na základě právě aktuálního dynamického sestavu oznámených webů útoku phishing a škodlivého softwaru. Pokud nalezne shodnou položku, SmartScreen zobrazí červené upozornění, že je web zablokován, aby se zvýšila vaše bezpečnost.
3. Kontroluje soubory stažené z webu na základě stejného dynamického seznamu oznámených webů škodlivého softwaru. Pokud nalezne shodnou položku, SmartScreen zobrazí červené upozornění, že je položka ke stažení zablokována, aby se zvýšila vaše bezpečnost.

[78] Filtr SmartScreen. 2011 Microsoft Corporation 2011 [Cit. 2011-09-08].
Dostupný z:http://windows.microsoft.com/cs-CZ/internet-explorer/products/ie-9/features/smartscreen-filter

Co dělat, pokud jsem zadal své osobní nebo finanční informace na podvodný web

- Změňte hesla nebo kódy PIN ve všech svých online účtech.
- Do svých finančních výpisů zahrňte výstrahu proti podvodu. Pokud si nejste jistí, jak postupovat, poraďte se s bankovním nebo finančním poradcem.
- Obracejte se přímo na banku nebo online prodejce. Neklikejte na odkaz v podvodném e-mailu.
- Pokud znáte podvodné účty, na které jste přešli nebo které jste otevřeli, zavřete je.
- Podejte zprávu místní policii.

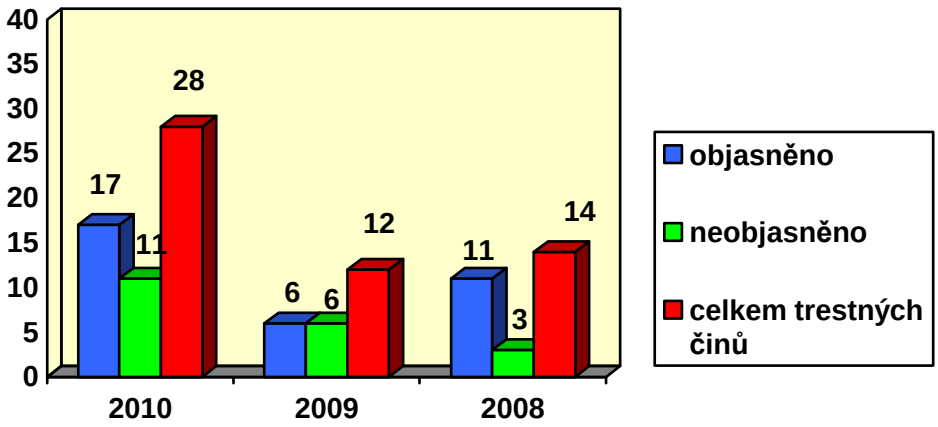
7. STATISTIKA PŘIJATÝCH OZNÁMENÍ TÝKAJÍCÍCH SE PODVODNÉHO JEDNÁNÍ NA AUKČNÍCH SERVERECH

Využití Evidenčně statistického systému kriminality policejního prezidenta ČR (ESSK) k přehledu informační kriminality se zaměřením na majetkovou trestnou činnost je v současné době problematické. Kategorie informační kriminality se zaměřením na majetkovou trestnou činnost se ve statistickém vykazování nevyskytuje. Neumožňuje to používaný číselník, který neobsahuje potřebné položky charakterizující tuto formu páchání uvedených trestných činů.

V České republice zatím nejvíce odhalených a potrestaných případů souvisí se samotným nabízením neoriginálních nosičů se softwarem, hudebními a filmovými nahrávkami nebo počítačovými hrami pomocí inzerátů umístěných někde na internetových inzertních stránkách, např. www.sbazar.cz, apod. Ač se oproti ostatním způsobům informační kriminality jedná o jednu z nejsnáze odhalitelných činností, která není nijak zvlášť výdělečná, stále se tento trend drží a počet pachatelů zřetelně neklesá. Tohoto trestného činu se bohužel dopouští i hodně nezletilých.

7.1 STATISTIKA PODVODNÉHO JEDNÁNÍ NA INTERNETOVÝCH AUKCÍCH

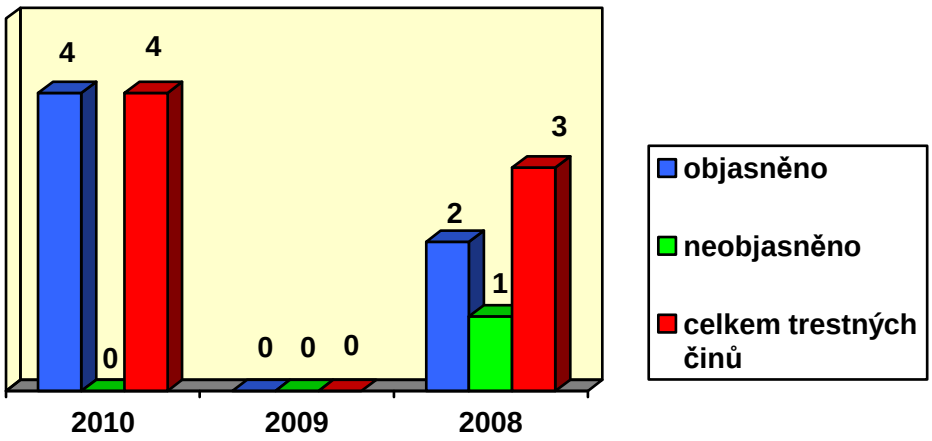
Graf 4 ÚO České Budějovice



Zdroj: Evidence trestního řízení (ETŘ), a Kriminalistický statistický údaj (KSU) Policie ČR

Dvojnásobný nárůst trestné činnosti v roce 2010, oproti roku 2008 s výrazným snížením objasněnosti.

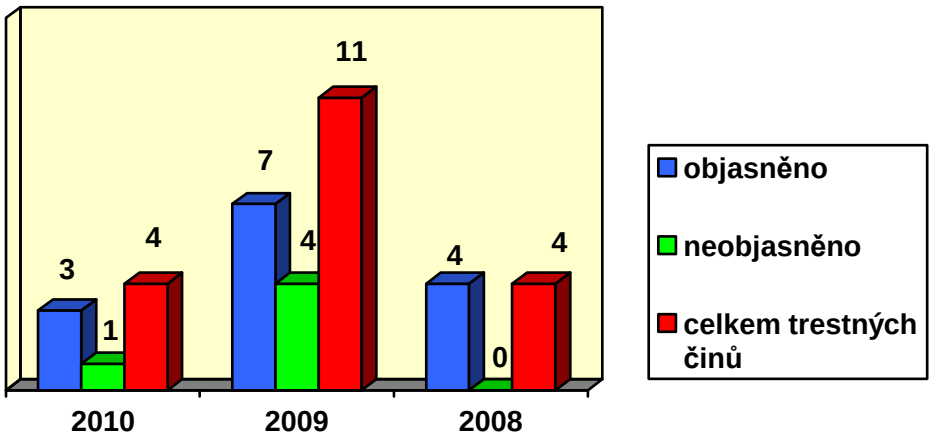
Graf 5 ÚO Prachatice



Zdroj: Evidence trestního řízení (ETŘ), a Kriminalistický statistický údaj (KSU) Policie ČR

Téměř stoprocentní objasněnost v letech 2008 a 2010.

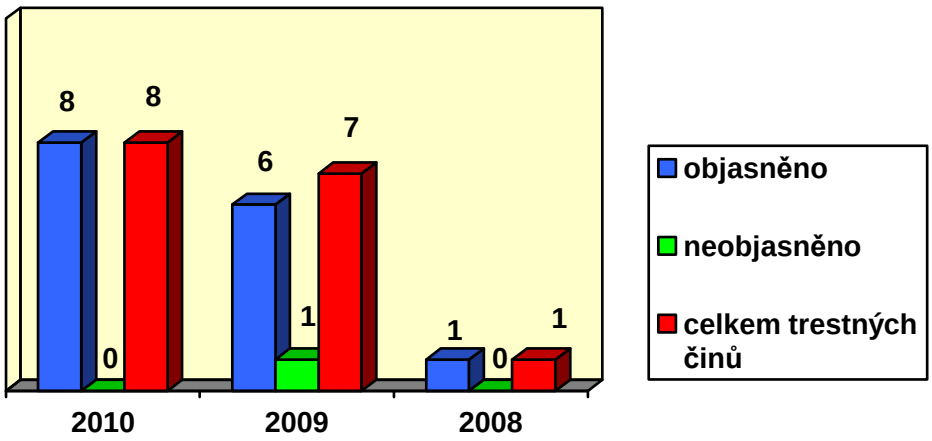
Graf 6 ÚO Tábor



Zdroj: Evidence trestního řízení (ETŘ), a Kriminalistický statistický údaj (KSU) Policie ČR

Rok 2009 vykazuje rapidní nárůst trestné činnosti. Její objasněnost v tomto roce dosahuje mírně nad polovinu. Roky 2008 a 2010 znamenají objasněnost téměř stoprocentní.

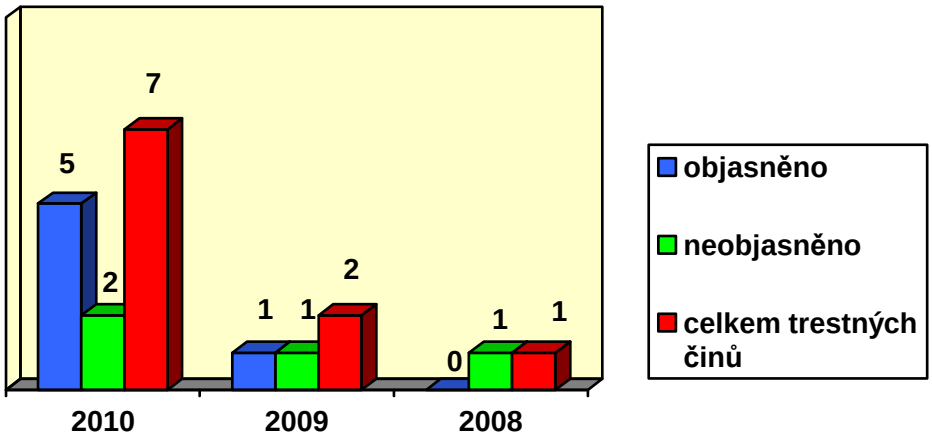
Graf 7 ÚO Jindřichův Hradec



Zdroj: Evidence trestního řízení (ETŘ), a Kriminalistický statistický údaj (KSU) Policie ČR

Ze šestnácti případů v letech 2008 – 2010 jich bylo objasněno 15. Vynikající stabilní objasněnost. Nejvíce trestných činů bylo opět spácháno na internetovém aukčním portálu Aukro.cz.

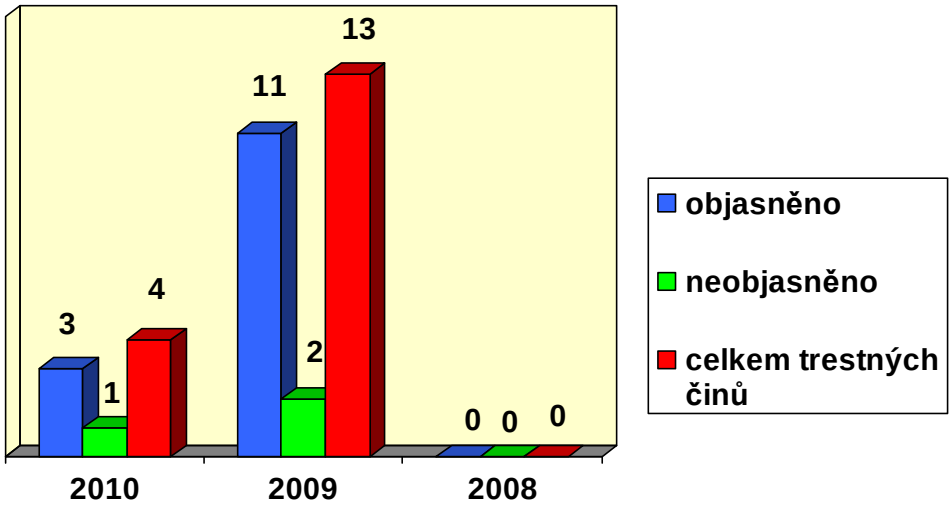
Graf 8 ÚO Český Krumlov



Zdroj: Evidence trestního řízení (ETŘ), a Kriminalistický statistický údaj (KSU) Policie ČR

Vysoký nárůst trestné činnosti v roce 2010 oproti předcházejícím dvěma rokům, s objasněností přes sedmdesát procent.

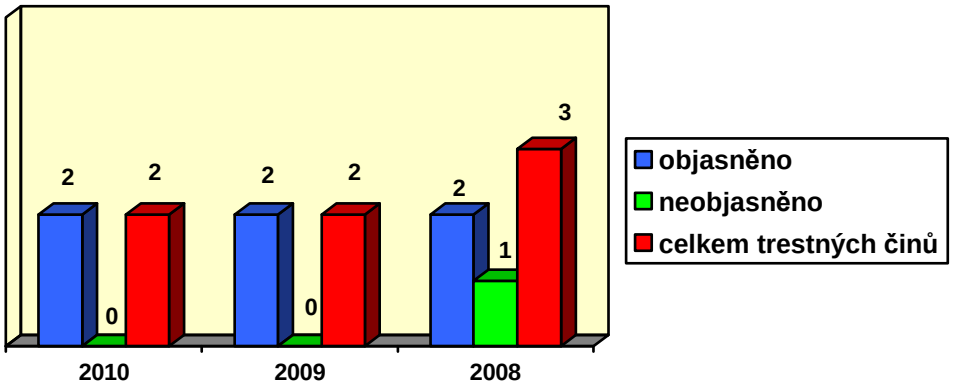
Graf 9 ÚO Strakonice



Zdroj: Evidence trestního řízení (ETŘ), a Kriminalistický statistický údaj (KSU) Policie ČR

Strakonice vykazují nejvyšší nárůst trestné činnosti v roce 2009, s vysokou objasněností. Následující rok počet trestné činnosti strmě klesá, objasněnost zůstává vysoká.

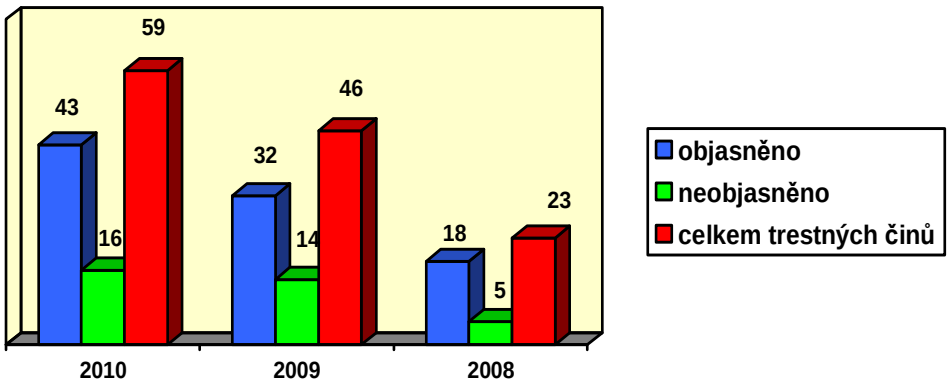
Graf 10 ÚO Písek



Zdroj: Evidence trestního řízení (ETŘ), a Kriminalistický statistický údaj (KSU) Policie ČR

Počet trestné činnosti nezaznamenává v letech 2008 – 2010 žádné výkyvy. Objasněnost je téměř stoprocentní. Nejvíce trestných činů bylo opět spácháno na internetovém aukčním portálu Aukro.cz.

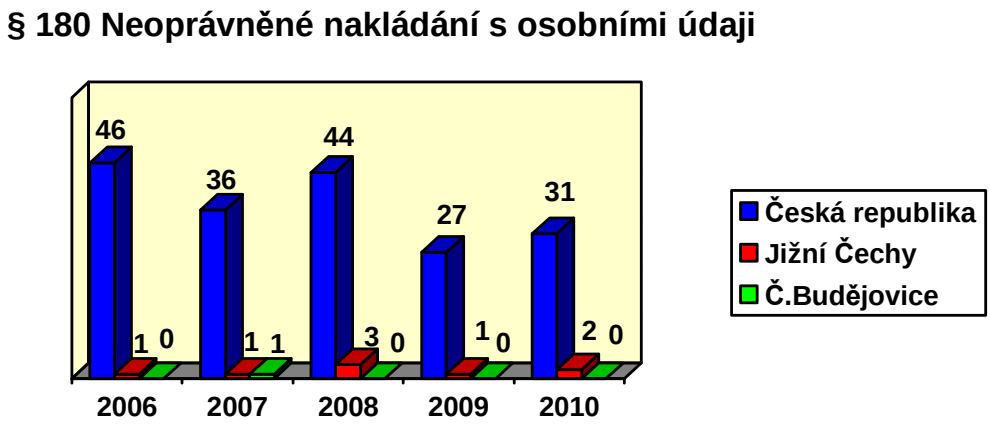
Graf 11 Jihočeský kraj



Zdroj: Evidence trestního řízení (ETŘ), a Kriminalistický statistický údaj (KSU) Policie ČR

Ze 128 spáchaných trestných činů v letech 2008 – 2010 objasněno 93. Nejvíce trestných činů bylo opět spácháno na internetovém aukčním portálu Aukro.cz, ale přibylo trestných činů i na ostatních aukčních portálech. (příloha 5)

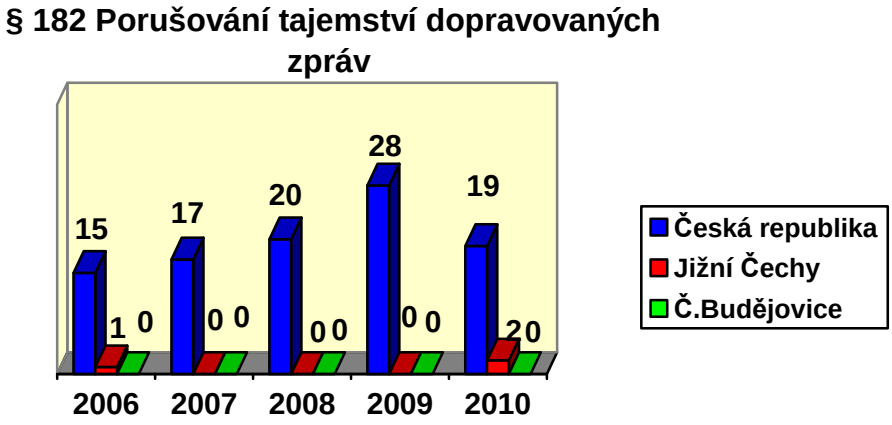
Graf 12 § 180 Neoprávněné nakládání s osobními údaji



Zdroj: Evidence trestního řízení (ETŘ), a Kriminalistický statistický údaj (KSU) Policie ČR

Na území celé České republiky bylo do roku 2010 spácháno celkem 184 trestných činů vztahujících se k § 180 (Neoprávněné nakládání s osobními údaji). V Jihočeském kraji bylo celkem spácháno 8 trestných činů souvisejících s tímto paragrafem. Na ÚO České Budějovice se objevil pouze v roce 2007 1 případ.

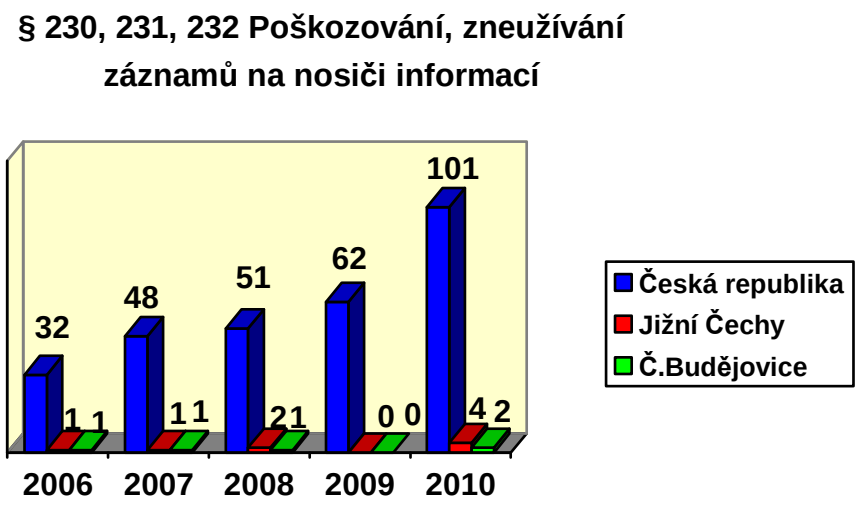
Graf 13 § 182 Porušování tajemství dopravovaných zpráv



Zdroj: Evidence trestního řízení (ETŘ), a Kriminalistický statistický údaj (KSU) Policie ČR

V souvislosti s § 182 (Porušování tajemství dopravovaných zpráv) bylo v celé České republice od roku 2006 spácháno celkem 99 trestných činů a v jižních Čechách pouze 3 trestné činy. Na ÚO České Budějovice nebyl v souvislosti s § 182 spáchán žádný trestný čin.

Graf 14 § 230, 231, 232 poškozování, zneužívání záznamů na nosiči informací



Zdroj: Evidence trestního řízení (ETŘ), a Kriminalistický statistický údaj (KSU) Policie ČR

V grafu 14 je patrný značný nárůst počtu trestných činů spojených s § 230, 231, 232 v roce 2010 na celém území České republiky.

7.2 PRAKTICKÉ PŘÍKLADY U POLICIE ČR

Způsob prověřování

- lustrace v evidencích PČR
- lustrace v systému provozovatele internetového aukčního - inzertního portálu (hodnocení prodejců)
- místní příslušnost
- žádost na provozovatele internetového aukčního – inzertního portálu
- bankovní informace (kamerové záznamy, internetové bankovnictví), zvážit postup podle § 79 a tr. řádu - zajištění peněžních prostředků na účtu banky
- zajistit uskutečněný telekomunikační provoz dle 88a/1 tr. řádu (IP adresy, telefonní čísla, emailové schránky)
- aktivně vyhledávat poškozené
- výslech podezřelého

Případy informační kriminality na ÚO České Budějovice

Na úvod této kapitoly bych rád poukázal, že v ní nepůjde o postižení celé problematiky informační a počítačové kriminality. Účelem je ilustrativní doplnění a dokreslení předchozí textové části pro její snadnější pochopení.

Při výběru jednotlivých případů jsem se zaměřil na kauzy související s podvodným jednáním při obchodování prostřednictvím Internetu. Při jejich vyhledávání jsem se omezil na období po roce 2008. Jedná se o případy, které patří k nejtypičtějším, nejčastějším, nejzajímavějším nebo k těm, které dle mého názoru vykazují vysoký stupeň nebezpečnosti pro společnost.

Kazuistika 1

Poškozenému z Českých Budějovic nevyplatilo zaslat peníze předem. Na internetovém portálu nalezl nabídku prodeje nového notebooku za „dobrý peníz“, necelých 6.000 korun, poslal tedy peníze na uvedený účet předem prodávajícímu pod přezdívkou „kumr…“ a počítače se nedočkal. Na jeho urgence pak nikdo na uvedeném kontaktním mailu nereagoval. Policisté

se i přes anonymní internetové prostředí dopátrali pachatele (muž 23 let) z Litomyšle a obvinili jej z trestného činu podvodu.[79]

Kazuistika 2

V březnu 2011 vypátrali kriminalisté muže, který provozoval internetové stránky vytvořené jako solidně se tvářící e-obchod. Také on prodával pouze virtuálně, nabízel zboží, spíše jeho fotografie na stránkách za velmi výhodné ceny, zboží však ve skutečnosti nikdy neměl. Stránky měl v provozu jeden měsíc. Tedy jen tak dlouho, aby desítky podvedených nestačily cestou policie reagovat. Za měsíc provozu stránek si přišel po malých částkách, (prodával drobnou kosmetiku) za několik set korun, na bezmála 1.000 000 korun. Jeho náklady byly nulové.[80]

[79] Policie České republiky – KŘP Jihočeského kraje. Matzner, J. Počítačová kriminalita roste. [online]. 29.4.2011 [Cit. 2011-09-08]. Dostupný z: <http://www.policie.cz/clanek/pocitacova-kriminalita-roste.aspx

[80] Policie České republiky – KŘP Jihočeského kraje. Matzer, J. Počítačová kriminalita roste. [online]. 29.4.2011 [Cit. 2011-09-08]. Dostupný z: <http://www.policie.cz/clanek/pocitacova-kriminalita-roste.aspx

ZÁVĚR

Při nákupu prostřednictvím internetu je potřeba být pozorný, prověřit si prodejce na diskusních fórech a srovnávacích webech, podívat se na důležité body obchodních podmínek. Tak se lze snáz vyhnout nedůvěryhodnému prodejci nebo přímo podvodnému webu. Je důležité být ostražitý při nákupu výrazně levného zboží. Nakupovat u e-shopů řádně registrovaných, osvědčených, působících na trhu již několik let. Kupující na internetu by měli sledovat recenze spokojenosti nakupujících s daným obchodem, aukční síní či e-bazarem. V poslední řadě by neměli přistupovat na nabídku typu: „Ušetříte 15-25 či více %, platba na uvedený účet předem."

Důvěra či nedůvěra mezi obchodními partnery nás provází od počátků vzniku obchodních transakcí mezi lidmi nebo skupinami lidí. V klasickém pojetí obchodu často odhadujeme důvěryhodnost obchodního partnera z našeho prvního dojmu (oblečení, vzhled, vystupování, instinkt…), nebo spíše dáme na své minulé zkušenosti s ním nebo na doporučení svých známých. Pokud využíváme online systému, kdy velké množství našich interakcí je prováděno za situace, kdy s druhým člověkem nejsme ve fyzickém kontaktu a ani o něm nic nevíme, musíme se spoléhat na jiné mechanismy, na reputační mechanismy implementované v online systému. Využíváme např. i toho, že většina webových stránek i obchodních společností v současné době má v sobě zabudovaný mechanismus, pomocí kterého mohou vyjádřit uživatelé své názory například na produkty apod., a tím dát i určitým způsobem najevo důvěru k produktům. V rámci těchto C2C online systémů můžeme definovat důvěru jako „explicitní názor vyjádřený uživatelem o jiném uživateli, který vyjadřuje vnímání určitých charakteristik tohoto uživatele".[81]

Pro uchopení problematiky počítačové a informační kriminality je zapotřebí si uvědomit několik souvislostí: A sice, že výše uvedená problematika je s ohledem na historii kriminality novým oborem, a tudíž by bylo vhodné, aby se jí zabývali z hlediska organizačně-technického odborníci, kteří:„[...] jsou schopni držet krok s aktuálními trendy v dané problematice; disponují technickým vybavením, které jim umožňuje efektivně čelit existujícím hrozbám ...".[82] To vyžaduje především neustálé vzdělávání v oblasti ochrany dat, informační

[81] BERÁNEK, L. *Modelování důvěry a reputace se zaměřením na C2C systémy*. České Budějovice: Kopp, 2009. 182 s. ISBN 978-80-7232-387-6.

[82] JIROVSKÝ, V. – HNÍK, V. – KRULÍK, O. Kybernetické hrozby: Výzva pro moderní společnost. In *Přítomnost a budoucnost krizového řízení* [online]. Praha: T-Soft, 2006 [cit. 2007-06-26]. Dostupné z WWW: <http://www.mvcr.cz/bezpecnost/informacni/kyberneticke_hrozby.pdf>.

bezpečnosti aj. na úrovni politiků, manažerů, informačních specialistů, zaměstnanců firem, policistů a zaměstnanců dalších státních organizací.

Stále častěji se objevují případy, na které náš právní řád nedokáže promptně reagovat. Novelizace právních předpisů mnohdy probíhá pomaleji než vývoj ve vynalézavosti nových přístupů ve zneužívání informačních technologií.

Proto je nezbytná pro řešení počítačové a informační kriminality také kvalitní vnitrostátní legislativa. Je zapotřebí, aby zároveň se společenskými změnami, kterými procházíme, byly modernizovány i legislativní dokumenty jako trestní zákony týkající se ekonomické kriminality související s využitím počítače; zákony na ochranu duševního vlastnictví; zákony na ochranu údajů, ochranu soukromí, ochranu před nezákonným či škodlivým obsahem; trestní právo procesní; právní regulace bezpečnostních opatření, jako je šifrování nebo elektronický podpis.[83] Důležité je také správné načasování modernizace legislativy tak, aby se nedařilo počítačovým zločincům být vždy o krok vpřed před zákonem.

Závěrem lze konstatovat, že ať se bude vývoj informačních technologií ubírat jakkoliv, je boj s informační kriminalitou marný, pokud nedojde ke sjednocení právních řádů jednotlivých zemí. Internet nemá hranice a tudíž jeho omezování jen v některých státech se tak míjí účinkem. Zde už je tak dán prostor pro mezinárodní společenství a mezinárodní dohody.

Přes složitost vyšetřování a dokazování podvodu konkrétnímu pachateli však kriminalisté zhruba polovinu případů objasní. To však neznamená, že usvědčený podvodník vrátí poškozenému peníze. Co se týče trendů budoucího vývoje, lze říci, že v současné době jsou na vzestupu různá podvodná jednání, a to i přes častá varování v médiích. Doufejme, že se jedná jen o dočasný trend, který se rychle zvrátí poté, co společnost nabude větších zkušeností s počítači.

[83] Institut pro kriminologii a sociální prevenci. *11. kongres OSN o prevenci kriminality a trestní justici: Bangkok 18. – 25. dubna 2005 : Základní dokumenty 11. kongresu předložené delegátům* [online]. 2006 [cit. 2011-11-18]. Dostupné z WWW: <http://www.ok.cz/iksp/docs/322.pdf>.

SEZNAM POUŽITÉ LITERATURY

1. Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení. www.mvcr.cz/dokument/2006/informacni.doc
2. BERÁNEK, L. *Modelování důvěry a reputace se zaměřením na C2C systémy*. České Budějovice: Kopp, 2009. 182 s. ISBN 978-80-7232-387-6.
3. Citibank, a.s. Dementi. *Měšec.cz* [online]. 25.11.2006. [2011-08-12]. Dostupné z WWW:< http://www.mesec.cz/tiskove-zpravy/dementi/>. ISSN 1213-4414.
4. Citibank, a.s. Dementi. *Měšec.cz* [online]. 25.11.2006. [2011-09-02]. Dostupné z WWW:< http://www.mesec.cz/tiskove-zpravy/dementi/>. ISSN 1213-4414.
5. Council of Europe. *Additional protocol to the Convention on cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems : CETS No. : 189* [online].[cit. 2011-08-14]. Dostupné z WWW: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=6/14/2007&CL=ENG>.
6. Council of Europe. *Convention on Cybercrime* [online]. 2001.[cit. 2011-09-08]. Dostupné z WWW: <http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.
7. CHMELÍK, J. a kol. *Rukověť kriminalistiky*. Vyd. Plzeň: Aleš Čeněk 2005. 532 s. ISBN 80-86898-36-9.
8. ČERMÁK, J. *Internet a autorské právo*. 2. aktualiz. a rozš. vyd. Praha: Linde, 2003. 251 s. ISBN 80-7201-423-4.
9. Česká spořitelna, a.s. Čs. odvrací napadení svého internetbankingu phishingem a pharmingem. *Měšec.cz* [online]. 16.3.2007 [cit. 2007-06-19].
10. Dostupné z WWW: < http://www.mesec.cz/tiskove-zpravy/cs-odvraci-napadeni-sveho-internetbankingu-phishingem-a-pharmingem/>. ISSN 1213-4414
11. Česká spořitelna, a.s. Čs. odvrací napadení svého internetbankingu phishingem a pharmingem. *Měšec.cz* [online]. 16.3.2007 [cit. 2011-08-12].
12. Dostupné z WWW:<http://www.mesec.cz/tiskove-zpravy/cs-odvraci-napadeni-sveho-internetbankingu-phishingem-apharmingem/>. ISSN 1213-4414.
13. DASTYCH, J. *Počítačová kriminalita* [online]. 1998. [cit. 2011-08-03]. Dostupné z WWW: http://www.dolphin.cz/policie/pocitacova_kriminalita.html
14. DLOUHÝ, M. Úmluva o počítačové kriminalitě. *Kriminalistický sborník*. 2004, roč. 48, č. 2, s. 37-38

15. HODBOĎ, T. Internetové obchody tak jak je známe, zahynou. *Lupa: server o českém internetu* [online]. 2008 [Cit. 2011-09-08].
Dostupné z: <http://www.lupa.cz/clanky/internetove-obchody-tak-jak-je-zname-zahynou/>. ISSN 1213-0702.
16. HURYCH, J. Etika v informační společnosti. *Národní knihovna: knihovnická revue* [online]. 2003, roč. 13, č. 1 [cit. 2011-09-08]. Dostupné z WWW: <http://knihovna.nkp.cz/NKKR0301/0301003.html>.
17. E-tržiště. *B2B Centrum* [online]. c2011 [Cit. 2011-09-08]. Dostupné z: <http://www.b2bcentrum.cz/cs/e_marketplace>.
18. Frequently Asked Questions. *Programmable Web* [online]. c2011 [Cit. 2011-09-08]. Dostupné z: <http://www.programmableweb.com/faq>.
19. Internetový obchod. *Wikipedie: otevřená encyklopedie.* [online]. 2011 [Cit. 2011-09-08]. Dostupné z: <http://cs.wikipedia.org/wiki/Internetov%C3%BD_obchod>.
20. JIROVSKÝ, V.: Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství, Praha: Grada, 2007. 284 s. ISBN 80-247-1561-9.
21. JIROVSKÝ, V. – HNÍK, V. – KRULÍK, O. Kybernetické hrozby: Výzva pro moderní společnost. *In Přítomnost a budoucnost krizového řízení* [online]. Praha: T-Soft, 2006 [cit. 2011-09-08]. Dostupné z WWW: <http://www.mvcr.cz/bezpecnost/informacni/kyberneticke_hrozby.pdf>.
22. JIROVSKÝ, V. – HNÍK, V. – KRULÍK, O. *Základní definice, vztahující se k tématu kybernetických hrozeb* [online]. c2005. [cit. 2011-09-08]. Dostupné z WWW: <http://www.mvcr.cz/bezpecnost/informacni/zakladni_info.pdf>.
23. JELÍNEK, J. A KOL.: Trestní právo hmotné. Obecná a zvláštní část. 2. aktualizované vydání. Linde, Praha 2006. ISBN 80/7201/533/8.
24. KLEGA, V. Povedený nákupní rádce. *Chip.cz* [online]. 2007 [Cit. 2011-09-08]. Dostupné z: <http://www.chip.cz/cs/novinky-ze-sveta-it/povedeny-nakupni-radce.html>.
25. KOČIČKA, P. Jak se nenechat napálit v internetových aukcích. *Technet.cz* [online]. 2008 [Cit. 2011-09-08]. Dostupný z: <http://technet.idnes.cz/jak-se-nenechat-napalit-v-internetovych-aukcich-f5a-/sw_internet.asp?c=A080114_210515_sw_internet_vse>.
26. Kolektiv autorů. Manuál OSN pro prevenci a kontrolu počítačového zločinu (United Nations Manual On The Preventiv and Kontrol Of The Komputer Crime), OSN, 1994, hptt/www.uncjin.org/Dokument/EightsCongress.html
27. KŘÍŽ, J., HOLCOVÁ, I., KORDAČ, J., KŘESŤANOVÁ, V.: *Autorský zákon a předpisy související – komentář.* 2. aktualizované vydání podle stavu k 1.9.2005, Praha, Linde Praha a.s., 2005

28. MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002. 106 s. ISBN 80-7226-419-2.
29. MINÁRIK, T.: *Počítačová kriminalita z pohledu trestního práva hmotného*. Rigorózní práce. Právnická fakulta Univerzity Karlovy 2007.
30. MUSIL, S.: *Počítačová kriminalita*. IKSP, 2000,
31. NESEJT, P. První phishing v Česku, terčem byla CitiBank. *finance.cz* [online]. 16.3.2006. [cit. 2011-06-21]. Dostupné z WWW: <http://www.finance.cz/zpravy/finance/63677/?auth=391272ec5c170738ad1dedc21a8d4214>. ISSN 1213-4325.
32. NOVOTNÝ, F. *Trestní právo hmotné*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2004. 310 s. ISBN 80-8647-367-8.
33. NOVOTNÝ, O., VANDUCHOVÁ, M. a kol.: *Trestní právo hmotné – I. Obecná část.* 5., jubilejní, zcela přepracované 5. vydání. Praha: ASPI, a.s., 2007, s 555. ISBN 978-80-7357-258-7 (sv. 1 : váz.).
34. NOVOTNÝ, O., VOKOUN, R. a kol.: *Trestní právo hmotné – II. Zvláštní část*. 5., jubilejní, zcela přepracované vydání. Praha: ASPI, a.s., 2007, s 479. ISBN 978-80-7357-259-4 (sv. 2 : váz.).
35. Policie České republiky – KŘP Jihočeského kraje. Matzner, J. Počítačová kriminalita roste. [online]. 29.4.2011 [Cit. 2011-09-08]. Dostupný z: <http://www.policie.cz/clanek/pocitacova-kriminalita-roste.aspx
36. SMEJKAL, V. *Právo informačních a telekomunikačních systémů*. 2., aktualiz. a rozš. vyd. Praha: C. H. Beck, 2004. 770 s. ISBN 80-7179-765-0.
37. SMEJKAL, V. a kol.: *Právo informačních a telekomunikačních systémů.* 1. vydání. Praha: C.H.Beck, 2001. 542 s. ISBN 80-7179-552-6.
38. SMEJKAL, V. *Internet a §§§*. 2. aktualiz. a rozš. vyd. Praha: Grada, 2001. 284 s. ISBN 80-247-0058-1.
39. SMEJKAL, L. *Nová evropská směrnice o ochraně autorského práva v informační společnosti* [online]. [cit. 2011-06-15]. Dostupné z WWW: < http://www.itpravo.cz/index.shtml?x=48901>.
40. SMEJKAL, V. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. *Trestněprávní revue*, 2003, 2. roč., č. 6, s. 161-167 ISSN 1213-5313.
41. SMEJKAL, V. – SOKOL, T. – VLČEK, M. *Počítačové právo*. Praha : C.H. Beck: SEVT, 1995. 264 s. ISBN 80-7179-009-5.

42. STEINOVÁ, M; HLUCHNÍKOVÁ, M; PŘÁDKA, M. *E-marketing II.: marketingová komunikace na internetu: elektronické obchodování.* 1. vyd.. Ostrava: Vysoká škola báňská - Technická univerzita, 2003. 107 s. ISBN 80-248-0351-8.
43. STUCHLÍK, P; DVOŘÁČEK, M. *Marketing na Internetu*. 1. vyd.. Praha: Grada, 2000. 247 s. ISBN 80-7169-957-8.
44. TREVATHAN, J. Security, Anonymity and Trust in Electronic Auctions. ACM Crossroads [online]. 2004[cit.2011-09-10]. Dostupné z WWW: <http://www.acm.org/crossroads/xrds11-3/sat.html>.
45. ŠÁMAL, P., PÚRY, F., RIZMAN, S.: *Trestní zákon*. Komentář. 6. vydání. C.H.Beck, Praha 2004. ISBN 80-7179-896-7.
46. ÚZ *Úplné znění. Trestní zákoník 2010*. vyd. Sagit,a.s. ISBN 987-80-7208-736-5.
47. ZÁMEČNÍK, Petr. Podvodná stránka České spořitelny. *Měšec.cz* [online]. 19.3.2007. [cit. 2011-09-08]. Dostupné z WWW: <http://www.mesec.cz/clanky/podvodna-stranka-ceske-sporitelny/>. ISSN 1213-4414.
48. ZELENKA, J. – ČECH, P. – NAIMAN, K. *Ochrana dat: Informační bezpečnost – výkladový slovník.* Hradec Králové: Gaudeamus, 2002. 164 s. ISBN 80-7041-197-X.

Elektronické zdroje

http://cms.e-bezpeci.cz
http://computerworld.cz/
http://cs.wikipedia.org
http://en.wikipedia.org
http://idnes.cz
http://sk.wikipedia.org
http://trestnizakonik.cz
http://www.dsl.cz
http://www.emag.cz
http://www.hackery.estranky.cz
http://www.hoax.cz
http://www.info-koktejl.cz
http://www.itpravo.cz
http://www.lupa.cz
http://www.mvcr.cz
http://www.novinky.cz
http://www.pripojtese.cz
http://www.root.cz

http://www.trosky.cz
http://www.warez.cz
http://www.webcrunchers.com/crunch

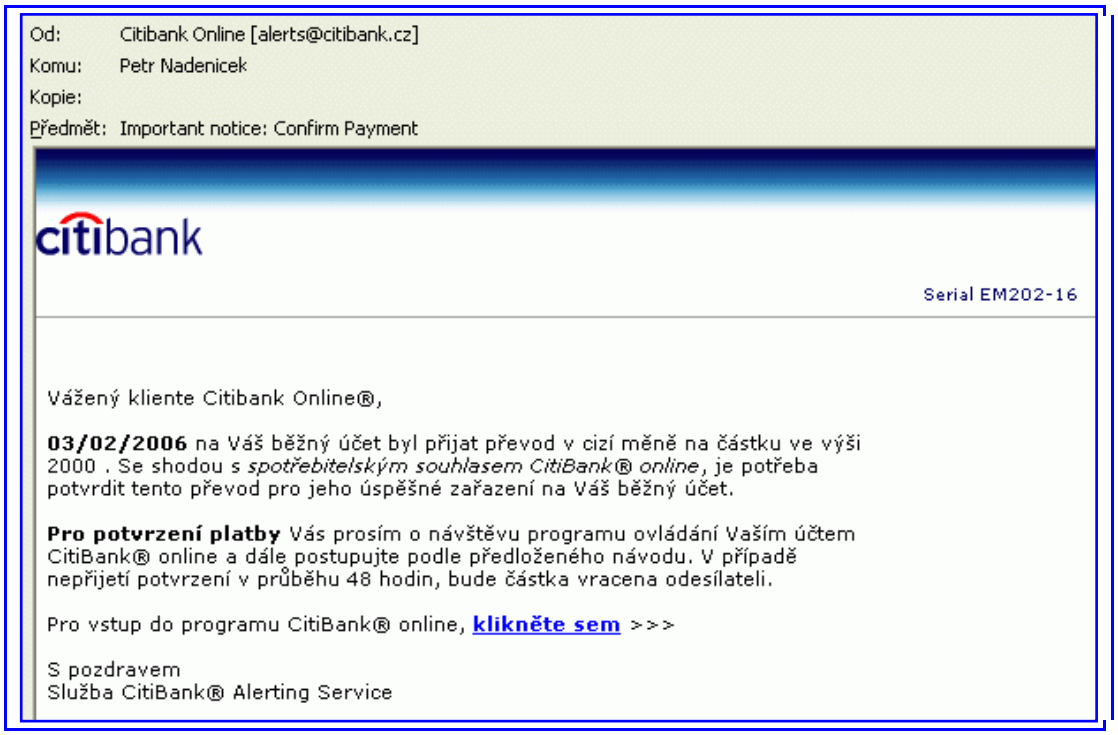
SEZNAM GRAFŮ

SEZNAM PŘÍLOH

Příloha 1

První phishing v České republice

Česká pobočka bankovního ústavu CitiBank byla **v březnu roce 2006** napadena historicky prvním phishingovým útokem v českém jazyce. Zákazníci zmíněného ústavu obdrželi na první pohled zcela běžný email:


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

citibank

Serial EM202-16

Vážený kliente Citibank Online®,

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

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

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

S pozdravem
Služba CitiBank® Alerting Service

Obr. 1 – Falešný email zaslaný klientům bankovního ústavu CitiBank [84]

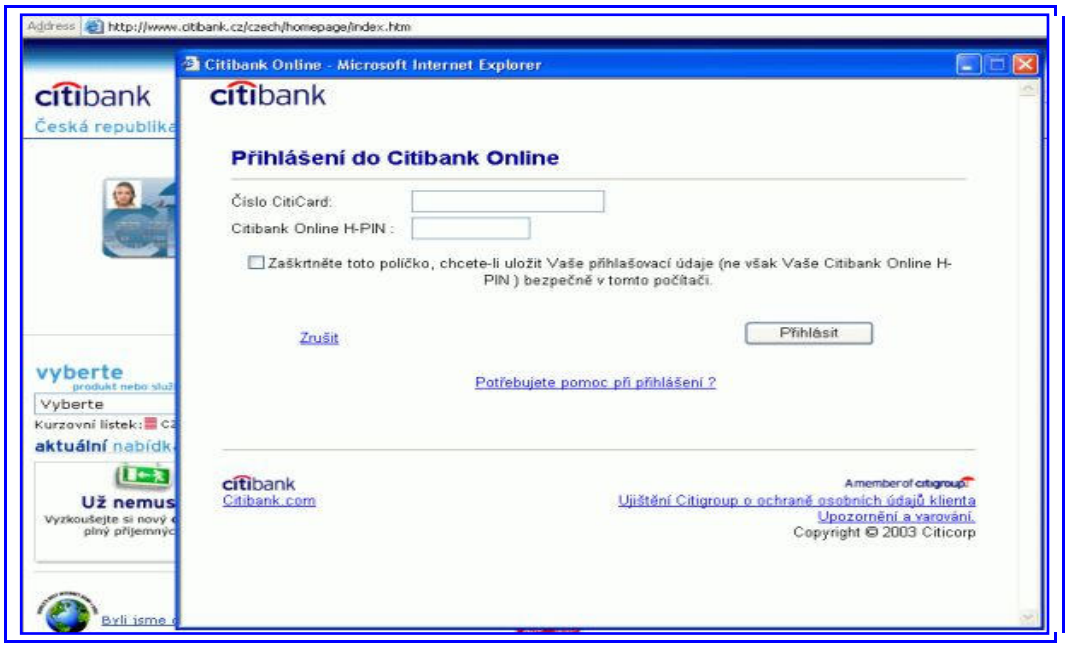
Pokud by některý z klientů banky uposlechl a řídil se pokyny na emailu, byl by přesměrován na falešnou webovou stránku a zřejmě by přišel o své úspory uložené v bance. Text tohoto falešného emailu byl vytvořen podle pravidel sociálního inženýrství s cílem oklamat příjemce a vylákat od něj citlivé informace o jeho bankovním kontě.

V tomto případě prvního zachyceného phishingového podvodu se nakonec nic vážného nestalo; bance se zavčas podařilo vyřadit falešnou stránku z provozu a žádný z klientů banky o své úspory nepřišel. [85]

---

[84] NESEJT, P První phishing v Česku, terčem byla CitiBank. *finance.cz* [online]. 16.3.2006. [cit. 2011-09-02].Dostupné z WWW: <http://www.finance.cz/zpravy/finance/63677/?auth=391272ec5c170738ad1dedc21a8d4214>.

[85] NESEJT, P První phishing v Česku, terčem byla CitiBank. *finance.cz* [online]. 16.3.2006. [cit. 2011-09-02].Dostupné z WWW: <http://www.finance.cz/zpravy/finance/63677/?auth=391272ec5c170738ad1dedc21a8d4214



Obr. 2 - Podvodná webová stránka bankovního ústavu CitiBank [86]

Obr. 3 – Skutečná webová stránka bankovního ústavu CitiBank [87]

[86] NESEJT, P První phishing v Česku, terčem byla CitiBank. *finance.cz* [online]. 16.3.2006. [cit. 2011-09-02].Dostupné z WWW: <http://www.finance.cz/zpravy/finance/63677/?auth=391272ec5c170738ad1dedc21a8d4214>.

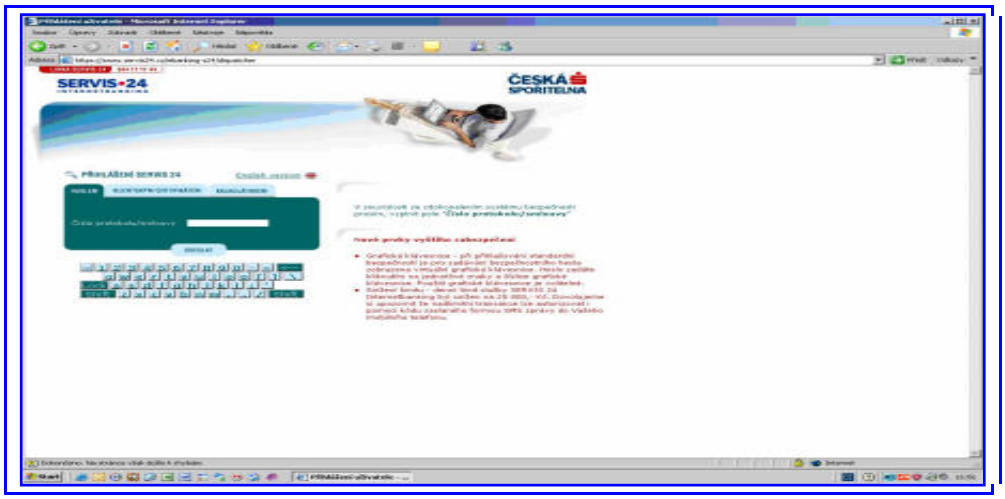
[87] NESEJT, P První phishing v Česku, terčem byla CitiBank. *finance.cz* [online]. 16.3.2006. [cit. 2011-09-02].Dostupné z WWW: <http://www.finance.cz/zpravy/finance/63677/?auth=391272ec5c170738ad1dedc21a8d4214>.

Příloha 2

Případ nebezpečného phishingu a pharmingu

V České republice byl v **březnu 2007** zaznamenán útok ve formě phishingu na internetové bankovnictví České spořitelny. Média informovala, že se s největší pravděpodobností jednalo o rozsáhlou mezinárodní akci, která souvisí s napadením dřívějším – banky Raiffeisenbank u nás. Údajně byly napadeny stejným způsobem i další banky v zahraničí. [88]

Jak uvedla zpráva České spořitelny, použili pachatelé mimo metod phishingu i tzv. pharming. Zhruba 50 klientů České spořitelny nahlásilo setkání s falešnou webovou stránkou ústavu. Podle vyjádření banky nebyl nikdo poškozen.



Obr. 4 – Podvodná webová stránka České spořitelny [89]

Obr. 5 – Pravá přihlašovací webová stránka České spořitelny [90]

[88] ZÁMEČNÍK, P. Podvodná stránka České spořitelny. *Měšec.cz* [online]. 19.3.2007. [cit. 2011-09-01]. Dostupné z WWW: <http://www.mesec.cz/clanky/podvodna-stranka-ceske-sporitelny/>.
[89] ZÁMEČNÍK, P. Podvodná stránka České spořitelny. *Měšec.cz* [online]. 19.3.2007. [cit. 2011-09-01]. Dostupné z WWW: <http://www.mesec.cz/clanky/podvodna-stranka-ceske-sporitelny/>.

Příloha 3

Příklad e-mailu

Následující e-mail obdrželo velké množství českých uživatelů na začátku **října 2006**:

Dobrý den vážení klienti!

Léto roku 2006 bylo pro Banku nejzávažnějším z hlediska počtu nelegálních operací. Čím dál více mají podvodníci zájem o důvěrnou informaci našich zákazníků. Velké množství lidí se na nás obrací s žádostí zamezit vzniku nebezpečí ztráty peněžních prostředků z účtu.

S ohledem na současný stav vyhlašuje Banka následující měsíc za měsíc boje s frodem. Do 1. listopadu musí všichni naši klienti aktivovat nový systém bezpečnosti vlastních účtů.

Provedli jsme velkou práci pro zlepšení bezpečnosti. Systém byl zkontrolován uznávanými odborníky v oboru elektronických plateb, a všechny nezávislí experti potvrdili účinnost systému proti frodu. Z důvodu nebezpečí možného zneužití těchto údajů podvodníky nejsou tyto data zveřejněna v otevřených zdrojích.

Vy jste byl(a) zvolen(a) jako jeden z účastníků finálního stadia testovaní systému. V současné době Vám navrhujeme využít odkaz *podvržený odkaz* a standardním způsobem přihlášení do Internet bankingu aktivovat nový bezpečnostní systém. V aktuálním stadiu provozu jsou možné některé nesrovnalosti.

Připouštíme jejich existenci, a proto prosím nezasílejte dodatečné popisy vznikajících potíží, práce na jejich odstranění již probíhají.

Musíme Vás informovat o bezpodmínečném použití nového systému od listopadu, v opačném případě budou Vaše účty zablokovány do okamžiku úplné identifikace Vaší osoby. Proto doporučujeme v nejkratší možné době přejít na nový bezpečnostní standard.

S pozdravem, Oddělení Banky pro ochranu před frodem.

---

[90] ZÁMEČNÍK, P. Podvodná stránka České spořitelny. *Měšec.cz* [online]. 19.3.2007. [cit. 2011-09-01]. Dostupné z WWW: <http://www.mesec.cz/clanky/podvodna-stranka-ceske-sporitelny/>.

Příloha 4 Statistické tabulky

Tabulka 1 České Budějovice

ÚO České Budějovice		Zjištěno	Objasněno		Spácháno skutků		Stíháno, vyšetřováno osob			
			Počet	Tj.%	Recidivisté	Mladiství 15-17 let	Celkem	Recidivisté	Nezletilí 1-14 let	Mladiství 15-17 let
ROK	Název									
2010	Neoprávněné nakládání s osobními údaji 180 (§ 178)	0	0	0,00	0	0	0	0	0	0
2009		0	0	0,00	0	0	0	0	0	0
2008		0	0	0,00	0	0	0	0	0	0
2007		1	1	100,00	0	0	1	0	0	0
2006		0	0	0,00	0	0	0	0	0	0

Tabulka 2 České Budějovice

ÚO České Budějovice		Zjištěno	Objasněno		Spácháno skutků		Stíháno, vyšetřováno osob			
			Počet	Tj.%	Recidivisté	Mladiství 15-17 let	Celkem	Recidivisté	Nezletilí 1-14 let	Mladiství 15-17 let
ROK	Název									
2010	Porušování tajemství dopravovaných zpráv § 182 (§§ 239/2, 240/2)	0	0	0,00	0	0	0	0	0	0
2009		0	0	0,00	0	0	0	0	0	0
2008		0	0	0,00	0	0	0	0	0	0
2007		0	0	0,00	0	0	0	0	0	0
2006		0	0	0,00	0	0	0	0	0	0

Tabulka 3 České Budějovice

ÚO České Budějovice		Zjištěno	Objasněno		Spácháno skutků		Stíháno, vyšetřováno osob			
ROK	Název		Počet	Tj.%	Recidivisté	Mladiství 15-17 let	Celkem	Recidivisté	Nezletilí 1-14 let	Mladiství 15-17 let
2010	Poškozování a zneužívání záznamů na nosiči informací §§ 230, 231, 232 (§ 257a)	2	2	100,00	0	0	2	0	1	0
2009		0	0	0,00	0	0	0	0	0	0
2008		1	0	0,00	0	0	1	0	0	0
2007		1	1	100,00	0	0	1	0	0	0
2006		1	1	100,00	0	0	1	0	0	0

Tabulka 4 Jihočeského kraje

KŘP Jihočeského kraje		Zjištěno	Objasněno		Spácháno skutků		Stíháno, vyšetřováno osob			
ROK	Název		Počet	Tj.%	Recidivisté	Mladiství 15-17 let	Celkem	Recidivisté	Nezletilí 1-14 let	Mladiství 15-17 let
2010	Neoprávněné nakládání s osobními údaji 180 (§ 178)	2	1	50,00	0	0	2	0	0	0
2009		1	1	100,00	0	0	1	0	0	0
2008		3	1	33,33	0	0	1	0	0	0
2007		1	1	100,00	0	0	1	0	0	0
2006		1	1	100,00	0	0	0	0	0	0

Tabulka 5 Jihočeského kraje

KŘP Jihočeského kraje		Zjištěno	Objasněno		Spácháno skutků		Stíháno, vyšetřováno osob			
ROK	Název		Počet	Tj.%	Recidivisté	Mladiství 15-17 let	Celkem	Recidivisté	Nezletilí 1-14 let	Mladiství 15-17 let
2010	Porušování tajemství dopravovaných zpráv § 182 (§§ 239/2, 240/2)	2	0	00,00	0	0	0	0	0	0
2009		0	0	0,00	0	0	0	0	0	0
2008		0	0	0,00	0	0	0	0	0	0
2007		0	0	0,00	0	0	0	0	0	0
2006		1	1	100,00	0	0	1	0	0	0

Tabulka 6 Jihočeského kraje

KŘP Jihočeského kraje		Zjištěno	Objasněno		Spácháno skutků		Stíháno, vyšetřováno osob			
ROK	Název		Počet	Tj.%	Recidivisté	Mladiství 15-17 let	Celkem	Recidivisté	Nezletilí 1-14 let	Mladiství 15-17 let
2010	Poškozování a zneužívání záznamu na nosiči informací §§ 230, 231, 232 (§ 257a)	4	3	75,00	0	0	3	0	1	0
2009		0	0	0,00	0	0	0	0	0	0
2008		2	0	0,00	0	0	1	0	0	0
2007		1	1	100,00	0	0	1	0	0	0
2006		1	1	100,00	0	0	1	0	0	0

Tabulka 7 Česká republika

ROK	Česká republika	Zjištěno	Objasněno		Spácháno skutků		Stíháno, vyšetřováno osob			
	Název		Počet	Tj.%	Recidivisté	Mladiství 15-17 let	Celkem	Recidivisté	Nezletilí 1-14 let	Mladiství 15-17 let
2010	Neoprávněné nakládání s osobními údaji § 180 (§ 178)	31	5	16,13	2	0	6	2	0	0
2009		27	10	37,04	0	0	12	0	0	0
2008		44	20	45,45	3	0	16	2	0	0
2007		36	14	38,89	2	0	14	2	0	0
2006		46	31	67,39	3	0	8	2	0	0

Tabulka 8 Česká republika

ROK	Česká republika	Zjištěno	Objasněno		Spácháno skutků		Stíháno, vyšetřováno osob			
	Název		Počet	Tj.%	Recidivisté	Mladiství 15-17 let	Celkem	Recidivisté	Nezletilí 1-14 let	Mladiství 15-17 let
2010	Porušování tajemství dopravovaných zpráv § 182 (§§ 239/2, 240/2)	19	5	26,32	0	1	4	0	0	1
2009		28	15	53,57	2	0	11	0	0	0
2008		20	10	50,00	0	1	5	0	0	0
2007		17	10	58,82	1	0	9	1	0	0
2006		15	8	53,33	1	0	8	1	0	0

Tabulka 9 Česká republika

ROK	Česká republika	Zjištěno	Objasněno		Spácháno skutků		Stíháno, vyšetřováno osob			
	Název		Počet	Tj.%	Recidivisté	Mladiství 15-17 let	Celkem	Recidivisté	Nezletilí 1-14 let	Mladiství 15-17 let
2010	Poškozování a zneužívání záznamů na nosiči informací §§ 230, 231, 232 (§ 257a)	101	30	29,70	13	0	31	6	1	1
2009		62	20	32,26	5	0	16	3	0	0
2008		51	15	29,41	3	2	15	1	2	0
2007		48	13	27,08	0	0	10	0	0	0
2006		32	11	34,38	0	0	9	0	0	0

Příloha 5

Tabulka 10 Č. Budějovice

2010	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	19	11	8
Hyperinzerce.cz	4	3	1
Mimibazar.cz	2	2	0
Sbazar.cz	1	0	1
Bazoš.cz	2	1	1
Celkem	**28**	**17**	**11**

Tabulka 11 Č. Budějovice

2009	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	11	5	6
Hyperinzerce.cz	1	1	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	0	0
Bazoš.cz	0	0	0
Celkem	**12**	**6**	**6**

Tabulka 12 Č. Budějovice

2008	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	13	10	3
Hyperinzerce.cz	1	1	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	0	0
Bazoš.cz	0	0	0
Celkem	**14**	**11**	**3**

Tabulka 13 Prachatice

2010	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	3	3	0
Hyperinzerce.cz	0	0	0
Mimibazar.cz	0	0	0
Sbazar.cz	1	1	0
Bazoš.cz	0	0	0
Celkem	**4**	**4**	**0**

Tabulka 14 Prachatice

2009	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	0	0	0
Hyperinzerce.cz	0	0	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	0	0
Bazoš.cz	0	0	0
Celkem	**0**	**0**	**0**

Tabulka 15 Prachatice

2008	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	3	2	1
Hyperinzerce.cz	0	0	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	0	0
Bazoš.cz	0	0	0
Celkem	**3**	**2**	**1**

Tabulka 16 Tábor

2010	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	1	1	0
Hyperinzerce.cz	2	1	1
Mimibazar.cz	0	0	0
Sbazar.cz	1	1	0
Bazoš.cz	0	0	0
Celkem	**4**	**3**	**1**

Tabulka 17 Tábor

2009	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	11	7	4
Hyperinzerce.cz	0	0	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	0	0
Bazoš.cz	0	0	0
Celkem	**11**	**7**	**4**

Tabulka 18 Tábor

2008	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	2	2	0
Hyperinzerce.cz	0	0	0
Mimibazar.cz	0	0	0
Sbazar.cz	2	2	0
Bazoš.cz	0	0	0
Celkem	**4**	**4**	**0**

Tabulka 19 Jindřichův Hradec

2010	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	5	5	0
Hyperinzerce.cz	1	1	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	0	0
Bazoš.cz	2	2	0
Celkem	**8**	**8**	**0**

Tabulka 20 Jindřichův Hradec

2009	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	4	3	1
Hyperinzerce.cz	1	1	0
Mimibazar.cz	0	0	0
Sbazar.cz	2	2	0
Bazoš.cz	0	0	0
Celkem	**7**	**6**	**1**

Tabulka 21 Jindřichův Hradec

2008	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	1	1	0
Hyperinzerce.cz	0	0	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	0	0
Bazoš.cz	0	0	0
Celkem	**1**	**1**	**0**

Tabulka 22 Český Krumlov

2010	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	5	3	2
Hyperinzerce.cz	1	1	0
Mimibazar.cz	0	0	0
Sbazar.cz	1	1	0
Bazoš.cz	0	0	0
Celkem	**7**	**5**	**2**

Tabulka 24 Český Krumlov

2008	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	1	0	1
Hyperinzerce.cz	0	0	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	0	0
Bazoš.cz	0	0	0
Celkem	**1**	**0**	**1**

Tabulka 23 Český Krumlov

2009	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	2	1	1
Hyperinzerce.cz	0	0	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	0	0
Bazoš.cz	0	0	0
Celkem	**2**	**1**	**1**

Tabulka 26 Strakonice

2010	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	4	3	1
Hyperinzerce.cz	0	0	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	1	0
Bazoš.cz	0	0	0
Celkem	**4**	**3**	**1**

Tabulka 27 Strakonice

2009	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	12	10	2
Hyperinzerce.cz	1	1	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	0	0
Bazoš.cz	0	0	0
Celkem	**13**	**11**	**2**

Tabulka 28 Strakonice

2008	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	0	0	0
Hyperinzerce.cz	0	0	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	0	0
Bazoš.cz	0	0	0
Celkem	**0**	**0**	**0**

Tabulka 29 Písek

2010	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	1	1	0
Hyperinzerce.cz	0	0	0
Mimibazar.cz	0	0	0
Sbazar.cz	1	1	0
Bazoš.cz	0	0	0
Celkem	**2**	**2**	**0**

Tabulka 30 Písek

2009	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	0	0	0
Hyperinzerce.cz	1	1	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	0	0
Bazoš.cz	1	1	0
Celkem	**2**	**2**	**0**

Tabulka 31 Písek

2008	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	3	2	1
Hyperinzerce.cz	0	0	0
Mimibazar.cz	0	0	0
Sbazar.cz	0	0	0
Bazoš.cz	0	0	0
Celkem	**3**	**2**	**1**

Tabulka 32 Jihočeský kraj

2010	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	39	28	11
Hyperinzerce.cz	9	6	3
Mimibazar.cz	2	2	0
Sbazar.cz	7	6	1
Bazoš.cz	2	1	1
Celkem	**59**	**43**	**16**

Tabulka 33 Jihočeský kraj

2009	Trestný čin	Objasněno	Neobjasněno
Aukro.cz	40	26	14
Hyperinzerce.cz	4	4	0
Mimibazar.cz	0	0	0
Sbazar.cz	2	2	0
Bazoš.cz	0	0	0
Celkem	**46**	**32**	**14**

Zdroj: Evidence trestního řízení (ETŘ), a Kriminalistický statistický údaj (KSU) Policie

Tabulka 34 Jihočeský kraj

2008	Trestný čin	Objasněno	Neobjasněno
Aukro	20	15	5
Hyperinzerce	1	1	0
Mimibazar	0	0	0
Sbazar	2	2	0
Bazoš	0	0	0
Celkem	**23**	**18**	**5**