JUDr. Jan Kolouch

KYBERNETICKÉ ÚTOKY

Cílem článku je uvést nejběžnější útoky, ke kterým dochází v síti Internet. Určitá protiprávní jednání v kyberprostoru je možné podřadit pod příslušná ustanovení platného trestního zákona, existují však určité typy jednání, jejichž označení za trestné činy může být podstatně obtížnější, či dokonce nemožné.

V současné době dochází ke stále častějším útokům[1] na počítače (hardware), software, data či sítě samotné. Útoky jsou stále sofistikovanější, účinnější a to i díky absenci trestněprávní ochrany před těmito novými protiprávními způsoby jednání. Počítač zde může být cílem útoku, ale současně je však vždy i prostředkem sloužícím k napadení. De facto jsou tyto útoky největší hrozbou v rámci kyberprostoru (prostoru informačních sítí). **Hrozbu** jako takovou lze definovat jako akt směřující ke změně[2] informace, aplikací či systému samotného.

Jirovský vymezuje čtyři skupiny základních hrozeb a také velmi výstižně charakterizuje jejich vztah:[3]

1. **Únik informace** je stav, kdy dojde k vyzrazení chráněné informace neautorizovanému subjektu.
2. **Narušení integrity** představuje poškození, změnu, či vymazání dat.

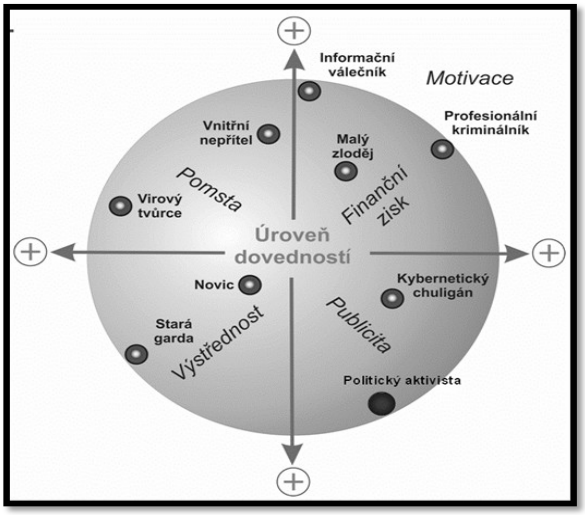
1Srov. PROSISE, Ch., MANDIVA, K. *Incident response & komputer forensic, second edition.* Emeryville : McGraw-Hill Companies, 2003. s. 13

2Změnou je míněna i krádež informace, její zničení, či zmaření jejího užití.

3Srov. JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha : Grada Publishing, a. s., 2007. s. 21 a násl.

3. **Potlačení služby** znamená úmyslné bránění v přístupu k informacím, aplikacím, či systému.[4]
4. **Nelegitimní použití** je užití informací neautorizovaným subjektem či neoprávněným způsobem.[5]

Je zřejmé, že veškeré hrozby musejí pocházet od určitých subjektů (útočníků), které je možné členit z různých hledisek. Jedno z nich je možné na podkladě výše uvedených hrozeb. Členění uvedené na obrázku č. 4 znázorňuje nejobecnější typizaci útočníků dle jejich motivace, mnohé z uvedených typů se mohou následně dělit či vzájemně splývat.



6

Možné členění útočníků v kyberprostoru dle motivace

4Jde například o útoky typu **DoS - Denial of Service**, kdy dojde k zahlcení informačního kanálu nesmyslnými informacemi. Následkem je pak nedostupnost informačních zdrojů.

5Například dojde k napadení zpoplatněného systému a využívání jeho služeb bez platby za služby.

6Zdroj: RAK, R. Homo sapiens versus security. ICTfórum/PERSONALIS 2006. [předneseno 27.9.2006]. Praha (prezentace na konferenci).

V této kapitole uvedu v současnosti nejběžnější kybernetické útoky včetně jejich charakteristiky. Pokud jednotlivá jednání budou naplňovat znaky skutkové podstaty trestného činu, bude zde uvedeno, o jaký trestný čin jde.

1.1.HACKING

Pojem **„hacker“**[7] a **„hacking“** pochází z USA a vznikl v 50. letech 20. století a označoval technicky nadanou osobu (a její činnost) schopnou nalézat nová, mnohdy neortodoxní řešení problému.

Z hlediska obsahu této práce by bylo možné **hacking** charakterizovat jako **proniknutí do počítačového systému jiným než standardním způsobem, zpravidla obejitím či prolomením jeho bezpečnostního systému. Účelem takového jednání je pouhé dokázání si své schopnosti a intelektuální převahy bez toho, že by hacker měl zájem na zisku či zničení informací nacházejících se v systému samotném.**

Hackeři sami sebe označují za:[8]

„Člověka, vyžívajícího se v bádání po detailech programových systémů a překračování jejich schopností. Člověka, který má potěšení z detailní znalosti vnitřních pochodů systému, počítače a sítí. Experta na určitý program či experta v jiném oboru. Jako jedince užívajícího si intelektuální výzvy k překonání či obcházení limitů.“

7Tento pojem lze přeložit mnoha způsoby a je třeba vycházet z kontextu. V americkém žargonu to původně znamenalo bezcílně se projíždět na koni. Hack také označoval jednoduché řešení problému. Následně znamenalo spáchání nějaké nepravosti studenty univerzity.

8[cit. 13.3.2008]. Přeloženo z World Wide Web: <http://catb.org/jargon/html/index.html>

Především díky médiím a jejich neznalosti věci se však do podvědomí široké veřejnosti zapsal hacker jako osoba slídící a snažící se odhalit citlivé informace nebo prolamující kódy, či jako zloděj a vetřelec. Hackeři sami takového jedince označují jako **crackera**.[9]

Není pochyb o tom, že **ne každá aktivita hackerů je legální**. Ve vztahu k zásahu do počítačového systému jistě dojde k porušení ústavně zaručených základních lidských práv a svobod. Zejména se bude jednat o

lánek 7 odst. 1 [10] a **článek 13 LZPS.**[11] Obsah těchto dvou článků bude možné užít i u dále uvedených kybernetických útoků.

U hackingu však nastává problém v možnosti případného trestněprávního postihu výše uvedeného jednání. Nejproblematičtější je vymezení případné škody (neboť ji často není možné vyčíslit, zejména proto, že k žádné škodě nedošlo), či jiného následku a dále subsumpce jednání pod zákonné znaky některé ze skutkových podstat trestných činů.

Někteří z autorů uvádí možnost subsumpce jednání hackera pod ustanovení § 257a tr. zákona. Např. Jirovský uvádí:[12]

9Viz kap. 2.2

10„**Nedotknutelnost** osoby a jejího **soukromí je zaručena**. Omezena může být jen v případech stanovených zákonem.“

11„**Nikdo nesmí porušit** listovní tajemství ani **tajemství** jiných písemností a **záznamů**, **ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem**, s výjimkou případů a způsobem, které stanoví zákon. **Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.**“

„Skutková podstata § 257a TZ nevyžaduje ke svému naplnění, aby došlo k účinku, a postačuje, že pachatel jednal v úmyslu tento účinek způsobit. Skutková podstata tedy bude naplněna, jestliže pachatel získá přístup k nosiči informací ve shora uvedeném specifickém úmyslu. Jestliže k účinku nakonec nedojde, může to mít vliv na společenskou nebezpečnost trestného činu, avšak formálně bude trestný čin dokonán.“

S tímto tvrzením lze souhlasit pouze částečně, neboť postihuje ty případy, kdy hacker provede některé z jednání uvedených pod písmeny a) - c) citovaného ustanovení. Nejčastěji pak půjde o situaci, kdy dojde k změnění informací (např. vzhledu www stránek).

Nelze s ním však v žádném případě souhlasit v případě pouhého vniknutí hackera do systému bez motivu způsobení škody, jiné újmy či získání neoprávněného prospěchu.[13] Dále také bezpochyby nedojde k naplnění jednání uvedeného pod písmeny a) - c). Domnívám se, že v tomto případě **zákon neposkytuje dostatečnou ochranu před zde uvedeným jednáním**.

12Srov. JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha : Grada Publishing, a. s., 2007. s. 102.

13Jeho jediným cílem je překonání výzvy v podobě zabezpečení systému.

Ukázka hackerovy práce - pozměněné webové stránky Google

1.2.CRACKING

„C**racking**“[14] znamená prolamování nebo obcházení ochranných prvků systému, programů nebo aplikací, s cílem jejich následného neoprávněného užití. Jednou z forem je **„password cracking“** sloužící k zjišťování přístupového hesla do licencovaného systému či programu. Cracker zpravidla vytvoří keygen či crack, který umožní následné užití programu. Takto upravené programy jsou pak zpravidla sdíleny na warez fórech či P2P sítích. Cracker de facto zneužívá hackerských metod zpravidla k obohacení sebe sama.

Jednání pachatele, kdy dochází k prolamování ochrany systému či programu s úmyslem zisku informací a jejich následné neoprávněné užití naplňuje ustanovení § 257a tr. zákona. Při distribuci chráněného autorského díla pak dochází k naplnění ustanovení § 152 tr. zákona.

1.3.WAREZ

Velmi zjednodušeně řečeno **představuje warez novou formu softwarového pirátství**, kde informační technologie jsou pouze prostředkem pro urychlení šíření

14Z anglického **crack - lámat.**

nelegálních kopií autorských děl prostřednictvím Internetu. Domnívám se však, že by bylo vhodné problematiku warezu o něco více vysvětlit.

Warezová fóra v současnosti slouží zejména ke stahování cracků a keygenů, ale i kompletních upravených programů, filmů a hudby. Výsledný produkt warezové scény se nazývá **release**. Pro ochranu soukromí používají klienti warezových fór proxy servery a bouncery sloužící k maskování jeho IP adresy a tím znemožňující případné sledovaní. Vlastní komunikace a nabízení release probíhá v privátních místnostech, vytvořených k tomuto účelu na Internetu, kam mají přístup pouze členové skupiny.

Warez scény jsou zpravidla postaveny na principu **„nonprofit“**, uznávající tak jedno ze základních hackerských pravidel o **volném sdílení informací**. V rámci warezu se vytvářejí **skupiny** zaměřující se na různé oblasti (filmy, hry, aplikace, hudba, aj.), dělící si mezi sebe práci (leader, counsils, supplier, cracker, carder, tester, aj.) a stanovující pravidla pro provoz toho kterého warez fóra. V okamžiku, kdy takováto skupina vydá release, je tento zveřejněn na „topsites“, což jsou v hierarchii warezu elitní servery, určené pro omezený okruh lidí o diskové kapacitě několika TB. Z topsites jsou pomocí kurýrů data kopírovány na nižší stupně warezu. Zjednodušeně řečeno, za každý nově vložený release získává skupina určitý profit, ať již v možnostech vstupu či kapacitě stažitelných dat. Dochází tak k „obchodu“, při němž je jediným směnitelným artiklem informace, zejména informace nová.

Je pravdou, že současná nejrozšířenější forma sdílení a nabízení nelegálních kopií autorských děl pomocí P2P sítí by bez warezu nemohla existovat, neboť mezi běžnými uživateli nejsou osoby schopné takové cíleně zaměřené činnosti, jako je tomu právě ve warezových skupinách. Na druhou stranu, obrovská omezenost možnosti proniknutí do této komunity[15] podporuje právě masivní vznik a rozšiřování P2P sítí, jejichž prostřednictvím je nabízen největší obsah dat.

Poskytování souborů ať v rámci warezu či P2P sítě, lze postihnout dle ustanovení § 152, případně § 257a tr. zákona.

15Zejména ze strany warezových skupin, které se tak snaží chránit před odhalením orgány činnými v trestním řízení.

Ukázka P2P sítě - Megatorrent.cz[16]

16Zdroj: databáze autora

1.4.PHISHING

Phishing[17] je způsobem, jímž se dá prostřednictvím informačních a komunikačních technologií spáchat trestný čin podvodu. V češtině se slovo používá velmi často neupravené, případně se používá „počeštěná“ varianta ***rhybaření***, případně *rhybhaření, rhybolov, rhybholov*. Tento kalk je však poněkud umělý, anglická homofonie *ph↔f* v češtině protějšek nemá.[18]

U phishingu se pachatel snaží získat neoprávněný přístup k peněžnímu účtu finančního ústavu, platební kartě a následně z těchto zdrojů odčerpat dostupné finance. De facto dochází ke zcizení osobních údajů osoby vedených v digitální podobě. Útok jako takový nesměřuje vůči finanční instituci, ale přímo proti klientovi této instituce. Oběťmi pishingových útoků jsou ti klienti finančních ústavů, kteří díky neznalosti a lehkomyslnosti sdělí osobní údaje, aniž by respektovali zásady bezpečného pohybu na Internetu.

Útočník získá seznam klientů finanční instituce, na jejich osobní emaily pak rozešle zprávu (více či méně věrohodnou) nabádající je ke kontaktování klientského centra prostřednictvím interaktivního odkazu, který je součástí emailu. Jako záminka často slouží informace o chybě v bezpečnostním systému společnosti či jiné varování, které má vzbudit u klienta pocit autentičnosti této zprávy. Po aktivaci interaktivního odkazu je osoba přesměrována na webovou stránku, vytvořenou phisherem, věrně

---

17 Je několik teorií vysvětlujících vznik slova **phishing**. Uvádím tři z nich.
První z nich je, že jde o kombinaci slov **fishing** [rybaření či rybolov, což v tomto kontextu označuje rozesílání „návnady“ (e-mailových zpráv) v naději, že „se chytí“ některé oběti] a **phreaking** (jedná se o první hackerský útok na telefonní síť v USA).
Druhá uvádí, že písmena **ph** naznačují **specializovanost útoků pachatelů** phishingu (srov. LANCE, J. Phishing bez záhad. 1. vyd. Praha : Grada Publishing, a.s., 2007. s. 22).
Třetí teorie uvádí, že jde o zkratku slov *password harvesting fishing*“, což je do češtiny volně přeložitelné jako „rybolov sklízením hesel“ - [cit. 20.11.2006]. Dostupné na World Wide Web <http://www.honeynet.org/papers/phishing/>

18 [cit. 23.11.2007]. Dostupné na World Wide Web:
<http://encyklopedie.seznam.cz/heslo/484279-phishing>

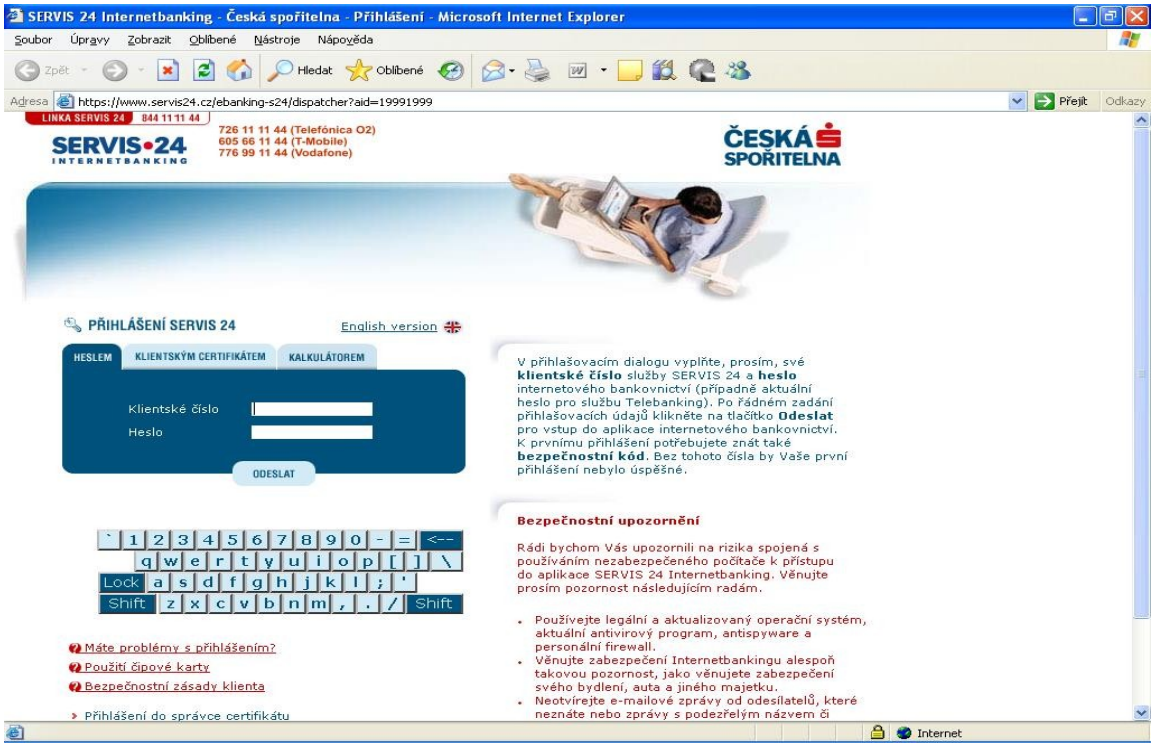
kopírující originální stránku finanční instituce. Klient je vyzván k vyplnění přihlašovacích údajů, zpravidla včetně čísla karty a PIN kódu. Vyplněné údaje jsou odeslány na adresu phishera, který následně odčerpá z účtu část či veškeré finanční prostředky a způsobí tím klientovi škodu (viz obrázek č. 10).

Obdobně funguje i **„maškaráda“** - tj. situace, kdy útočník přesměruje provoz z originální adresy na adresu vlastní, která se tváří věrohodně. Tím se snaží přesvědčit klienty finančních institucí o bezpečnosti prostředí. Následně je po nich, stejně jako v phishingu, žádáno vyplnění údajů o kartě a PIN kódu.

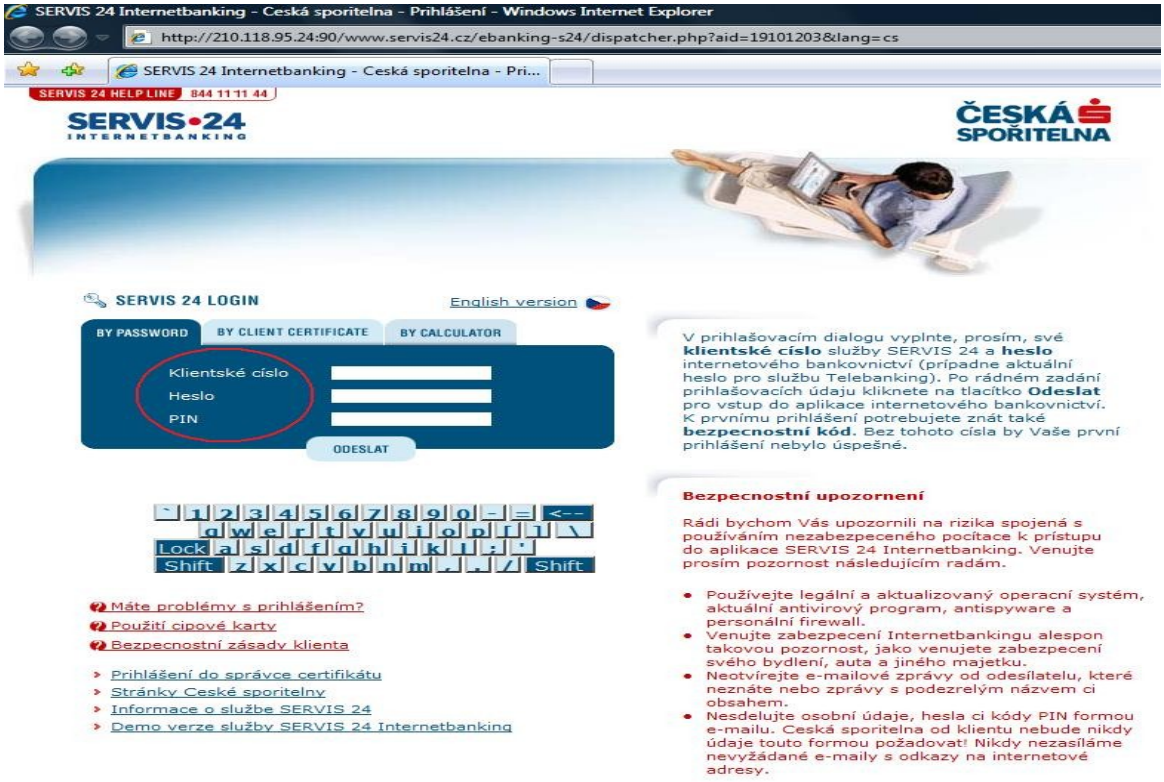
Phishingovým útokům jsou zejména vystaveny platební systémy umožňující elektronický převod peněz, jako jsou PayPal, PayPay, BidPay, MoneyBookers, Neteller, StrormPay či E-gold. V České republice pak nejčastěji dochází k útokům na účty klientů České spořitelny, a.s. Další podrobné informace o phishingu je možné získat na http://www.usdoj.gov/opa/report_on_phishing.pdf.

Z výše uvedeného lze dovodit, že phishing naplňuje skutkovou podstatu trestného činu podvodu dle ustanovení § 250 tr. zákona. Podvod je dokonán obohacením se. Vytvoření repliky webové stránky a získání přihlašovacích jmen a vstupních hesel, by pak bylo možné kvalifikovat jako přípravu či pokus trestného činu dle ustanovení § 250 tr. zákona. Samotné získání osobních údajů, včetně čísel účtů, čísel platebních karet a PIN kódů bez jejich dalšího užití pak nebude trestné.

Iniciační mail s interaktivním odkazem



Originální stránka České spořitelny a.s.



Stránka České spořitelny a.s. vytvořená Phisherem

Struktura Phiserské organizace a její fungování[19]

1.5.PHARMING

Pharming[20] je sofistikovanější a nebezpečnější formu phishingu. Jde o útok na DNS server, na kterém dochází k překladu doménového jména na IP adresu. K útoku dochází v momentu, kdy klient finančního ústavu zadá na internetovém prohlížeči adresu svého ústavu. Nedojde však k propojení na příslušnou IP adresu, ale na jinou, podvrženou. Webové stránky na falešné adrese zpravidla velmi věrně imitují originální stránky, de facto jsou od nich k nerozeznání. Uživatel následně zadá přihlašovací údaje, které získá útočník. Druhým způsobem pharmingu je napadení počítače koncového uživatele, kde se dá předpokládat menší míra zabezpečení. Pokud se podaří

19MUSTERMANN, M. Internetové mafii na stopě. In *Chip* 2008, roč. 18, č. 1, s. 158

20Jedná se o kombinaci slov **farming** (farmaření/hospodaření) a **phreaking**.

úspěšně počítač napadnout, stačí v něm upravit soubor Hosts obsahující URL a jim přiřazené IP adresy.

Tento způsob útoku je nyní na vzestupu. Svědčí o tom například zveřejněné případy, kdy útočníci přesměrovali návštěvníky serverů eBay či Google na podvržené stránky, kde následně došlo k pokusu o nainstalování spyware do počítačů návštěvníků.[21]

1.6.SNIFFING

Jedná se o metodu nelegálního zachytávání dat (volných packetů) procházejících sítí prostřednictvím tzv. **snifferu,**[22] který umožňuje monitorování a prohlížení si cizí komunikace. Sniffing je hrozbou díky tomu, že ve většině síťových spojení dochází k nešifrované komunikaci, což poskytuje útočníkům možnost „číst“ soukromá data vysílaná a přijímaná v rámci sítě. De facto by takovou činnost bylo možné označit jako **nelegální odposlech** či **záznam telekomunikačního provozu**.

Prakticky situace vypadá tak, že pokud uživatel pomocí prohlížeče zobrazí stránku, která je nešifrovaná[23], pak požadavek na cílový server i následná odpověď putují v čitelné podobě. Útočník tak má možnost zjistit informace, které jsou součástí komunikace mezi koncovým uživatelem a serverem. Může jít například o hesla, čísla kreditních karet, uživatelská jména a další citlivé informace. Útočník je tedy schopen odchytávat volné packety, čímž získá přístup

21Srov. World Wide Web: <http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/> [cit. 18.3.2008].

22**Sniffing** je anglické slovo znamenající - **čmuchat, čenichat**.Sniffer je pak možné přeložit jako čichač.

23Jichž je většina.

k veškeré komunikaci uživatele. Navíc díky zastaralosti běžně užívaných protokolů, které řádně nezabezpečují ochranu dat, má značně ulehčenou práci. Pro zajímavost lez uvést, že protokol FTP nenasazuje žádnou techniku šifrování přenosu stejně jako HTTP protokol. Šifrovaná verze je pak poskytována v rámci protokolu HTTPS,[24] který sice nezabrání odchytu volných packetů, ale díky šifrování znemožní přečtení si jejich obsahu. Protokol HTTPS využívají zejména finanční instituce k ochraně údajů sdělovaných jejich klienty. Jako příklad je možné uvést Českou spořitelnu a.s.:

https://www.servis24.cz/ebanking-s24/dispatcher?aid=19991999 .

Snifferem je možné sledovat například i komunikaci uskutečněnou přes program ICQ. Mimo „hackerů“ dochází k zneužití sniffingu i v rámci zaměstnání, kdy IT administrátoři[25] sledují činnost zaměstnanců např. pomocí tzv. keyloggerů[26] (programů, které „odposlouchávají“, co je psáno na klávesnici nebo který program byl spuštěn, jaká webovou stránka je otevírána apod.) či procházením e-mailových schránek zaměstnanců apod.

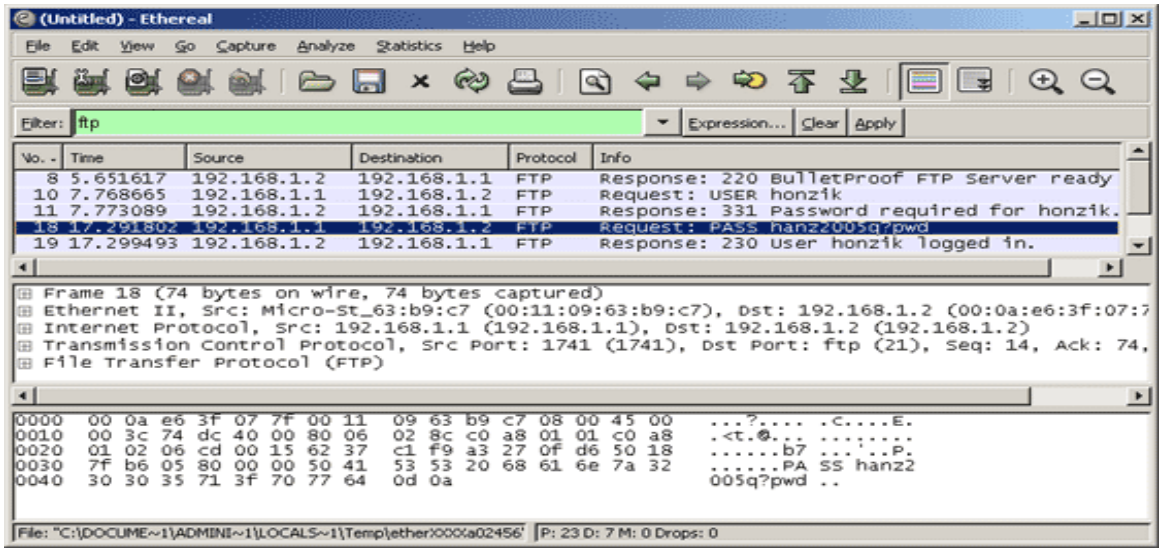
Uvedenou činností jistě dojde k zásahu do základních lidských práv a svobod, zejména se jedná o **čl. 13** LZPS, a je zcela lhostejné, zda sniffing provádí externí útočník, či administrátor sítě. Dle norem trestního práva by bylo možné takové jednání subsumovat pod

24Jedná se o šifrovanou SSL komunikaci.

25Srov. World Wide Web: <http://www.security-portal.cz/clanky/sniffing-v-rukou-spravce-site.html> [cit. 7.12.2007].

26Jde o programy, které „odposlouchávají“ (respektive zaznamenávají) veškerou činnost spojenou s užitím klávesnice.

ustanovení **§ 239** v tr. zákona a v případě zneužití takto získaných informací by se mohlo jednat o trestný čin dle ustanovení **§ 240** tr. zákona.



Sniffer. Modře vyznačené pole ukazuje odchycené heslo.[27]

1.7.SPAMMING

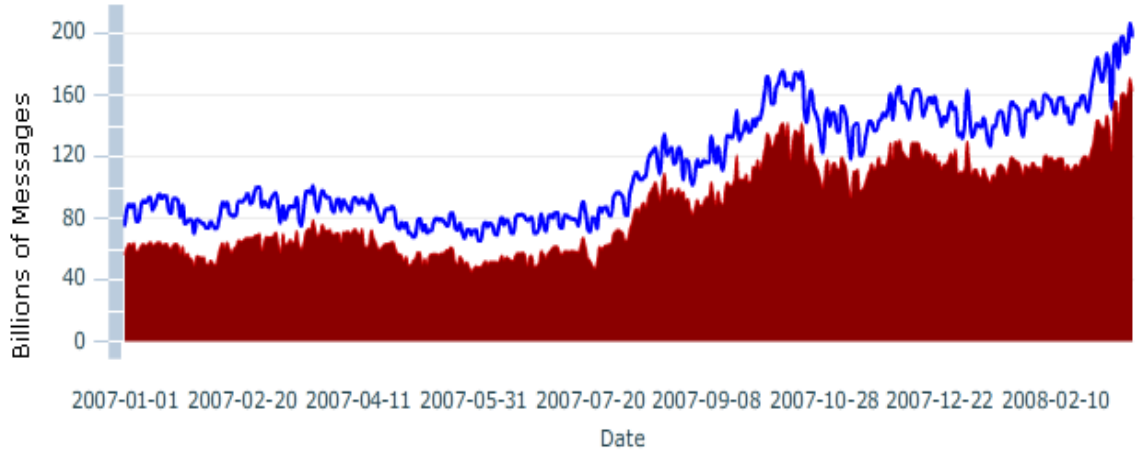
Spamming lze nejjednodušeji charakterizovat jako **zasílání nevyžádané elektronické pošty, zpravidla s reklamním obsahem.** Pojem SPAM pochází z názvu šunkových konzerv firmy Hormel foods nejvíce distribuovaných za 2. sv. války.[28] V rámci informačních sítí pak spam získal význam „plané řeči“ či „kecy“. V současnosti existuje velké množství statistik uvádějících různé počty spamů

27Zdroj: databáze autora

28Blíže World Wide Web: <http://www.hormelfoods.com/> [cit. 1.2.2008]. K pojmu samotnému.

v elektronických poštách. Jirovský například uvádí, že lze očekávat více jak 90 % podíl spamu v elektronické poště.[29]

Jiné statistiky uvádí, že průměrně v roce 2006 došlo k odeslání 12,5 miliardy spamových zpráv za den.[30] Díky tomu došlo i ke vzniku mnoha organizací zabývajících se spamem a poskytujících nástroje k ochraně před ním. Jednou z nich je TrustedSource[31], odkud pochází i následující graf znázorňující obsah spamu v elektronické poště za poslední rok. Modrá linie znázorňuje počet emailových zpráv a červené pole odráží počet spamů v emailové poště (obojí je uvedeno v miliardách).



Vývoj spamu za poslední rok

Spam zasahuje do elektronické komunikace, mnohdy ji zcela znemožní (dojde k zahlcení informační struktury) a snižuje tak důvěru společnosti v informační technologie. Pokud však dochází k omezování spamu, de facto dochází k omezování

29Srov. JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha : Grada Publishing, a. s., 2007. s. 104

30Srov. World Wide Web: <http://spam-filter-review.toptenreviews.com/spam-statistics.html> [cit. 10.6.2007].

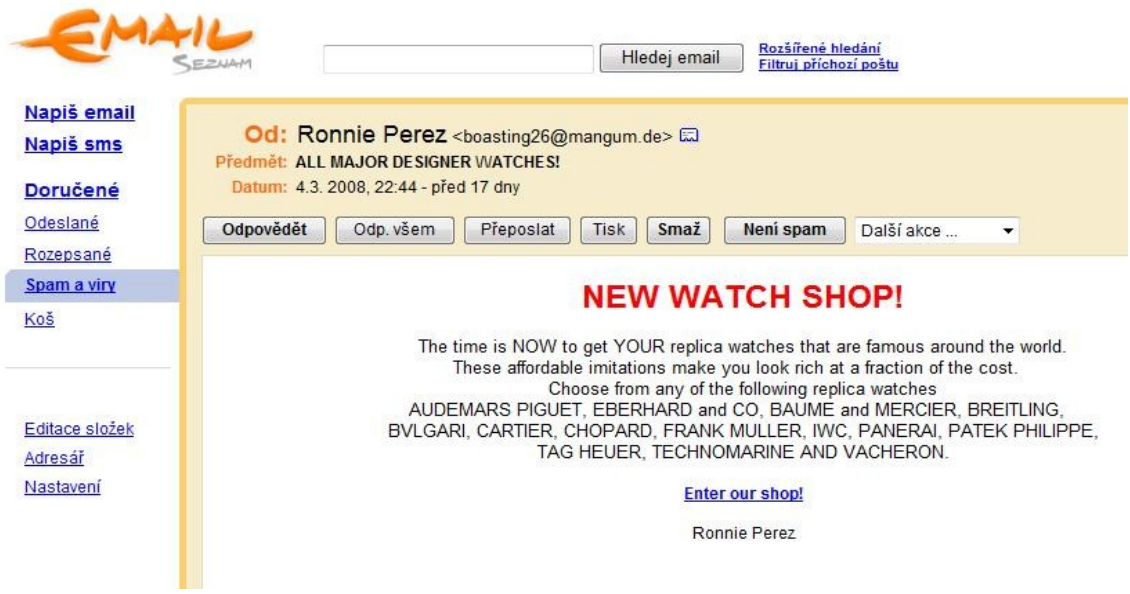
31Blíže World Wide Web: <http://www.trustedsource.org/TS?do=home> [cit. 21.3.2008].

práva na svobodu projevu (viz **čl. 17** LZPS) ve prospěch práva ochrany osobní integrity (viz **čl. 10 odst. 2** LZPS). I z tohoto důvodu je právní postih spamera značně komplikovaný a v současnosti dochází k využití institutů práva občanského a správního, neboť trestní právo neumožňuje potrestat spamera. Mimo trestní právo je možné postihnout spamera dle ustanovení § 120 odst. 1 písm. g) zák. č. 127/2005 Sb., kde se osoba dopustí přestupku, pokud užije adresu elektronické pošty pro odeslání zprávy, nebo zpráv. Regulaci spamu řeší i zákon č. 480/2004 Sb., který v ustanovení § 2 písm. f) charakterizuje, co se považuje za obchodní sdělení (spam je za ně považován - viz § 7 a násl. uvedeného zákona).

Trestněprávní postih spamu a spamerů v České republice je v současnosti neřešený. Absentuje jak vnitrostátní, tak i mezinárodněprávní ochrana před tímto nežádoucím jednáním. Ani Úmluva o kyberkriminalitě v sobě neobsahuje vymezení spamu jako trestného činu. V **USA** již však došlo k odsouzení spamera za rozesílání nevyžádané pošty. **Jeremy Jaynes** byl v roce 2007 odsouzen soudem ve Virginii k 9 ročnímu trestu odnětí svobody. Obviněn byl již v roce 2003, jako důkaz sloužilo 53 000 spamů odeslaných během tří dnů. Prokurátor však dle svého vyjádření věří, že Jaynes je odpovědný za rozesílání více jak 10.000.000 spamů denně, což mu mělo vynést přibližně 750.000 USD měsíčně.[32] Domnívám se, že by bylo vhodné i v rámci trestního práva České republiky posílit ochranu osobního soukromí před neoprávněnými průniky do něj.

32Blíže World Wide Web:

<http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm> [cit. 7.2.2008].



Ukázka spamu[33]

1.8.ŠÍŘENÍ IDEOLOGIE A MATERIÁLŮ SE ZÁVADNÝM OBSAHEM

V rámci tohoto jednání dochází k šíření materiálů obsahujících dětskou pornografii, zobrazující zoofilii, extremistické názory či jiné podobné materiály. Stejně jako u warezu se nejedená o nový druh protiprávního jednání, pouze zde informační a komunikační technologie umožňují masivní a značně latentní nárůst takového jednání. Pachatele by v těchto případech bylo možné postihnout například dle některého z uvedených ustanovení **§ 205, 205a, 198, 198a** a **§ 260 - 261a** tr. zákona.[34]

1.9. ZNEUŽITÍ INTERNETOVÝCH STRÁNEK

Díky nárůstu elektronické komunikace dochází mnohdy v prostředí Internetu k vytvoření či pozměnění webových stránek, jejichž obsah pak zasahuje do soukromí jiného. Příkladem může být uvedení nepravdivých informací o osobě, ale i prosté

33Zdroj: databáze autora

34Blíže viz příloha č. 4 a č. 6

zveřejnění kontaktu a fotografie (podvržené) na stránkách erotické seznamky. Z hlediska trestního práva jsou pak v prostředí Internetu v tomto případě nejčastěji naplněny znaky skutkové podstaty trestného činu dle ustanovení **§ 206** tr. zákona. Jelikož je však čin proveden prostřednictvím Internetu, bude se jednat i o kvalifikovanou skutkovou podstatu uvedeného trestného činu, neboť bude naplněn i znak spáchání činu *jiným obdobným způsobem*.

Z praxe je možné uvést případ, kdy pod jménem kandidátky do obecního zastupitelstva byly vytvořeny internetové stránky s nabídkou erotických služeb, včetně uvedení jejího mobilního telefonu a erotických fotek (ty byly výtvorem fotomontáže). Popsané jednání mělo vliv na výsledek voleb a zasáhlo i kandidátčin osobní život. Využívání webových stránek k šíření pomluvy je v současnosti stále častější, například Policie v rámci správy hl. města Prahy řešila v roce 2007 sedm trestních oznámení, kdy došlo ke zneužití webové stránky právě k šíření pomluvy.

1.10.KYBERNETICKÉ VÝPALNÉ (RACKETEERING)

Podstatou uvedeného jednání je **vyvolání strachu z možné penetrace systému, zničení, odcizení dat a poškození hardwaru**. Opět se jedná o klasický trestný čin, avšak páchaný novými prostředky, kdy nedochází k fyzickému kontaktu s obětí. Tím se čin stává hůře zjistitelným a odhalitelným. V současnosti tuto formu začíná stále více využívat organizovaný zločin. Vyděrač v mnohých případech využívá pouhé neznalosti koncového uživatele. Uvedené jednání je bezpochyby možné postihnout dle ustanovení **§ 235**, případně dle **§ 257a** tr. zákona.

1.11.CYBERSQUATTING

Squatting znamená nelegální obsazení určitého prostoru, v tomto případě určitého doménového jména. Pachatel si zaregistruje doménové jméno, jehož součástí je název některého známého produktu či instituce, např.: www.ministerstvodopravy.eu či www.zeletava.eu. Zpravidla pak dojde k nabídce ze strany zaregistrovatele, aby si subjekt, jehož se doména dotýká, odkoupil doménové jméno za úplatu s tím, že pokud tak neučiní, bude na uvedených stránkách zobrazena pornografie. V poslední době

dochází právě k zaregistrování zatím neregistrovaných doménových jmen ze strany různých spekulantů.

Tímto jednáním se však pachatel vystavuje možnosti případného trestněprávního postihu dle ustanovení **§ 149, 150** tr. zákona.

Právě velké množství problémů souvisejících se spory o doménová jména vedlo v roce 2004 k vydání pravidel k registraci doménových jmen v doméně **.CZ**. Uvedená pravidla vydalo sdružení CZ NIC (www.nic.cz). Spory týkající se doménových jmen jsou pak řešeny Rozhodčím soudem při Hospodářské komoře ČR a Agrární komoře ČR.

1.12.KYBERTERORISMUS

V souvislosti s kybernetickými útoky nelze opomenout problematiku terorismu. Představuje jednu z nejaktuálnějších forem globálních hrozeb a lze sledovat jeho dynamický nárůst a rozšiřování do celého světa.

Terorismus můžeme rozdělit podle formy na *letální* a *neletální* formy terorismu, kde první skupina se vyznačuje použitím běžných prostředků pro realizaci násilí (*konvenční* – útoky páchané pomocí běžně dostupných bojových prostředků, např. střelných zbraní a *nekonvenční* – zneužití zbraní hromadného ničení). V oblasti Internetu jsou však **běžnější neletální formy terorismu** nebo útoky, při kterých jsou využívány moderní nástroje v kombinaci s letálními prostředky.

Konvenční forma neletálního terorismu zahrnuje níže uvedené podskupiny:

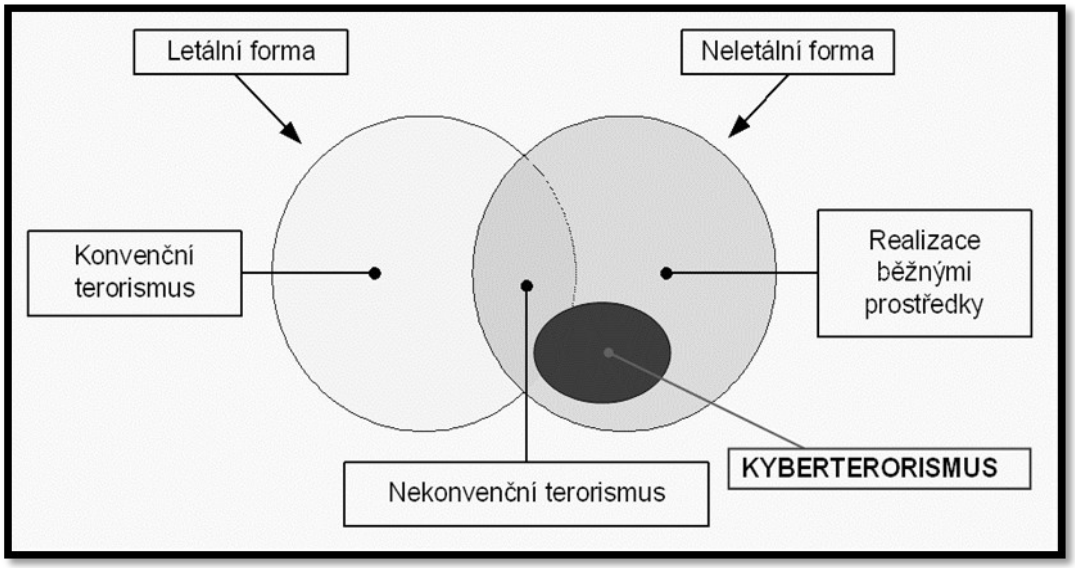
- *Neozbrojený terorismus*.

- *Kyberterorismus*, který patří mezi největší nebezpečí 21. století. Principem je především zneužívání výpočetní a telekomunikační techniky včetně Internetu jako prostředku a prostředí pro uskutečnění útoku. Jedná se, podobně jako u klasického konvenčního teroristického útoku, o plánovanou činnost motivovanou zpravidla politicky či nábožensky a realizovanou spíše malými, ne vojensky organizovanými strukturami. Cílem těchto skupin je především ovlivnění veřejného mínění. Vzhledem k rychlému šíření informačních a komunikačních technologií po celém světě

představuje kyberterorismus významné nebezpečí a je teroristickými skupinami využíván ve stále rostoucí míře.[35]

- *Mediální terorismus*, při němž dochází k plánovanému zneužívání hromadných sdělovacích prostředků a jiných psychologických prostředků za účelem ovlivnění názorů celé populace, nebo cílových skupin obyvatelstva.

Nejvýstižněji tento vztah charakterizuje schéma uvedené na obrázku č. 14.



[36]

Znázornění kyberterorismu

Globální charakter informatického a telekomunikačního prostředí umožňuje předávání informací a koordinaci teroristických aktivit v rámci celého světa. Uvádí se, že např. útok na WTC v New Yorku byl organizován právě s využitím Internetu.

Je možno uvést i další případy zneužití Internetu pro šíření závadných informací nebo pro psychologické operace související s mediálním terorismem. Internet poskytuje zcela výjimečné možnosti extremistickým a teroristickým skupinám i

35 JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha : Grada Publishing, a. s., 2007. s. 129

36 Srov: JIROVSKÝ, V. Kyberterorismus. ICTfórum/PERSONALIS 2006. [předneseno 27.9.2006]. Praha (prezentace na konferenci).

jednotlivcům, a to zejména v oblasti rychlé a relativně utajené komunikace, kdy slouží ke vzájemné výměně informací a pokynů k plánování a koordinaci akcí nebo převodu finančních prostředků. Internet se podstatnou měrou podílí na šíření propagandy, získávání a mobilizaci nových aktivistů, sympatizantů či sponzorů, obhajobě teroristických činů a podněcování jednotlivců k jejich páchání. Internetové servery teroristických skupin často obsahují návody na výrobu improvizovaných zbraní, nebo propagandu zacílenou na mladší generaci.

Bezmála všechny teroristické skupiny a organizace provozují své internetové stránky. Obvykle jsou zveřejňovány v několika jazykových mutacích a nechybí ani speciální stránky zaměřené na děti a ženy obsahující pohádky či komiksy, do nichž jsou zapracovány například příběhy sebevražedných atentátníků.[37]

Z hlediska trestního práva pak uvedené jednání může naplňovat skutkové podstaty trestných činů dle ustanovení **§ 95 odst. 2, § 198, 198a, § 260 - 261a tr. zákona.**

Existují i další protiprávní jednání, které je možné označit jako kybernetické útoky.

37JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha : Grada Publishing, a. s., 2007. s. 138