UNIVERZITA KARLOVA V PRAZE
FAKULTA SOCIÁLNÍCH VĚD

Institut sociologických studií

„Češky a Češi v kyberprostoru“: Zpráva výzkumného týmu sociologie a psychologie v rámci projektu bezpečnostního výzkumu „Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky“

PRAHA 2008: ZESTRUČNĚNÉ VÝSLEDKY VÝZKUMU

Zpráva sumarizuje výsledky několika výzkumů (dílem provedených výzkumným týmem, dílem převzatých). Jedná se o několik velkých kvantitativních šetření zejména čtyři vlny výzkumu v rámci projektu World Internet Project (2005-2008) a 3 samostatná šetření kvalitativní povahy, zaměřená na určité specifické cílové skupiny (jejichž povaha byla, s ohledem na následně provedené velké kvantitativní šetření World Internet Project 2008, spíše přípravná). Konkrétně byly prováděny hloubkové rozhovory s nezletilými, s odborníky v oblasti informačních a komunikačních technologií (zaměřené na bezpečnostní otázky) a skupinové diskuse s osobami, které neužívají Internet. Kapitoly zprávy jsou následující:

- **Kapitola I: Úvod**
- **Kapitola II: Zpracování základních výsledků z kvantitativních šetření populace České republiky v rámci projektu World Internet Project 2005-2008**. Pozornost je věnována popisu internetové populace, její typologii a službám, které lidé na Internetu využívají. Analýza zaměřená na bezpečnost na Internetu vychází z doplňku výzkumu provedeného v roce 2008.
- **Kapitola III: Mezinárodní srovnání užívání Internetu a jeho služeb** (s využitím mezinárodních dat z projektu World Internet Project 2007).
- **Kapitola IV: Dvě šetření zaměřená na mládež**. Konkrétně se jedná o šetření „Pocit bezpečí“ provedené Institutem sociologických studií a doplňkově též mezinárodní kriminologické šetření „ISRD2“ z roku 2006, zaměřené na kriminalitu mládeže. Obě šetření slouží spíše pro doplnění obrazu mládeže v České republice s ohledem na informační kriminalitu a bezpečnostní aspekty Internetu.
- **Kapitola V.: Shrnutí výsledků výzkumu zaměřeného na uživatele Internetu ve věku 11-19 let týkající se zejména bezpečnostních aspektů Internetu** (jednalo se o 12 hloubkových rozhovorů o délce cca 1 hodiny) s uživateli různého věku, různého typu navštěvované školy a různé intenzity užívání Internetu. Výsledky těchto rozhovorů byly využity pro návrh dotazníku kvantitativního šetření v roce 2008 (součást Word Internet Project 2008 v rámci České republiky).
- **Kapitola VI.: Výsledky skupinových diskusí s osobami, které Internet, případně mobilní telefon, GSM či internetové bankovnictví téměř či vůbec neužívají.** Tato skupina je velmi specifická a doposud ji byla ve výzkumech World Internet Project věnována jen okrajová pozornost. Za pomoci agentury NMS byly provedeny 3 skupinové diskuse o délce cca 90 minut.
- **Kapitola VII.: Výsledky hloubkových rozhovorů s odborníky na problematiku informačních a komunikačních technologií, zaměřených na bezpečnostní otázky** (12 hloubkových rozhovorů o délce cca 1 hodiny, s odborníky pracujícími v bankovních službách, u mobilních operátorů, případně spravujícími velké počítačové systémy – universitní, fakultní atd.).
- **Kapitola VIII.: Výsledky bezpečnostní studie z června 2008 z firemního prostředí v České republice.** Studie shrnuje výsledky pro cca 2 000 firem o různé velikosti a oboru (s ohledem na informační bezpečnost). Pasáž tak tvoří jakýsi doplněk obrazu běžné populace a umožňuje nalezení slabých míst v oblasti informační bezpečnosti v rámci celé České republiky.
- **Kapitola IX.: Zaměření budoucna a výhled dalších aktivit** týmu sociologie a psychologie, (včetně výstupů, které je od týmu možné očekávat).
- **Příloha:** Její text obsahuje zejména materiály použité k popisovaným výzkumům (tedy zejména dotazníky a scénáře jednotlivých výzkumných projektů).

Cílové skupiny výzkumů

Pro větší pochopení výzkumné strategie týmu je třeba uvést, na jaké skupiny populace se výzkum soustředí. Celkové směřování výzkumných snah chce (zejména v první fázi) popsat celou populaci a její vztah ke kyberprostoru. Nicméně některé skupiny zaslouží podrobnější pozornost:

a) **Mladí lidé (cca do 30 let) užívající Internet.** Tato skupina uživatelů je specifická v tom smyslu, že začala moderní technologie (počítače, Internet, mobilní telefony) používat naprosto samozřejmě a to od nejútlejšího věku. Jejich socializace byla tedy poprvé výrazněji ovlivněna kyberprostorem, o němž zejména jejich rodiče a učitelé často nevědí tolik jako oni. Je proto důležité znát hodnotové orientace těchto osob, problémové prvky při jejich začleňování do (informační) společnosti a potenciální rizika, spojená s jejich pohybem v kyberprostoru.
b) **Neuživatelé či lidé, kteří užívají moderní technologie minimálně.** Tyto osoby jsou spíše starší, z nejrůznějších důvodů nevyužívají technické novinky a kyberprostor je pro ně často velkou neznámou. S ohledem na to, že se často jedná o rodiče osob, které moderními technologiemi žijí, respektive o osoby, které se mohou snadno stát oběťmi trestného jednání v kyberprostoru, je třeba věnovat této skupině pozornost.
c) **Specialisté na informační a komunikační technologie.** Ti se aktivně podílejí na utváření kyberprostoru. Setkávají se každý den (každý okamžik) s jeho nástrahami. Pohled těchto osob je přínosný zejména pro nastavení bezpečnostního standardu pro soukromé i firemní uživatele a také pro prognózování dalšího vývoje v kyberprostoru.
d) **Lidé, páchající závadné jednání v kyberprostoru.** Tyto osoby se z nejrůznějších důvodů pokouší, resp. úspěšně provádějí různé útoky v kyberprostoru. Cílem projektu v roce 2009 je pokusit se vytvořit sociálně-psychologický profil těchto osob (doplňkově bude pozornost zaměřena též na osoby ve výkonu trestu, odsouzené za informační kriminalitu).

V této zprávě jsou obsaženy výsledky zkoumání pro cílové skupiny a) a b) a c), skupina uvedená pod písmenem d) bude zkoumána v roce 2009 (resp. výzkum již probíhá).

Přehled členů týmu sociologie a psychologie.

Část sociologie:

- Bc. Martin Buchtík, student Fakulty sociálních věd University Karlovy, obor sociologie.
- Mgr. Petr Lupač, katedra sociologie Filosofická fakulta University Karlovy.
- Bc. Petra Nováková, studentka Fakulty sociálních věd University Karlovy, obor sociologie.
- PhDr. Natálie Simonová, Sociologický ústav Akademie věd České republiky, v. v. i.
- Mgr. Jan Sládek, katedra sociologie Filosofická fakulta University Karlovy.

Část psychologie:

- Doc. PhDr. et Mgr. David Šmahel, Ph.D., Institut výzkumu dětí, mládeže a rodiny, Fakulta sociálních studií Masarykovy university.
- Mgr. Štěpán Konečný, Institut výzkumu dětí, mládeže a rodiny, Fakulta sociálních studií Masarykovy university.

Koordinace:

- Petr Soukup (spolupříjemce za Fakultu sociálních věd University Karlovy), katedra sociologie Fakulty sociálních věd University Karlovy.

Základní informace o populaci kyberprostoru v České republice

- Česká republika byla k síti Internet připojena roku 1993.
- Procento uživatelů Internetu v České republice stále narůstá, v roce 2005 bylo v populaci starší 11 let 50 % uživatelů Internetu, v roce 2008 již dokonce 57 %.
- V České republice je tak dnes (2008) zhruba 5,3 milionu uživatelů Internetu ve věku 12 let a více.
- Neuživatelé Internetu jsou často lidé starší s nižším vzděláním, skeptičtější k možnostem využití Internetu jakožto důvěryhodného zdroje informací (ve srovnání s uživateli Internetu). Uživateli Internetu jsou častěji mladší lidé.
- Šedesát procent respondentů odpovědělo, že vlastní alespoň jeden počítač. Čtvrtina respondentů uvedla, že vlastní alespoň jeden notebook.
- Vlastnictví alespoň jednoho počítače na osobu v domácnosti uvedla desetina respondentů. Čím déle a intenzivněji osoba používá Internet, tím pravděpodobnější je, že v její domácnosti bude alespoň jeden notebook. Výrazně nižší šance vlastnit alespoň jeden počítač je u respondentů starších 46 let.
- To, kdo se v domácnosti stará o počítač, souvisí jednak s kombinací intenzity a délky užívání Internetu, jednak – což s tímto faktorem rovněž koreluje – s věkem. Výrazně častěji (ve srovnání se zbytkem populace) se o počítač v domácnosti starají zkušení uživatelé a uživatelé ve věku 19-30 let.
- Vždy nebo většinou se o počítač v domácnosti stará 35 % respondentů ve věku 12-18 let.

Prvním výzkumem, na základě kterého vznikla tato zpráva, je **World Internet Project** (dále jen **WIP**). Cílem tohoto projektu je provádění opakovaných studií, zabývajících se vlivem počítačů, Internetu a příbuzných technologií na jedince, rodinu a společnost v celosvětovém měřítku. V České republice se výzkum provádí každoročně od roku 2005 a je financován z grantu Ministerstva školství, mládeže a tělovýchovy „Světový projekt o Internetu – Česká republika“ (1P05ME751) v rámci projektů mezinárodní spolupráce. Projekt realizuje Fakulta sociálních studií Masarykovy university v Brně, řešitelem projektu je Doc. PhDr. David Šmahel, Ph.D. (smahel@fss.muni.cz). Cíle projektu WIP jsou v České republice následující:

- zjištění míry využívání informačních technologií a Internetu, včetně mezinárodního srovnání v tomto ohledu;
- měření různých psycho-sociálních charakteristik uživatelů Internetu;
- hledání odpovědí na otázky, proč a jakým způsobem lidé Internet využívají;
- proč někteří lidé naopak Internet nevyužívají, jaké jsou důvody nedostupnosti Internetu;
- analýza problému vlivu Internetu na život jedince a jeho sociální chování.

První výzkum v České republice byl proveden agenturou STEM v září 2005 (formou osobních rozhovorů). Výzkumu se zúčastnilo 1 831 respondentů ve věku 12 let a starších. Výzkumný vzorek byl reprezentativní pro Českou republiku s ohledem na pohlaví, vzdělání, věk, region a velikost místa bydliště respondenta. V dalších letech (2006 a 2007) byl výzkum opět proveden agenturou STEM se stejnou metodologií. Velikost výběrových souborů činila 1 706, resp. 1 586 osob starších 11 let.

Vzhledem k tomu, že toto reprezentativní šetření obyvatelstva České republiky zaměřené na Internet je hrazeno z veřejných prostředků, a respondenti jsou navíc zachyceni již od 12 let věku,[1] rozhodl se řešitelský tým navázat spolupráci s tímto projektem a využít výše popsaná data ze šetření z let 2005 - 2007.

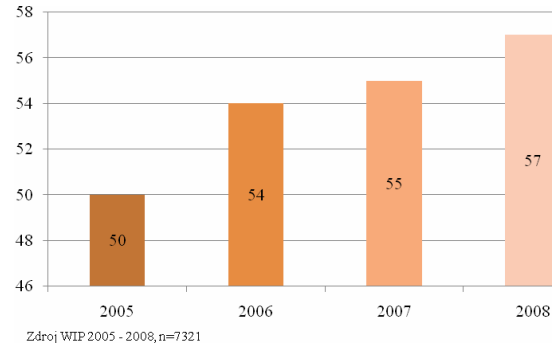
[1] Běžně prováděné výzkumy se zaměřují na populaci dospělou, případně populaci ve věku od 15 let. Osoby mladší jsou zkoumány zpravidla samostatně ve speciálních studiích.

Zjištění č. 1: Uživatelé Internetu: Rozdíly na základě věku, vzdělání i majetku

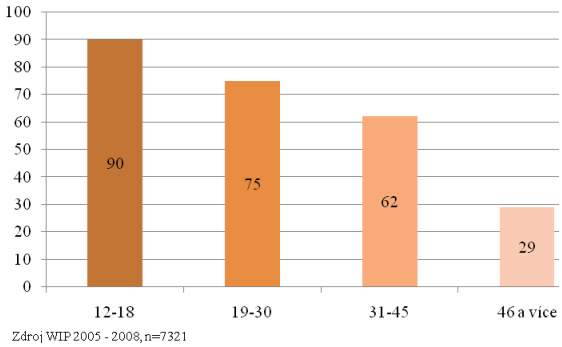
Používání Internetu není nikde na světě rozděleno v populaci rovnoměrně. Tato nerovnost je nazývána „digital divide“ a patří dnes ke standardním oblastem sociálního výzkumu. Jednou z hlavních proměnných je v tomto ohledu věk. Graf II.2 ukazuje procento uživatelů v jednotlivých věkových kategoriích během let 2005 až 2008. Mezi nejmladšími lidmi je uživatelem Internetu devět z desíti dotázaných. Oproti tomu v kategorii 46 let a více nepatří mezi uživatele ani jedna třetina dotázaných. Platí tedy, že s vyšším věkem procento uživatelů klesá.

Věk však není jediným faktorem, který používání Internetu ovlivňuje, byť většina ostatních faktorů s ním souvisí. Jeden z největších rozdílů je v tomto ohledu způsoben vzděláním: obzvlášť patrný je mezi středoškoláky s maturitou a středoškoláky bez maturity. Mezi prvně jmenovanými se nachází 70 % uživatelů Internetu, oproti 35 % u druhé skupiny.

Graf II.1:
Podíl odpovědí na otázku „Používáte Vy osobně Internet, to jest www stránky, e-mail nebo kteroukoliv jinou část Internetu, z domova nebo z kteréhokoliv jiného místa?“ (v %)



Graf II.2:
Podíl uživatelů Internetu v jednotlivých věkových kategoriích (v %)



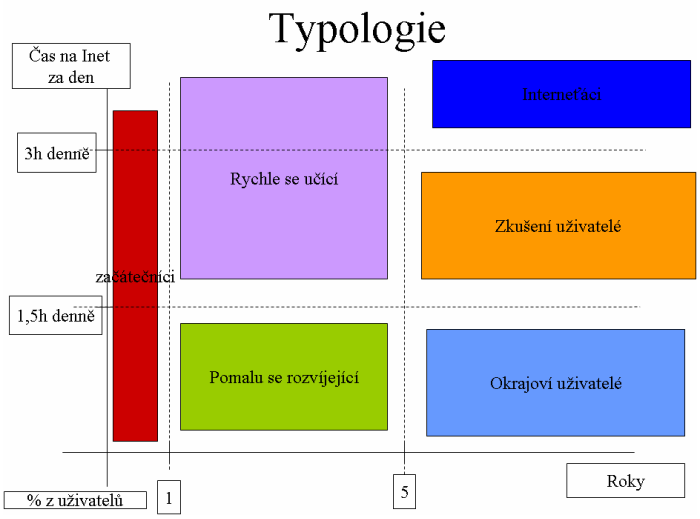
Dalším faktorem nerovnosti v možnosti užívat Internet je materiální zajištění. Výzkum pracuje s pěti skupinami respondentů podle velikosti jejich příjmu a majetku[2]. Střední skupina, „průměrně zajištění“, vykazuje podíl uživatelů Internetu 60 %, což je mírně nad průměrem České republiky. **Ve skupinách „velmi“ a „solidně“ zajištěni patří mezi uživatele 80 % jedinců, zatímco mezi nejchudšími se nachází pouze 18 % uživatelů Internetu.** Mezi krajními skupinami (z hlediska jejich materiálního postavení) existuje tedy více než čtyřnásobný rozdíl.

Sledovanou proměnnou je i způsob připojení na Internet z domova (graf II.8). Pokud se jedná o celková čísla za roky 2007 a 2008, pak **dominantní variantou je vysokorychlostní připojení**. V roce 2007 bylo takto připojeno 67 % respondentů, o rok později pak 75 %. Druhým nejčastěji uvedeným způsobem byla „běžná telefonní linka“, kterou v roce 2007 užívalo 24 % dotázaných, o rok později pak o něco méně (17 %). Přes mobilní telefon se během obou let připojovalo okolo 3-4 % dotázaných.

[2] Respondenti odpovídali na otázku, jaké je zajištění jejich domácnosti z hlediska příjmů a majetku. Mohli přitom odpovědět: velmi dobře zajištěni, solidně zajištěni, průměrně zajištěni, špatně zajištěni a v zásadě chudí. Jedná se tedy o subjektivní sebezařazení respondentů.

Zjištění č. 2: Výrazně odlišné subkultury

Skupina uživatelů Internetu v České republice je poměrně nestejnorodá. Proto došlo v rámci výzkumu k její typologizaci, která je založena na délce užívání Internetu (v letech, zachycených na ose x v následujícím schématu) a počtu hodin strávených na Internetu (v hodinách za den, zachycených na ose y). Na základě těchto dvou dimenzí došlo k identifikaci šesti typů uživatelů Internetu v České republice (**Schéma II.1).**



Jednotlivé typy byly pojmenovány tak, aby sám jejich název získal co možná největší vypovídací hodnotu (Začátečníci, Okrajoví uživatelé, Pomalu se rozvíjející uživatelé, Rychle se učící uživatelé, Zkušení uživatelé a tzv. Internetáci). Nejkratší dobu na Internetu tedy zatím tráví tzv. **Začátečníci**, jsou připojeni maximálně jeden rok. Naopak **Okrajoví uživatelé, Zkušení uživatelé a Internetáci** pracují s Internetem již 5 let a déle. Mezi sebou se pak liší intenzitou jeho využívání. Ta je nejmenší u Okrajových uživatelů (do 1,5 hodiny denně), o něco vyšší u Zkušených (mezi 1,5 hodinou a 3 hodinami denně) a nejvyšší u tzv. Internetáků. Mezi těmito skupinami se nachází **Pomalu se rozvíjející a Rychle se učící uživatelé**, tedy lidé, kteří používají Internet déle než rok (ale ne více než 5 let). Tyto dva typy se mezi sebou opět liší intenzitou užívání (Pomalu se rozvíjející na Internetu tráví do 1,5 hodiny denně, Rychle se učící pak více než 1,5 hodiny).

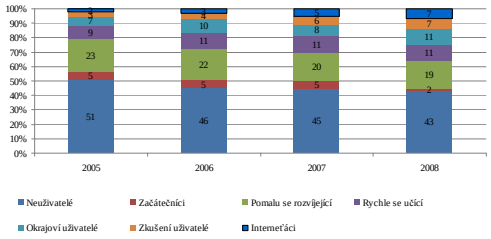
Tabulka II.1: *Podíly výskytu jednotlivých typů internetových uživatelů v České republice (internetová populace starší 11 let):*

Typ:	Podíl na všech uživatelích Internetu	Odhad absolutního počtu osob
Začátečníci	4 %	230 000
Pomalu se rozvíjející	34 %	1 750 000
Rychle se učící	19 %	1 030 000
Okrajoví uživatelé	19 %	1 030 000
Zkušení uživatelé	12 %	630 000
Internetáci	12 %	630 000
Celkem	100 %	5 300 000

Zdroj: WIP 2008, n = 1251

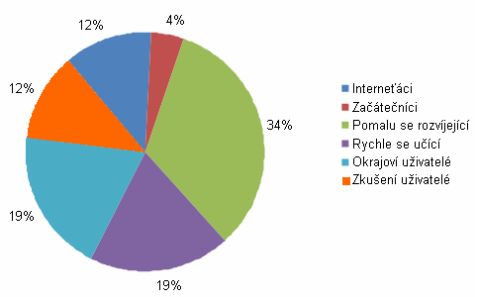
Z grafu II.4 je zřejmé, že narůstá nejen podíl uživatelů Internetu, ale proměňuje se i jejich struktura. Přibývá osob, které užívají Internet více let a také tráví na Internetu více času (nejmarkantnější je nárůst výskytu typů označených jako Internetáci a Zkušení uživatelé.

Graf II.4: *Vývoj podílu jednotlivých typů uživatelů a neuživatelů Internetu v České republice v letech 2005-2008 (populace starší 11 let)*



Zdroj: WIP 2005-2008, n = 7334

Graf II.5: *Proporce jednotlivých typů uživatelů Internetu v České republice (jen uživatelé Internetu – v roce 2008)*



Zdroj: WIP 2008, n = 1251

Sociodemografickou odlišnost jednotlivých typů uživatelů (rozdíly dle věku, vzdělání, pohlaví či velikosti místa bydliště) přibližuje **Tabulka II.2** (populace starší 11 let):

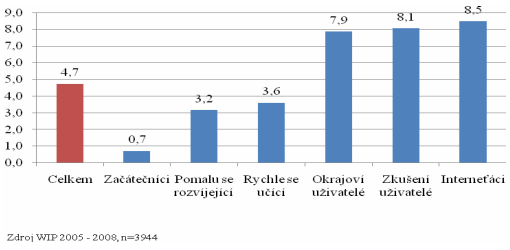
Charakteristiky a jejich kategorie		Začátečníci	Pomalu se rozvíjející	Rychle se učící	Okrajoví	Zkušení	Interneťáci
Věk	průměr	32	34	30	38	33	34
Věkové kategorie	12-18	43	20	34	5	7	6
	19-30	18	25	27	33	42	43
	31-45	20	29	19	30	32	31
	46 a více	19	26	20	32	20	19
Vzdělání	základní	40	25	35	8	10	7
	SŠ bez maturity	27	35	20	22	19	15
	SŠ s maturitou	29	36	33	51	48	53
	VŠ, VOŠ	4	4	13	19	23	25
Pohlaví	muž	41	48	50	49	55	53
	žena	59	52	50	51	45	47
Počet obyvatel obce	do 1 000	20	13	12	15	13	16
	1 000 – 2 000	12	12	8	7	10	1
	2 000 – 5 000	8	12	8	11	6	9
	5 000 – 20 000	8	17	20	14	16	21
	20 000 – 90 000	19	22	23	22	19	18
	nad 90 000	33	24	30	31	35	33

Poznámka: Údaje (s výjimkou průměrného věku) jsou sloupcovými procenty[3]. Zdroj: WIP 2008, n = 2210

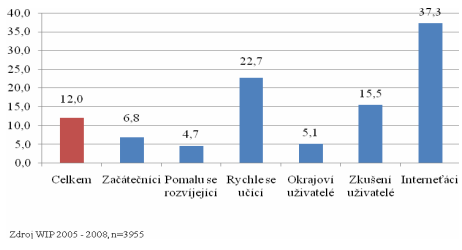
Také struktura z hlediska pohlaví je odlišná. Zatímco mezi neuživateli převažují ženy (52 %), mezi Interneťáky převažují muži (53 %). Z hlediska velikosti obce pak platí, že více uživatelů Internetu se nachází ve větších obcích a vice versa.

Průměrnou dobou strávenou on-line je pro všechny uživatele (zkoumané v letech 2005 až 2008) 12 hodin týdně. Rychle se učící uživatelé tráví na Internetu bezmála 23 hodin týdně, zatímco **Interneťáci se blíží 38 hodinám**. **Zkušení uživatelé tráví týdně na Internetu bezmála 16 hodin, což lze přirovnat ke dvěma pracovním dnům.** Ostatní skupiny se pohybují mezi pěti až sedmi hodinami týdně (tedy zhruba jedna hodinu denně). Intenzita užívání Internetu v celé populaci roste: v roce 2005 činila 10,3 hodiny týdně, o tři roky později to bylo 13,2 hodiny.

Graf II.6: *Délka užívání Internetu (roky)*



Graf II.7: *Délka užívání Internetu za týden (hodiny)*



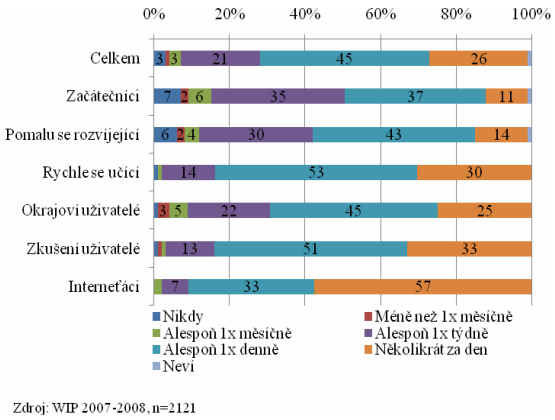
[3] Součet procent ve všech kategoriích příslušné proměnné je 100.

Zjištění č. 3: Jakým činnostem se veřejnost na Internetu věnuje?

Zjišťovány byly způsoby a frekvence používání Internetu jako zdroje informací, ale také navštěvování Internetu za účelem zábavy či seznámení. Každá aktivita je spojena s různou mírou rizika, ale také se jí často dominantně věnují jen některé skupiny. Cílem studie bylo na tyto skupiny poukázat a porovnat je s ohledem na on-line aktivity skupin ostatních. Z hlediska rizikového chování či informační kriminality byla pozornost věnována také **navštěvování erotických stránek, stahování dat, zkušenosti s internetovou seznamkou nebo s nakupováním on-line.**

Výzkum WIP rovněž ukázal, že jednoznačně nejpoužívanějším komunikačním kanálem, a to bez ohledu na věk, pohlaví či uživatelský typ, je e-mail. Pokud se jedná o spíše mladší respondenty, ti výrazně častěji používají programy jako ICQ či MSN a patří mezi časté návštěvníky chatovacích místností. Obecně více elektronicky komunikují dlouhodobější uživatelé; tato skupina také více používá telefonování přes Internet.

Je zřejmé, že ke zcela základním činnostem na Internetu patří komunikace, tedy přinejmenším kontrola e-mailu. Pouze mezi Začátečníky a Pomalu se rozvíjejícími lze najít uživatele, kteří tuto zkušenost zatím postrádají. Pokud se jedná o frekvenci kontroly e-mailu, devět z deseti Interneťáků nahlíží do své e-mailové schránky alespoň jednou denně. Varianta „alespoň jednou denně“ je téměř u všech typů uživatelů nejčastější odpovědí (**Graf II.10:** Jak často provádíte kontrolu e-mailu?).



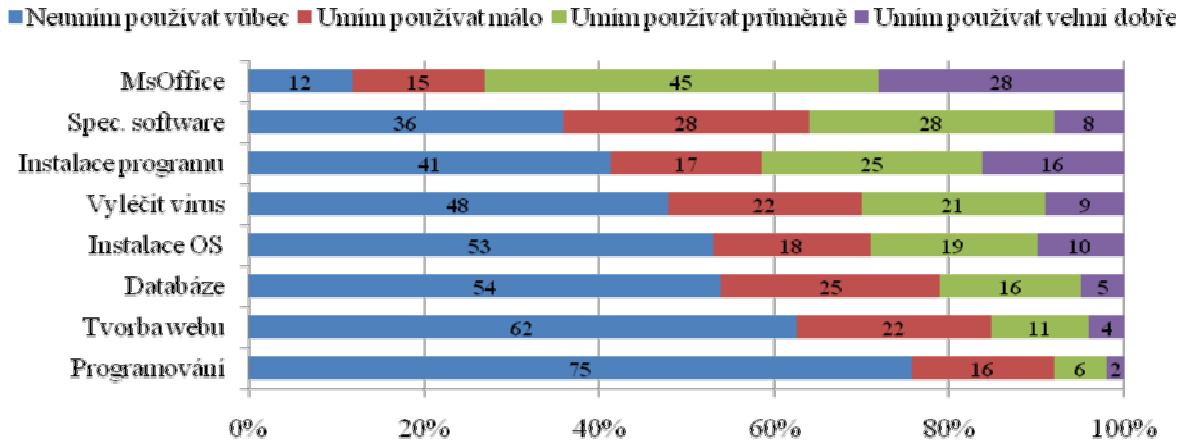
Zdroj: WIP 2007-2008, n=2121

Dílčí závěry:

- Nejčastěji užívanou službou na Internetu je komunikace, a to zejména e-mail.
- Zejména pro mladší veřejnost je Internet velmi častým zdrojem komunikace, okolo 80 % osob ve věku od 12 do 18 let používá ICQ či MSN (okolo 50 % z tohoto počtu tak činí denně).
- Cca. 70 % osob ve věku od 11 do 19 let údajně postrádá zkušenost se sledováním erotických stránek. Navštěvování erotických stránek se věnují hlavně muži „Interneťáci“.
- Cca 20 % uživatelů Internetu již alespoň někoho kontaktovalo pomocí internetové seznamky. Kontakt přes internetovou seznamku vyzkoušelo okolo 25 % osob ve věku od 12 do 30 let.
- Dominantními formami kontaktu přes seznamku jsou zprostředkování reálného setkání a/nebo telefonování.
- Více než polovina uživatelů Internetu v České republice již alespoň jednou nakoupila zboží přes Internet.

Zjištění č. 4: Počítačové dovednosti

Odpovědi na otázku "Řekněte nám, prosím, co umíte používat či dělat" (přepočet získaných údajů na populaci České republiky ve věku 12 a více let, v tisících), ukazují často propastné rozdíly v počítačové (ne)gramotnosti mezi jednotlivci a skupinami ve společnosti (**Graf II.78**):



Zdroj: WIP 2008, n=1332

Dílčí zjištění:

- Nejrozšířenější z měřených počítačových dovedností je schopnost používání základních součástí programového balíčku Microsoft® Office.
- **Téměř polovina z těch, kdo vlastní domácí počítač, neumí sama odstranit virus.**
- Mezi nejméně rozšířené dovednosti patří programování a tvorba webových stránek, následované schopností užívat databáze a schopností instalace operačního systému.
- Kombinace délky a intenzity užívání Internetu je velmi významným faktorem u takových dovedností, jako jsou používání Microsoft® Office, používání speciálního software či odstranění viru.
- U instalací obecně (jak operačního systému, tak programů) či u dovednosti tvořit webové schránky, se projevil nižší význam délky užívání Internetu oproti intenzitě, neboť úroveň dovedností v těchto oblastech nebyla u Okrajových uživatelů tak vysoká jako u typů uživatelů používajících Internet častěji.
- **Odborné počítačové kurzy mimo zaměstnání či školu absolvoval jen zlomek populace (13 %). Největší část z nich tvoří dlouhodobí uživatelé Internetu.**

Počty osob v České republice (v tisících), které umí/neumí užívat příslušné operace:

	Progra-mování	Tvorba webu	Databáze	Instalace operačních o systému	Odstra-nění viru	Instalace programu	Speciální software	MS Office
Neumím používat vůbec	4200	3 470	3 024	3 000	2 700	2 300	2 020	670
Umím používat málo	900	1 230	1 400	1 010	1 230	950	1 570	840
Umím průměrně	340	620	900	1 065	1 180	1 400	1 570	2 520
Umím velmi dobře	110	225	280	60	500	900	450	1 570

Zjištění č. 5: Zvláštnosti chování mládeže v kyberprostoru

Vztahy mezi rodiči a dětmi:

- **Rodiče kontrolují své děti při práci s Internetem ve zhruba dvou třetinách případů, nejčastěji však nejméně efektivním způsobem – pouhým omezením doby, kterou mohou děti u počítače denně strávit.**
- **Více než polovina rodičů se domnívá, že jejich schopnosti týkající se práce s počítačem jsou menší než schopnosti jejich dětí. To, že s počítačem umí zacházet lépe než jejich děti, si myslí pouze 15 % rodičů, nejvíce ze skupiny Interneťáků (50 %) a Zkušených uživatelů (37 %).**

Česká republika v mezinárodním srovnání:

- Mladší obyvatelé České republiky užívají Internet poměrně intenzivně (srovnatelně s vrstevníky v USA či Kanadě), přičemž častěji než oni využívají e-mail, chatování a telefonování přes Internet.
- Mladí obyvatelé České republiky patří v celosvětovém srovnání mezi nejintenzivnější on-line hráče a posluchače on-line rozhlasu.
- **Frekvence stahování audio a video souborů je v České republice obdobná jako v USA a Kanadě.**
- Služby obchodního charakteru užívají mladší uživatelé Internetu spíše okrajově. O to více (nejčastěji ze všech sledovaných států) hledají informace o cestování.
- **Mladší respondenti v České republice projevují v mezinárodním srovnání největší důvěru v informace obsažené na Internetu.**
- **Podobně jako jejich vrstevníci z ostatních zemí považují informace na Internetu za jeden z nejdůležitějších zdrojů informací vůbec (společně s informacemi z osobního styku).**

Hloubkové rozhovory s mládeží (mládež a informační bezpečnost):

- Mladí lidé užívají dle svých slov Internet zejména pro zábavu. Hlavním prostředkem pro dosažení tohoto cíle pro ně jsou komunikační prostředky jako ICQ, chatovací místnosti, fóra a seznamky.
- Mladí používají Internet převážně jako prostředek pro komunikaci s lidmi, které znají z běžného života a nenavazují zde (nová) reálná přátelství.
- **Rodiče nekontrolují, co jejich děti na Internetu dělají. Děti oproti svým rodičům vykazují výrazný náskok, co se týče zacházení s informační a komunikační technikou (Internetem).**
- **Ve školách absentuje systematičtější informování o možných rizicích, spojených s užíváním moderních informačních a komunikačních technologií (respektive výuka, zaměřená na jejich bezpečné užívání).**
- Internet školní mládeži usnadňuje přípravu školních prací a komunikaci k tomu potřebnou.
- **Mladí si obecně příliš nepřipouští rizika spojená s Internetem, cítí se na něm bezpečně a důvěřují mu.**
- **Informační kriminalita je mladými uživateli Internetu považována za méně či nanejvýš stejně závažnou, ve srovnání s kriminalitou páchanou mimo kyberprostor.**
- **Hacking a phishing jsou považovány za nejzávažnější útoky na Internetu. Viry a spam oproti tomu považují mladí za běžnou součást života.**
- **Některá jednání (neautorizované sdílení, spam) nepovažují mladí většinou za trestná a často tyto aktivity provozují (zejména neautorizované sdílení software, hudby a videa).**

Zjištění č. 6: Bezpečnostní chování není dostatečné

Zkušenosti s nelegálním nebo nežádoucím chováním on-line jsou v rámci České republiky následující:

- **Asi 25 % internetové populace České republiky dostává denně nevyžádanou elektronickou poštu (spam). Tento jev je však hodnocen jako nejmenší riziko spojené s užíváním Internetu.**
- **Obtěžování přes Internet zažilo 16 % všech uživatelů Internetu.**
- **Třetina uživatelů zažila pokus o phishing (snaha o vylákání hesel a osobních údajů). Častěji než ostatní skupiny mu čelí Interneťáci. Phishing považuje za nebezpečný 70 % všech dotázaných.**
- **Nejnebezpečněji je vnímán hacking, se kterým se však údajně setkalo jen asi 20 % uživatelů.**
- **S určitou formou šikany (vulgární nadávky atd.) se na Internetu setkalo 5 - 10 % dotázaných.**

Navzdory této skutečnosti jsou příslušná protiopatření spíše nedostatečná (otázky se týkaly těch uživatelů, v jejichž domácnosti je alespoň jeden počítač):

- **Pouze pětina z těchto respondentů si je zabezpečením svého počítače jista. Téměř žádní respondenti neodpověděli, že si nejsou vůbec jisti. Vliv věku na subjektivní vnímání zabezpečení počítače nebyl prokázán.**
- **Pocit bezpečí silně souvisí s přítomností antivirového programu v počítači – devět desetin z těch uživatelů, kteří na domácím počítači instalovali antivir, odpověděli kladně na otázku, zda považují svůj počítač za zabezpečený. Polovina Neuživatelů Internetu neví, zda antivir nainstalovala.**
- **Pět procent počítačů v domácnostech podle vyjádření respondentů postrádá antivir (bez ohledu na to, jak zkušeným uživatelem respondent je).**
- **Na zabezpečení svého počítače ani na zabezpečení internetových aplikací hesla nepoužívá pětina dotázaných, přičemž u Začátečníků je tento podíl dvojnásobný. Čtyřicet tři procent dotázaných používá hesla všude (jak u zapnutí počítače, tak při připojení na Internet). Méně často hesla používají respondenti starší 46 let.**
- **Pouze jedno heslo používá všude jedna třetina dotázaných, stejný podíl osob vždy používá jiné heslo.**
- **Téměř polovina dotázaných používá hesla složená pouze z jednoho typu znaků (převážně malá písmena), jedinou výjimku představují Interneťáci, kteří významně častěji používají složitější hesla.**
- **Téměř čtvrtina populace vždy využívá uživatelské nastavení programu.**
- **Polovina uživatelů Internetu nezálohuje svá data. Nejméně zálohují Začátečníci a Pomalu se rozvíjející uživatelé, nejčastěji zálohují Interneťáci.**
- **Nejpoužívanějším záložním médiem je ve všech typologizovaných skupinách CD/DVD, které následuje flash disk (USB klíč).**
- **Stahování hudby a videa či sdílení těchto souborů není vnímáno jako příliš nebezpečné (jen asi 15-20 % uživatelů Internetu vyjádřilo ohledně bezpečnosti takového chování obavy; naopak zhruba polovina respondentů takové obavy zcela postrádá). Nejmenší obavy z takového jednání vyjádřili respondenti ve věku 12 až 30 let.**

Zjištění č. 7: Zranitelné internetové bankovnictví

Specifickou oblastí, které je třeba věnovat výslovnou pozornost, jsou finanční operace na Internetu, se zvláštním důrazem na tzv. internetové bankovnictví.

- Skoro třetina uživatelů nakupuje prostřednictvím Internetu alespoň jedenkrát měsíčně. S rostoucími zkušenostmi a časem stráveným na Internetu se zvyšuje i frekvence internetových nákupů.
- **Platba kartou na Internetu je částí populace vnímána jako riziková operace (30 % respondentů). U části populace tato operace naopak nevzbuzuje žádné nebo jen malé obavy (34 %). Vyšší důvěru v platbu kartou vyjádřily zejména osoby, které užívají Internet častěji a delší dobu (a také častěji platí kartou).**
- **Využití Internet bankingu z domova je podle 63 % uživatelů Internetu bezpečné.**
- **Využití Internet bankingu z internetové kavárny či ze zaměstnání (ze školy) se lidé obávají více než užívání této služby z domova. Zejména zkušenější uživatelé jsou vůči této variantě výrazněji ostražitější (ve srovnání s užíváním internetového bankovnictví z domova).**
- **Ke GSM bankovnictví (v porovnání s internetovým bankovnictvím) jsou respondenti poněkud více obezřetní. Stejně jako u Internet bankingu, i u bankovnictví přes mobilní telefon více obav vyjádřily méně zkušené skupiny uživatelů.**

Zjištění č. 8: Potenciál pro závislost na Internetu (netholismus)

- On-line závislostním chováním jsou ohrožena 4 % populace uživatelů Internetu v České republice. U dalších 3,5 % uživatelů Internetu lze pozorovat rozvinuté závislostní chování.
- V kategorii závislých či ohrožených není zřetelný rozdíl mezi zastoupením mužů a žen. Osoby ohrožené závislostním chováním nebo závislé mírně převažují v nejmladší věkové kategorii (12-15 let) a naopak nejmenší zastoupení lze pozorovat u kategorie 50 a více let.
- Délka a intenzita užívání Internetu nesouvisí výrazně se závislostí jako primárně psychiatrickým jevem. O něco častěji jsou diagnostikovány projevy závislostních chování u Interneťáků a Rychle se učících.

Zjištění č. 9: Česká republika v mezinárodním srovnání

Mezinárodní srovnání užívání Internetu v České republice a některých jiných zemích světa přináší výzkum WIP 2007. Mezi jeho závěry patří:

- **V České republice je v současnosti mezi dospělou populací zhruba polovina uživatelů Internetu, což je méně než v ekonomicky nejvyspělejších zemích, kde tento podíl činí zhruba tři čtvrtiny.**
- **Obyvatelé České republiky ve srovnání s populací jiných zemí nadprůměrně využívají e-mail, instantní komunikátory (ICQ, MSN apod.), chatování i telefonování přes Internet.**
- **Co se týče využívání Internetu pro zábavu, zdejší uživatelé jsou jedni z nejaktivnějších. Ve stahování hudby a videí předčí Českou republiku ze sledovaných zemí jen Čínská lidová republika. I v poslechu on-line rádia a hraní her na Internetu patří obyvatelé České republiky k uživatelům s největší aktivitou.**
- **V oblasti obchodních služeb patří obyvatelé České republiky mezi průměr (on-line nakupování, on-line bankovnictví je nejčastěji užíváno dospělými v USA, Austrálii, Kanadě a Švédsku).**

Zjištění č. 10: Postoje neuživatelů Internetu

Na základě diskusí s neuživateli a mírnými uživateli Internetu lze v kontextu výzkumu formulovat několik hypotéz:

- Neuživatelé jsou k možnostem využití Internetu jakožto důvěryhodného zdroje informací výrazně skeptičtější než zbytek populace. Podíl těch z nich, kteří Internet považují za důvěryhodný, nepřesahuje 10 %.
- **V případě, že jsou neuživatelé rodiči, nekontrolují co děti na Internetu dělají a ani neví, jak by to mohli kontrolovat, respektive omezovat.**
- **Neuživatelé zejména v roli rodičů přiznávají výrazný handicap v dovednostech s technikou a Internetem oproti svým dětem. Jsou si tohoto vědomi a někteří mají snahu toto řešit.**
- Neuživatelé často zmiňují rizika a negativa Internetu a vyjadřují své obavy z tohoto fenoménu. Lze předpokládat, že jejich obavy z Internetu jsou jednou z příčin, proč jej neužívají.
- Životní styl neuživatelů Internetu je v mnohém odlišný od jeho uživatelů (zjednodušeně ho lze pojmenovat jako „poklidnější životní styl“).
- **Informační kriminalita je považována neuživateli Internetu mnohdy za závažnější či stejně závažnou ve srovnání s reálnou kriminalitou (páchanou mimo kyberprostor).**

Zjištění č. 11: Rozhovory s odborníky

Na základě rozboru zkoumaného problému dospěl řešitelský tým k rozhodnutí provést také výzkum zaměřený na odborníky působící v oblasti informačních a komunikačních technologií, věnovaný otázkám bezpečnosti. V průběhu srpna, září a října 2008 bylo podle jednotného scénáře uskutečněno 11 individuálních rozhovorů v délce od 45 do 100 minut.

Tabulka VII.1: *Počty rozhovorů s odborníky podle oblastí, v nichž působí:*

Bankovní sektor	3
Telekomunikace	2
Správa velkých sítí (více než 1 000 stanic)	3
Správa sítí menšího rozsahu (do cca 1 000 stanic)	2
Akademici	1
Celkem	11 rozhovorů

Rozhovory byly zaměřeny na následující témata:

- Informační kriminalita a její vymezení.
- Typologie informační kriminality a četnosti jednotlivých útoků.
- Možné dopady informační kriminality a její prevence.
- Popis pachatelů informační kriminality.
- Doporučený standard pro domácí uživatele.

V průběhu rozhovorů se objevila také témata, která by sice zasloužila další zkoumání, ale v této zprávě jsou zastoupena pouze dílčím způsobem:

- Problematičnost spolupráce s Policií České republiky při reálných útocích.
- Interní informační kriminalita u určitých typů zaměstnavatelů (jako poměrně častý latentní jev).
- Výhledy do budoucna (speciální útoky, možná rizika).

Informační kriminalita a její vymezení

V obecné rovině existuje shoda na vymezení informační kriminality jako kriminality páchané v oblasti počítačové techniky (odtud také někdy vyplynul pojem „počítačová kriminalita“ nabízený některými odborníky jako synonymum), zpravidla v rámci sítí, zejména Internetu. Nutno dodat, že někteří odborníci poměrně striktně rozlišují tzv. „kriminalitu nového typu“ (informační kriminalitu v užším slova smyslu) a kriminalitu „starou“ (tradiční), páchanou pouze jinými prostředky.

Mezi kriminalitu již dříve známou lze řadit nejrůznější pokusy o získání finančních prostředků jinými způsoby (např. phishing, skimming apod.), kde je základní logika podobná prosté krádeži, pouze se liší použitý způsob páchání činů (namísto fyzického odcizení věcí či finančních prostředků se tak děje skrze výpočetní techniku). Kriminalita nového typu (informační kriminalita v užším slova smyslu) je přímo zaměřená na nové prostředí. Patří sem například DNS[4] útoky, či pokusy o průniky do systémů. Některé činy bylo pro většinu oslovených problematické zařadit do kategorie informační kriminality. To se týkalo zejména porušování autorských práv, které je vnímáno jako relativně malé nebezpečí a pod pojem informační kriminalita spíše nespadá (výjimkou byly názory odborníků, kteří tyto delikty ve své každodenní praxi správců sítí řeší).

Celkově lze konstatovat, že odborná komunita pojem informační kriminalita vnímá relativně nejednotně (a používání tohoto pojmu se tak v jejím rámci stává poněkud problematické).

[4] Denial of service (v češtině „odmítnutí služby“).

Poměrně překvapivě nebyla většinou explicitně zmiňována kriminalita mířící na mobilní telefony a do budoucna i další technologická zařízení (pouze jeden odborník naznačil budoucí nebezpečí „odposlechů“ domácích spotřebičů typu myčka, trouba, pračka apod.).

Typologie informační kriminality a četnosti jednotlivých útoků

Pokud byli odborníci v oboru informačních a komunikačních technologií vyzváni k provedení klasifikace či typologie informační kriminality, byly výsledky nejrůznější. Někteří respondenti odmítali možnost typologií vůbec a namítali, že používané typologie jsou pouze ad hoc přehledy, sestavené na základě podobných znaků. Nicméně většina oslovených používá kategorie jako je spam, viry, spyware, DNS poměrně běžně. Vychází z této klasifikace i ve své práci (například při monitoringu bezpečnostních incidentů se tyto kategorie užívají pro zachycení jejich dynamiky). Jako nejlépe rozlišitelný incident bývá uváděn spam a porušování autorských práv. U ostatních útoků je již rozlišování problematické.

Z hlediska četnosti útoků je mezi odborníky z jednotlivých oblastí shoda v tom, že nejvíce se vyskytuje nevyžádaná pošta (tzv. spam, a to v řádech stovek či tisíců případů denně u jednotlivých firem). Méně časté jsou útoky za použití virů či spyware. Podle charakteru organizace se poté liší další typy útoků (banky se potýkají s phishingovými útoky, jejichž četnost je závislá zejména na velikosti banky). Lze také zmínit útoky, které se odehrávají interně v sítích, na něž dohlížejí oslovení odborníci. V akademickém prostředí je poměrně časté porušování autorských práv a rozesílání spamu (méně časté jsou pokusy o narušení administrátorských práv). Banky a mobilní operátoři jsou často konfrontovány s pokusy o interní narušení systému, zejména za účelem získání finančních prostředků (defraudace).

Možné (negativní) dopady informační kriminality a její prevence

a) Dopady a prevence ve firmách

Z hlediska dopadů informační kriminality (zejména pro některé typy firem, jako jsou banky a telekomunikační společnosti) byly často zmíněny **přímé finanční ztráty**. Tento typ dopadů informační kriminality naopak u některých subjektů výrazně nehrozí (např. ve školách, u poskytovatelů připojení). Poměrně zajímavé bylo, že i zástupci bank zmiňovali, že finanční dopady stávajících útoků nejsou nijak výrazné a mnohem horším nebezpečím je **ztráta dobré pověsti** (např. při odcizení klientských údajů, kvůli kterému může dojít k odlivu klientů). **Tato obava způsobuje také časté nenahlášení těchto činů orgánům činným v trestním řízení a tedy vysokou latenci těchto forem kriminálního jednání**. Dalším dopadem informační kriminality ve firmách je zejména **nutnost věnovat odstraňování škod mnoho času jednotlivých pracovníků** či nutnost zaplatit specializované firmě za její pomoc. Tento důsledek informační kriminality spontánně zmínili téměř všichni odborníci a na jednotlivých příkladech demonstrovali velkou **pracnost odstraňování útoků** (např. kompletní přeinstalace mnoha počítačů v rámci systému může znamenat i několik týdnů pracovního času několika zaměstnanců). Tento dopad (společně s časem zaměstnanců věnovaným prevenci a monitorování provozu sítí) je vnímán jako největší náklad a „daň za užívání výpočetní techniky“.

V rámci preventivních opatření pro firmy byla nejčastěji zmiňována školení pro zaměstnance (či obecně pro uživatele pohybující se ve spravovaném systému). Dále byl uváděn bezpečnostní audit, nalezení slabých míst a implementace doporučení, vzešlých z tohoto auditu a v neposlední řadě bezpečnostní standard uživatelů (zpravidla zakotvený v písemné příručce). Zatímco v bankách jsou školení pro zaměstnance povinná, v jiných typech subjektů to může být problematické (vysoké školy neprovozují povinná školení pro všechny vyučující a studenty). Dalším preventivním opatřením je snaha zabránit uživatelům v provádění některých typů operací, např. v přístupu na soukromý e-mail, otevírání příloh či přístupu na Internet obecně apod. V bankách či telekomunikačních firmách se některá tato opatření uplatňují, u jiných subjektů jsou méně častá (dle názoru odborníků jsou tyto kroky méně účinné než poučení uživatelů). Zejména v akademické sféře odborníci upozorňovali na problematičnost takových omezení (s ohledem na akademické svobody a odlišné potřeby různých typů uživatelů).

Obecně se odborníci shodují v tom, že náklady na prevenci nesmí být „přehnané“ a musí respektovat hlídané hodnoty („*Trezor nesmí být dražší než peníze v něm uložené*“).

b) Dopady a prevence pro domácí uživatele

Z pohledu domácího uživatele hrozí dle odborníků tato nebezpečí:

- finanční ztráta (např. při phishingu, skimmingu apod.);
- ztráta osobních dat a jejich zneužití či kompletní krádež identity (tedy přístupových kódů či elektronického podpisu).

Zejména posledních zmíněných hodnot si dle názoru odborníků širší veřejnost dostatečně neváží (a proto vyjadřuje i nižší míru obav z informační kriminality).

Jen okrajově byly zmiňovány dopady sexuálně motivovaných útoků na děti. Důvodem je zřejmě zaměření zpovídaných odborníků na oblast informační bezpečnosti ve větších firmách či sítích.

Popis pachatelů informační kriminality

Odborníci se snažili rovněž vyjádřit k osobám pachatelů informační kriminality a jejich specifickým charakteristikám. Popisy pachatelů většinou nevycházely z osobní zkušenosti či kontaktů s pachateli (pouze jeden odborník byl aktivně v kontaktu s hackery). Jsou tak více založené na znalostech z odborné literatury a diskusí na odborných forech. Z názorů odborníků vyplývá, že již středoškoláci začínají experimentovat s různými jednoduchými útoky (tzv. skript kiddies), pro jejichž spáchání mohou na Internetu stáhnout nástroje vytvořené zkušenějšími hackery. Z výpovědí odborníků také vyplynulo, že hackeři často nebudují své znalosti formálně, tedy ve školách, ale pomocí neformálních sítí a zkoušením útoků. Při otázce po základní motivaci k páchání informační kriminality byly uváděny možnosti „něco si dokázat“ (klasický hacker) nebo „vydělat si“ (hacker někým najatý).

Odborníci často upozorňovali na nevhodné používání názvů pro pachatele, kdy slovo **hacker** ve skutečnosti označuje osoby, které do systému pronikají bez motivace jej zneužít, „pouze“ chtějí upozornit na jeho nedostatky. Naopak výraz **cracker** popisuje ty, kteří chtějí průniky do systémů zneužít. Pro speciální útočníky se vedle toho užívá i dalších výrazů.

Odborníci často zmiňovali, že dnes se již setkáváme s organizovanými skupinami, kde existuje vysoká míra dělby práce a kdy se k útokům používá velké množství počítačů. Organizovaná kriminalita se tedy částečně již přesouvá i do kyberprostoru, protože zde je možné docílit poměrně zajímavé zisky (navíc s relativně malým rizikem odhalení; jeden z odborníků právě nízkou míru objasněnosti použil jako charakteristický znak informační kriminality). Při posouzení četnosti útoků jednotlivců a organizovaných skupin převažují nejspíše útoky jednotlivců, nicméně souhrn škod způsobených organizovanými skupinami nejspíš převyšuje škody způsobené jednotlivci.

Doporučený standard pro domácí uživatele

a) softwarové vybavení

V oblasti softwarového vybavení lze shrnout doporučení lapidárně slovy jednoho z expertů: “antivir, firewall, legální software“. Po nahlédnutí do reality domácností v České republice lze pochybovat o naplnění těchto standardů (viz výše uvedený výzkum WIP 2008). Antivir je na cca 90 % počítačů, nicméně nelze rozlišit, zda jej respondenti aktualizují, respektive zda jej používají aktivně jako rezidentní ochranu. Otázka na firewall nebyla ve výzkumu World Internet Project 2008 ani kladena, protože ve zkušebních rozhovorech tomuto pojmu mnozí respondenti ani nerozuměli. Lze očekávat, že užívání tohoto prvku v domácnostech v České republice není příliš časté, nicméně empirická evidence neexistuje. Legální aktualizovaný software (zejména operační systém) je opět problémovým místem. Zhruba třetina počítačů v domácnostech v České republice je vybavena systémem Windows 2000, jehož pořizovací cena byla poměrně vysoká, tudíž se zřejmě často bude jednat o systém pořízený nelegálně.

U systému Windows XP lze očekávat, že zhruba polovina uživatelů provozuje nelegální verzi, tj. verzi bez bezpečnostních aktualizací. Z hlediska operačních systémů v tuzemských domácnostech lze tedy očekávat poměrně výrazné bezpečnostní riziko. Dalšími softwarovými prostředky, které by měly být opět aktualizovány (a legální), jsou zejména internetové prohlížeče. S ohledem na skutečnost, že převažujícím prohlížečem je Internet Explorer, bude i zde zřejmě platit, že řada z nich je nainstalována nelegálně. Samostatnou kapitolou je instalování rizikového software z nedůvěryhodných zdrojů.

b) doporučení pro chování uživatelů

Většina odborníků upozorňovala, že právě lidský faktor často selže a pak jsou všechna opatření neužitečná. Mezi problémové situace patří zejména:

- navštěvování pochybných webových stránek;
- povolení instalace různých „doplňků“, nabízených na internetových stránkách;
- klikání na neznámé odkazy;
- otevírání příloh/odkazů v mailech od neznámé (ale někdy i známé) osoby;
- používání internetového bankovnictví a placení na Internetu platební kartou;
- užívání hesel a jejich složitost;
- péče o počítač a software;
- výchova a vzdělávání uživatelů.

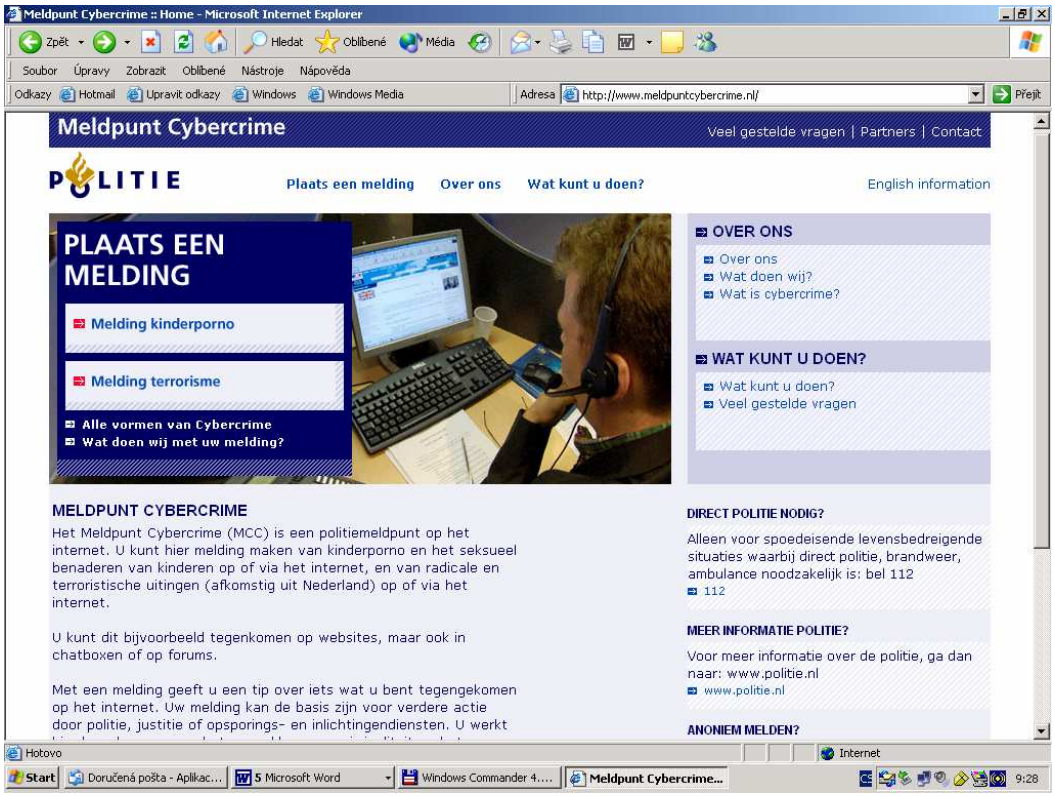
Problematičnost spolupráce s Policií České republiky při reálných útocích

Jako jedno z dalších témat v oblasti informační kriminality a bezpečnosti, sporadicky zmíněných samotnými odborníky, byla **spolupráce s Policií České republiky**. Zejména v bankovním sektoru a telekomunikacích postrádají odborníci rychlou spolupráci, která by umožnila řešení útoků v reálném čase. **Uvítali by existenci speciální policejní složky, se kterou by bylo možné komunikovat elektronicky a s jejíž pomocí by bylo možné operativně zastavit provoz z problémových serverů**. Současná situace vypadá dle odborníků tak, že napadený subjekt (jeho zaměstnanec) musí jít učinit oznámení na místně příslušnou služebnu Policie České republiky, kde se často setká s policistou, který této problematice nerozumí. Navíc je toto oznámení poměrně zdlouhavě předáváno v rámci Policie České republiky a než dojde k zastavení provozu problematických serverů či zablokování přístupu na problémové servery (např. při phishingovém útoku), je již útok ukončen, respektive došlo již ke značným škodám.

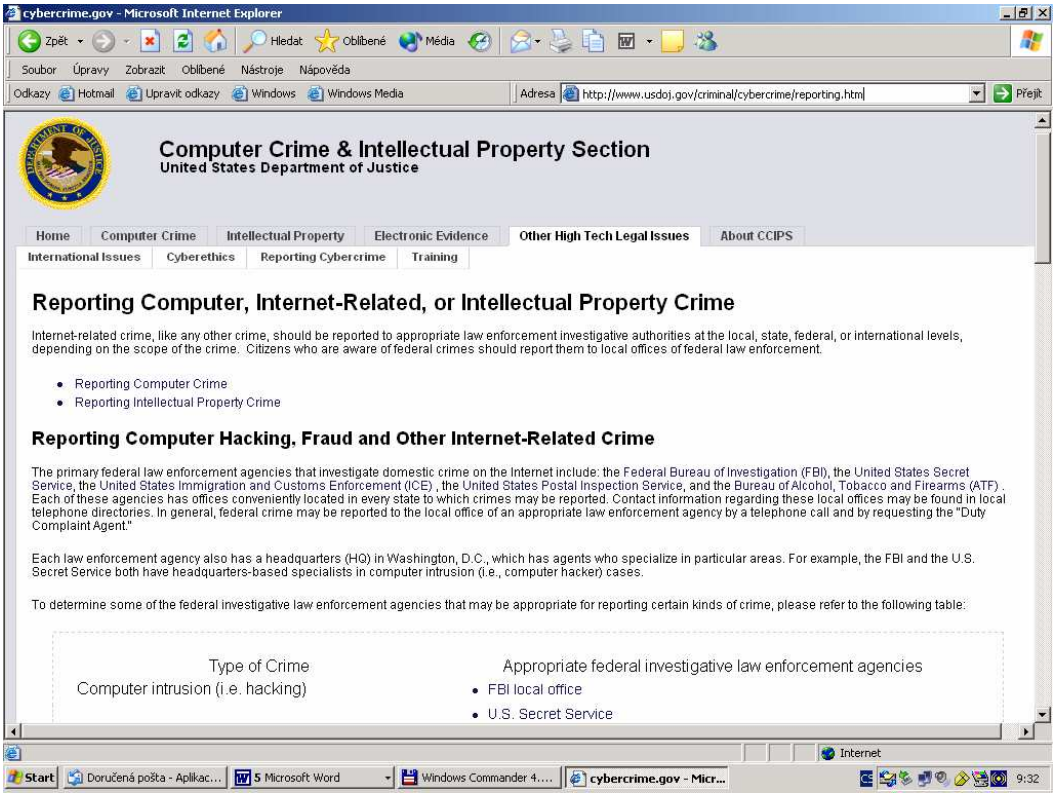
Na tuto skutečnost rovněž upozorňuje materiál, připravovaný pro jednání vlády České republiky (Analýza aktuální úrovně zajištění kybernetické bezpečnosti České republiky): *Situace je značně problematická i z hlediska „spotřebitele“ (zákazníka) policejní činnosti. Současný stav, kdy je například kybernetický útok na konkrétní banku nutné řešit podáním trestního oznámení na místně příslušné policejní služebně nebo státním zastupitelství, je dlouhodobě neúnosný. Ačkoli se jedná o incident, kdy o značných finančních škodách rozhodují prakticky minuty, je takový případ v praxi zprocesňován i několik měsíců. Situaci by přitom bylo možné, na základě zahraničních zkušeností, možné řešit výrazně efektivněji, elegantněji a pružněji (například prostřednictvím vytvoření speciálního internetového okna pro hlášení incidentů tohoto charakteru). Tento postup by přitom naprosto jistě znamenal několikanásobné navýšení počtu nahlášených informačních incidentů, a proto by nutně musel korespondovat s náležitým personálním a materiálním posílením příslušných policejních složek, zejména Skupiny informační kriminality Policejního prezídia České republiky).*[5]

[5] Tento aspekt byl, mimo jiné, výslovně zmíněn během porady pracovní skupiny pro vytváření standardů budování CSIRT v České republice (2. července 2008), kdy na něho upozornili **zástupci významných soukromých společností** (CZ.NIC, Telefonica O_2, Česká spořitelna a. s., Volksbank, GE Money Bank, mediální skupina MaFra atd.).

Příklad takového řešení z Nizozemska: http://www.meldpuntcybercrime.nl/



Přístup USA, různé činy je třeba hlásit různým institucím:
http://www.usdoj.gov/criminal/cybercrime/reporting.htm



Interní informační kriminalita u určitých typů zaměstnavatelů

Při rozhovorech s odborníky se jako samostatné téma objevil problém tzv. interní kriminality ve firmách a organizacích. Zaměstnanci se pokouší nejrůznějším způsobem získat neoprávněné výhody a přístup do chráněných systémů. Tato činnost je poměrně častá (zejména v bankovním sektoru), nicméně většinou jí zaměstnavatel neřeší trestněprávně (důvodem je ztráta dobré pověsti bankovního domu), ale pouze pracovněprávně (ukončením pracovního poměru). V oblasti akademické sféry (vysoké školy) je přístup ještě volnější a studenti (ale i pedagogové), kteří se dopouštějí problémového jednání, jsou většinou postaveni před fakultní disciplinární komise, kde bývá jediným trestem podmíněné vyloučení (správci fakultních či univerzitních sítí uváděli, že neví o tom, že by někdy došlo k vyloučení studenta i při opakování problémového jednání). Nutno dodat, že toto poměrně mírné trestání specifických forem informační kriminality nepůsobí odrazujícím způsobem na potenciální pachatele. Přitom je zřejmá problematičnosti trestněprávní ochrany v oblasti informační kriminality v České republice[6]. V souvislosti s interní informační kriminalitou zazněl i názor, že lidé nastupující na exponované pozice by měli povinně procházet psychologickým testováním a psychologickým pohovorem, aby se riziko jejich závadného jednání minimalizovalo.

Výhledy do budoucna (speciální útoky, možná rizika)

Při rozhovorech došlo také na úvahy o budoucím vývoji informační kriminality a bezpečnostních rizik. Odborníci upozorňovali, že s nárůstem počtu zařízení užívajících počítačové technologie a jejich síťového propojování bude narůstat možnost jejich zneužívání. Zároveň lze očekávat nárůst sofistikovanosti útoků. Někteří odborníci také spekulovali o přípravách na tzv. kyberválku, která může být vedena jednotlivými státy či jejich bezpečnostními službami (viz např. incidenty v Estonsku, Litvě či Gruzii). Odborníci upozorňovali na reálnou možnost výskytu obdobného útoku proti České republice, nicméně možnost obrany nenabídli.

Závěry, které z výše uvedených rozhovorů celkově vyplývají, jsou:

- Expertní komunita pojem informační kriminalita vnímá relativně nejednotně a někteří odborníci dokonce používání tohoto pojmu zpochybňují. Někteří odborníci odmítají možnost typologizace informační kriminality vůbec.
- **Negativní dopady informační kriminality pro firmy a organizace spočívají především v přímých a nepřímých finančních ztrátách. Výraznější jsou nepřímé náklady ve formě pracovního času zaměstnanců, kteří odstraňují vzniklé škody a věnují se prevenci. Z důležitých preventivních opatření byla zmiňována zejména nutnost školení uživatelů v rámci organizací.**
- **Negativní dopady informační kriminality pro jednotlivce na sebe mohou brát podobu finančních ztrát, ale i ztráty osobních údajů, případně elektronické identity.**
- **Pachatelé informační kriminality působí dle odborníků dnes častěji v organizovaných skupinách, vyznačujících se vysokou dělbou práce. „Vzdělávání" těchto pachatelů probíhá prostřednictvím neformálních sítí na Internetu.**
- Doporučení odborníků pro domácí uživatele Internetu a počítačů lze zařadit do dvou oblastí: ***doporučení softwarové a hardwarové:*** užívání legálního software s pravidelnou aktualizací, instalace antiviru a firewallu; ***doporučení s ohledem na uživatelské chování:*** nenavštěvování webových stránek, nepovolení instalace různých doplňků, neklikání na neznámé odkazy, neotevírání příloh či odkazů v e-mailech či komunikátorech (ICQ, MSN apod.), opatrné užívání internetového bankovnictví a plateb na Internetu kartou, užívání hesel a péče o počítač a software.
- **Je pociťována nedostatečná pozornost, která je věnována bezpečnostní problematice v rámci vzdělávání na základních a středních školách.**
- Interní informační kriminalita je poměrně častá, nicméně její řešení není většinou trestněprávní.
- **Do budoucna se lze obávat výraznějších útoků, které mohou způsobit mnohem větší škody.**

[6] Viz např. Gřivna; Polčák 2008 (http://www.auditorium.cz/kybe)

Zjištění č. 12: Bezpečnost v soukromém sektoru

Tato pasáž vychází z kvantitativního výzkumu věnovaného problematice bezpečnosti informačních technologií. Sběr příslušných dat se uskutečnil v květnu 2008 a výzkumu se zúčastnilo 2 358 respondentů (zástupců firem, které byly vybrány z panelu firem používaného firmou Digimark pro pravidelné výzkumy).[7] Z tohoto výzkumu vyplynuly následující skutečnosti:

- Firmy působící v České republice se nejčastěji potýkají s počítačovými viry a jiným škodlivým software (malware). V součtu více než třetina firem tyto problémy řešila za poslední rok vícekrát.
- **Útoky na webové stránky a vnitřní síť firmy zaznamenalo pouze cca 13 – 16 % firem.**
- **Nejlépe jsou zpravidla zabezpečeny webové stránky firmy a vnitřní síť.**
- Nejméně jsou podle názorů respondentů ve firmách zabezpečeny Wi-Fi sítě, respondenti uvádějí, že 27 % z nich není dostatečně zabezpečeno.
- **Platí, že větší firmy a firmy z oborů informačních technologií provozují zpravidla lepší zabezpečení.**
- Z hlediska oborů činnosti chystají v příštím roce do informační bezpečnosti technologií investovat nejvíce firmy působící právě v oblasti informačních technologií, nejméně pak firmy z oblasti (jiných) služeb. Téměř 40 % podnikatelů-fyzických osob nebude do informační bezpečnosti investovat, naopak nejvíce budou investovat zahraniční firmy.
- Investice plánují zejména firmy největší, případně firmy působící v oboru informačních technologií.

[7] Tuto studii provedla firma Digimark v červnu 2008. Celý název studie zní: „Bezpečnost v telekomunikacích, síťové prvky a ústředny v českých firmách“.