INFORMAČNÍ BEZPEČNOST

JARO 2013

KISK FF MU

KDO?

- PhDr. Pavla Kovářová
- ÚISK
- KISK
- SITMU
- Ikaros – členka redakce
- Kontakty: kovarovap@gmail.com

KDY A KDE?

- Každý týden
- Středa 9:10–10:45
- Seminární místnost KISK

CO?

- Přednášky vždy z teorie ode mne a Vašich diskuzí
- Před přednáškou nutná příprava na zadané téma (ODBORNÉ články)
- Nutná docházka, možné 2 absence
- Dálkaři místo diskuze doplňkový úkol (během semestru) – analýza preventivního zdroje + prezentace na přednášce 24. 4.
- Závěrečný úkol – termín 8. 5.
- Závěrečná diskuze

ÚKOL

- Skupiny po třech
- Každý o obou dalších zjistí na internetu osobní informace
- Na jejich základě vytvoří pro každou oběť 3 scénáře útoku (konkrétní, k provedení, 2x3=6)
- Zpráva o všem, konkrétní (kdo, co, kde, jak, s odbornými termíny)
- Vše s dodržením zákona
- Podmínkou kvalita, ne kvantita

K ČEMU TO?

- Ukončení předmětu
- Bližší poznání dvou spolužáků/spolužaček
- 2 osobní penetrační testy
- Zprávy budou využity při tvorbě mé disertační práce (lze odmítnout)

- Nějaký problém?

TÉMATA

- 20. 2. – úvodní informace, terminologie
- 27. 2. – zneužitelné osobní informace na internetu a sociální inženýrství (Kevin Mitnick)
- 6. 3. – malware (Stuxnet)
- 13. 3. – nevyžádané zprávy (Drahoušek zákazník – phishing pro Českou spořitelnu v 1Q 2008)
- 20. 3. – nevhodný a nelegální obsah – autorské právo a pornografie („osvětové akce“ BSA; Kolik je pornografie na internetu?)
- 27. 3. – nevhodný a nelegální obsah – agresivita a násilí a extremistická hnutí a náboženské sekty (Vesmírní lidé; Heaven's Gate a internet)

TÉMATA (2)

- 3. 4. – specifičtí uživatelé – děti (kybergrooming a případ Hovorka, kyberšikana a Star War Kid)
- 10. 4. – specifičtí uživatelé – firmy a jejich informační politika, stát a hacktivismus (Anonymous)
- 17. 4. – kryptologie (digitální podpis v ČR)
- 24. 4. – preventivní iniciativy (Saferinternet CZ)
- (1. a 8. 5. samostudium, co se nestihlo)
- 15. 5. – zabezpečení (sdílení zkušeností)

A TEĎ VY…

- Kdo?
- Proč?
- Co čekáte (od předmětu, ode mne)?

- Co je podle Vás informační bezpečnost?

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERSITAS MASARYKIANA BRUNENSIS
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

ZÁKLADNÍ TERMINOLOGIE

INFORMAČNÍ BEZPEČNOST

24. 2. 2011

INFORMAČNÍ BEZPEČNOST

- Pro každého něco jiného
  - Majitel firmy
  - Hacker
  - Politik
  - Rodič
  - Bezdomovec
  - Voják
- Z našeho pohledu zásadní role
  - Knihovník/informační pracovník
  - Vzdělávací pracovník
  - Uživatel

INFORMAČNÍ BEZPEČNOST

- I. etika
- I. gramotnost
- I. chování
- I. kanál
- I. pracovník
- I. služba
- I. společnost
- I. systém
- I. věda
- I. zdroj

INFORMAČNÍ GRAMOTNOST

- „To be information literate, a person must be able to recognize when information is needed and have the ability to locate, evaluate, and use effectively the needed information“ (def. ALA, 1989)
- „IG představuje komplexní znalost a schopnost práce s informacemi a technologiemi s nimi spojenými“ (Kovářová, ProInflow, 2011)

INFORMAČNÍ GRAMOTNOST (2)

- Někdy omezována na VŠ prostředí
- Podrobně popsána v mnoha modelech a standardech, které informační bezpečnost chápou jako nepopiratelnou součást
- Podřazeny např. počítačová/ICT a internetová/síťová gr. (Dombrovská, 2002)
- Někdy označován pojem jako nevhodný – nové gramotnosti, hl. mediální (TDKIV nezná X „Studia nových médií“)

- Podrobněji v ProInflow

INFORMAČNÍ ETIKA

- „Dílčí část etiky, která se zabývá morálními principy a pravidly souvisejícími se zpracováním informací. Informační etika dále zahrnuje etiku tvůrce informace (autorská etika), etiku zprostředkovatele informací a etiku uživatele informací.“ (TDKIV + další 3 zdroje)
- „Informační etika je oblast etiky, která zkoumá řád správného jednání v těch oblastech informační společnosti, které souvisí s informacemi a s informačními a komunikačními technologiemi (dále ICT).“ (M. Lorenz)
- Silná vazba na ICT, ale IE ≠ počítačová/ICT/internetová/síťová… etika

PROČ BEZPEČNOST?

- Základní lidská potřeba
- Může zničit mnohá pozitiva (jaderná energie)
- Někdy stačí minimální snaha či znalost, aby se člověk vyhnul maximálním nepříjemnostem (malware – zombie, nechtěné úložiště…)
- S rostoucím významem informací, jejich hodnotou a přesunem velké části života na internet roste i význam informační bezpečnosti

INFORMAČNÍ BEZPEČNOST

- Užší: „Ochrana počítačového systému a dat před poškozením a ztrátou informací.“ (Slovník výpočetní techniky, 334; TDKIV)
- IB řešili hl. informatici, ti ale často ve vzdělávání bezradní X vzdělání = základ
- Dle ostatních definic informačních záležitostí i IB nadřazená počítačové/ICT/síťové/internetové/datové a dalším
- IB = ochrana před ohrožením způsobeným informacemi a technologiemi s nimi spojenými
- Prvky IB nejen data, technologie, informace, systémy atd., ale i lidé
- Jako IE i IB na úrovni tvůrce, zprostředkovatele i příjemce informací (tj. od dezinformací a hodnocení informací po elektronické platby a jejich zajištění)

INFORMAČNÍ (NE)BEZPEČNOST

- Informační bezpečnost = zajištění ochrany
- Každá ochrana kvalitnější, když nebezpečí známé
- Některá nebezpečí lze omezit technologicky, ale každé chováním
- Jak zajistit spravedlnost nebo dokonce bezpečí?

  Číslo účtu u švýcarské banky, která má pobočku v Praze, zneužije Brazilec při své dovolené v Austrálii pomocí počítače vyrobeného v Číně s pirátským operačním systémem americké společnosti, který crackli Rusové.
- Zde – problém + ochrana proti němu (technologická, uživatelská, legislativní, etická) + jak to vypadá v praxi

PROTI KOMU?

- Hacker:
- 2WW – 70. léta 20. století: každý programátor kvůli nedostatečné technické podpoře
- 70.-90. léta: „zlatá éra“:
  - Kevin Mitnick a sociální inženýrství
  - Robert T. Morris a počítačový červ
  - Kevin Poulsen a phreaking („naboural se do telefonních linek kalifornské rozhlasové stanice, aby mohl vyhrát automobil značky Porsche v posluchačské soutěži“ - Matějka: Počítačová kriminalita, s. 28)
- Dnes: přechod překonávání hranic a touze po neomezeném přístupu k informacím a vzdělávání X praktičtější, snaha o finanční obohacení

PROTI KOMU? (2)

- Hacker: původní ideály
- Cracker: „zlý“ hacker NEBO ten, kdo obchází softwarové ochrany
- Další dělení...
- Média: nahodilé užití pojmů (např. hacker a pirát)

O CO JDE V PRVNÍ ŘADĚ?

- INFORMACE
- Zneužitelné nějakým způsobem všechny informace – omezení na legislativně opatřené = největší ohrožení

INFORMACE V ČESKÝCH ZÁKONECH

- § 3 zákona 106/1999 Sb. o svobodném přístupu k informacím:
  - „**Zveřejněnou informací** pro účel tohoto zákona je taková informace, která může být vždy znovu vyhledána a získána, zejména vydaná tiskem nebo na jiném nosiči dat umožňujícím zápis a uchování informace, vystavená na úřední desce, s možností dálkového přístupu nebo umístěná ve veřejné knihovně.“

INFORMACE V ČESKÝCH ZÁKONECH (2)

- § 2 písm. a zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti:
  - „**utajovanou informací** informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací“
- § 17 zákona 513/1991 Sb. (obchodní zákoník)
  - „**Obchodní tajemství** tvoří veškeré skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle vůle podnikatele utajeny a podnikatel odpovídajícím způsobem jejich utajení zajišťuje.“

ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ (§ 4)

- **Osobní údaj**: „jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“
- **Citlivý údaj**: „osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.“

OSOBNÍ INFORMACE (2)

- Někde i osobní a neosobní údaj
- Osobní informace – kvůli terminologii pro širší vymezení
- Většina problémů založena na osobních informacích
- V komerčním prostředí obvykle kvalitní technické zajištění – útoky na lidi a jejich osobní informace
- Pro uživatele největší ohrožení přes jejich soukromí
- Člověk = vždy nejslabší článek zabezpečení (sociální inženýrství)

ZÁKLADNÍ POJMY INFORMAČNÍ BEZPEČNOSTI (POŽÁR, S. 37-38)

- „Hrozba (Threat) je skutečnost, událost, síla nebo osoby, jejichž působení (činnost) může způsobit poškození, zničení, ztrátu důvěry nebo hodnoty aktiva. (…)
- Riziko (Risk) je pravděpodobnost, s jakou bude daná hodnota aktiva zničena nebo poškozena působením konkrétní hrozby, která působí na slabou stránku této hodnoty. Je to tedy míra ohrožení konkrétního aktiva. (…)
- Útokem, který nazýváme rovněž bezpečnostní incident rozumíme buďto úmyslné využitkování zranitelného místa, tj. využití zranitelného místa ke způsobení škod/ztrát na aktivech IS, nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. (…)
- Zranitelnost (Vulnerability) je nedostatek nebo slabina bezpečnostního systému, která může být zneužita hrozbou tak, že dojde k poškození nebo zničení hodnoty aktiv. (…)“

BEZPEČNOSTNÍ INCIDENT (DOSEDĚL, S. 22)

- Způsobený uživatelem
  - Úmyslné
  - Neúmyslné
- Jiné působení
  - Havárie
  - Chyba systému

TYPOLOGIE ÚTOKŮ PODLE POŽÁR, S. 118-119

- Způsob, jak se projeví způsobená škoda
  - Ztráta integrity (neporušitelnost dat)
  - Ztráta dosažitelnosti
  - Ztráta autenticity (entita je taková, za jakou se označuje)
- Druh způsobené ztráty
  - Neautorizované použití služeb (autorizace = důvěryhodnost uživatele z pohledu IS)
  - Přímá finanční ztráta
  - Fyzické poškození, vandalismus
- Role, kterou výpočetní technika hraje v tomto konání
  - Objekt útoku
  - Nástroj
  - Prostředí
  - Symbol

TYPOLOGIE ÚTOKŮ PODLE POŽÁR, S. 118-119 (2)

- Použité prostředky
  - Opisování údajů
  - Špionáž
  - Vkládání falešných dat
  - Krádež
  - Odposlech
  - Scanování, prohledávání (např. prolamování hesel zkoušením)
  - Piggybacking, tailgating (útočník se snaží projít vstupní kontrolou zároveň s autorizovanou osobou nebo pokračovat v započaté činnosti)
  - Malware
  - Pirátství

INFORMAČNÍ BEZPEČNOST A KNIHOVNÍCI/INFORMAČNÍ SPECIALISTÉ

- Oni sami svou roli vidí
- Pedagogové (učitelé na 1. a 2. stupni) také
- Neinformatici málo, ale přece (Požár, s. 282-283)

- Informatici téměř nikdy

POUŽITÁ LITERATURA

- BusinessCenter.cz [online]. 1991 [cit. 2011-02-23]. Zákon č. 513/1991 Sb., obchodní zákoník . Dostupné z WWW: <http://business.center.cz/business/pravo/zakony/obchzak/>.
- DOMBROVSKÁ, Michaela. Informační gramotnost: funkční gramotnost v informační společnosti. In Inforum 2002 [online] Praha: VŠE, 2002. [cit. 2010-08-16] Dostupné na WWW: <http://www.inforum.cz/inforum2002/prednaska37.htm>
- DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno : Computer Press, 2004.
- Global Network Initiative [online]. c2008 [cit. 2009-03-30]. Dostupný z WWW: <http://www.globalnetworkinitiative.org/>.
- HAMBRIDGE, Sally. Delaware Tech [online]. 1995, 24 October 1995 [cit. 2011-02-21]. RFC 1855: Netiquette Guidelines. Dostupné z WWW: <http://www.stanton.dtcc.edu/stanton/cs/rfc1855.html>.
- ICT New Zealand [online]. 23rd April 2009 [cit. 2011-01-23]. Information Literacy Models and Inquiry Learning Models. Dostupné z WWW: <http://ictnz.com/infolitmodels.htm>
- Information Literacy Instruction Handbook. Christopher N. Cox, Elizabeth Blakesley Lindsay. Atlanta : Association of College and Research Libraries, 2008. 236 s. ISBN-13: 978-0-8389-0963-8.
- Komora auditorů České republiky [online]. c2010 [cit. 2010-08-16]. Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Dostupné z WWW: <http://www.kacr.cz/Data/files/Metodika/Aktuality/300_2008.pdf>.
- LI, Lili; LESTER, Lori. Rethinking Information Literacy Instructions in the Digital Age. The International Journal of Learning. 2009, 16, 11, s. 569-577. Dostupný také z WWW: EBSCOhost. ISSN 1447-9494.
- LLOYD, Annemaree. Information Literacy Landscapes : Information literacy in education, workplace and everyday contexts. Oxford : Neal-Schuman Publishers, 2010. 200 s. ISBN-13: 978-1843345077.

POUŽITÁ LITERATURA (2)

- MATĚJKA, Michal. Počítačová kriminalita. 1. vyd. Praha : Computer Press, 2002. 106 s. ISBN 80-7226-419-2.
- Media Literacy : New Agendas in Communication (New Agendas in Communication Series). 1. New York : Routledge, 2009. s. 256. ISBN-13: 978-0415872218.
- Ministerstvo kultury [online]. c2007 [cit. 2010-08-16]. Zákon č.106/1999 Sb., o svobodném přístupu k informacím. Dostupné z WWW: <http://www.mkcr.cz/scripts/detail.php?id=325>.
- Ministerstvo vnitra České republiky [online]. c2010 [cit. 2010-08-16]. Zákon č. 227/2000 Sb., o elektronickém podpisu. Dostupné z WWW: <http://www.mvcr.cz/soubor/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>.
- Národní bezpečnostní úřad [online]. 2005 [cit. 2011-02-23]. Úplné znění zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Dostupné z WWW: <http://www.nbu.cz/_downloads/pravni-predpisy/container-nodeid-604/412-2005-po-11-2011---.pdf>.
- Národní knihovna ČR [online]. c2009 [cit. 2011-02-23]. KTD - Česká terminologická databáze knihovnictví a informační vědy (TDKIV) . Dostupné z WWW: <http://aleph.nkp.cz/F/?func=file&file_name=find-b&local_base=ktd>.
- POŽÁR, Josef. Informační bezpečnost. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005, 311 s.
- Přístupnost.cz [online]. 2007 [cit. 2010-08-16]. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. Dostupné z WWW: <http://www.pristupnost.cz/zakon-365-2000-sb-o-informacnich-systemech-verejne-spravy/>.
- ÚOOÚ [online]. Zákon č. 101/2000 Sb., o ochraně osobních údajů. c2000-2010 [cit. 2010-08-16]. Dostupný z WWW: <www.uoou.cz/uoou.aspx?menu=4&submenu=5>.
- ÚOOÚ [online]. Zákon č. 480/2004 Sb., o některých službách informační společnosti. c2000-2010 [cit. 2010-08-16]. Dostupný z WWW: <www.uoou.cz/uoou.aspx?menu=23&submenu=25>.

Děkuji za pozornost.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ