INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

SPECIFIČTÍ UŽIVATELÉ – FIRMY, STÁT

INFORMAČNÍ BEZPEČNOST

10. 4. 2013 KISK FF MU

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

FIRMY A JEJICH ZAMĚSTNANCI

BEZPEČNOSTNÍ POLITIKA

IS ORGANIZACÍ

- Roste tlak na zpřístupnění dokumentů
- Potřeba přístupu bez ohledu na geografickou vzdálenost
- Zabezpečení nikdy 100% – viz „neprolomitelná“ šifra
- *Riziko* je pravděpodobnost, s jakou bude daná hodnota aktiva zničena či poškozena *hrozbou* ve formě konkrétního *útoku*, který zapůsobí přes *zranitelnost* systému. (volně dle Požár, s. 37-38)
- Pro omezení rizik jsou řešení, vhodnější je aplikovat než odepsat elektronický IS

RISK MANAGEMENT

- Ocenění rizik (Risk Assessment) "*proces vyhodnocení hrozeb, které působí na informační systém s cílem definovat úroveň rizika, kterému je systém vystaven. Cílem je zjištění, jsou-li bezpečnostní opatření dostatečná, aby snížila pravděpodobnost vzniku škody na přijatelnou úroveň.*" (Požár, 2005, s. 37)
- Efektivita -> ALE (Annual Loss Expectancy)

$$\mathbf{ALE} = \sum_{|=|}^{n} P_i * c_i,$$

kde p je pravděpodobnost, že během jednoho roku nastane ohrožení, C je ztráta, jestliže k ohrožení dojde, i je pořadí ohrožení, n je celkový počet ohrožení za rok

- Risk management součástí informačního auditu

KLASIFIKACE HROZEB

POMŮCKY ZABEZPEČENÍ

- ISO normy
  - ČSN ISO/IEC 27000 - 27002 - Systém řízení bezpečnosti informací,
  - ČSN ISO/IEC 15408 - Kritéria pro hodnocení bezpečnosti IT,
  - ČSN ISO/IEC TR 13335-1 - 13335-4 - Směrnice pro řízení bezpečnosti IT,
  - ISO/IEC TR 13335-5 - Guidelines for the management of IT Security, Management guidance on network security
- Hodnocení důvěryhodnosti systému
  - TCSEC - Trusted Computer System Evaluation Criteria, tzv. Orange Book
  - ITSEC - Information Technology Security Evaluation Criteria + evaluační manuál ITSEM
  - CTCPEC - Canadian Trusted Computer Product Evaluation Criteria
- Metodiky a softwarová řešení
  - CRAMM
  - Cobra
  - DRAMBORA

KROKY PROCESU ŘEŠENÍ BEZPEČNOSTI

1. Cíle a strategie řešení informační bezpečnosti.
2. Analýza rizik informačního systému.
3. Bezpečnostní politika organizace.
4. Bezpečnostní standardy.
5. Implementace informační bezpečnosti.
6. Monitoring a audit.

- BS-7799 British Standard Institute a ISO/IEC 17799 pro řízení informační bezpečnosti a certifikace systému ISMS)

BEZPEČNOSTNÍ POLITIKA FIRMY

- Závazný písemný dokument schválený nejvyšším vedením pro celou organizaci a všem zaměstnancům známý
- Postupy pro předcházení a řešení bezpečnostních problémů – zaměstnanec má postupovat „podle příručky“ nejlepším možným řešením (nemělo by dojít k jeho chybě)
- Vznik dlouhý a složitý – obsah musí být dlouhodobě platný, tím obecný (např. neřeší postupný postup skartace, ale že proběhne a pro co)
- OECD vytvořila seznam doporučených principů Guidelines for the security of information systems

PRO ZAVEDENÍ MUSÍ BÝT UPRAVENO (POŽÁR, S. 101)

- „Požadavky na bezpečnost počítačů (HW bezpečnost, zabezpečení přístupu, dostupnost dat a informací, jejich důvěrnost, viry, zásady pro uživatele).
- Správa dat (požadavky na správu dat, definice pojmů, zásady bezpečnosti dat neelektronické formě).
- Provoz s uvedením zásad, zodpovědnosti za provoz IS, zálohování a obnova SW, hodnocení rizik, vývoj aplikací a audit s pojištěním.
- Řízení přístupu s uvedením zásad, odpovědnost za řízení přístupu, fyzická a logická bezpečnost, problematika virů a červů.
- BP počítačové sítě zásady bezpečnosti a účelu sítě, pravidla provo-zu na síti.
- Bezpečnost datových přenosů odpovědnost za provoz sítí, logická bezpečnost.
- Osobní odpovědnost správců dat hardwarová a softwarová bez-pečnost, zneužití počítačových prostředků, hlášení bezpečnostních incidentů.
- Právní a etické otázky trestné činy, copyrighty, ochrana osobních dat, etické otázky aj.
- Vzory dokumentů.“

PŘÍKLAD – NARUŠENÍ UTAJENÍ (KRÁDEŽ DAT KONKURENCÍ)

- Lidská hrozba úmyslná i ne (využití sociálního inženýrství), možný nátlak
- Fyzické prostředí či ICT (spyware)
- Primární zdroj konkurence, poslední kdokoli
- Odposlech dat, vč. chráněných informací
- Zabezpečení: správa dat/přístupu, bezpečnostní aplikace, fyzické prostředky, vzdělávání
- Problém nejen u e-IS – musí respektovat informační politika

- Více k CI v ČR – doporučuji článek T. Uhrína na Portálu CI o tom, jaké informace o firmách jsou cílem a jak se k nim dostat (legálně)

PŘÍKLAD – NARUŠENÍ INTEGRITY

- Změna dat či přidání hodnoty k nim
- Poškozen uživatel (chybná data), správce (důvěryhodnost, příp. zákon – jakýkoli z uvedených)
- Lidská hrozba úmyslná (odkudkoli) i ne (vnitřní)
- Zabezpečení: zálohování, fyzické prostředky, ostatní jako prevence

PŘÍKLAD – NARUŠENÍ DOSTUPNOSTI (DOS)

- Forma přerušení
- Cíl program či služba
- Téměř výhradně lidská úmyslná hrozba, zdrojem konkurence
- Zabezpečení: těžké, hl. nastavení HW/SW a bezpečnostní aplikace
- Často jediné řešení počkat, až to přejde

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

FINANCE

INTERNETOVÉ NAKUPOVÁNÍ

- Stále rozšířenější nákupy z e-shopů či e-akcí => téměř vše obvykle za nižší cenu
- Problém v důvěryhodnosti prodejce (falešné zboží či celé e-shopy, nezaslání zboží)
- Propagace i bezpečnostní upozornění od státu i firem

PRAVIDLA PRO BEZPEČNÉ NAKUPOVÁNÍ

- Dle občanského zákoníku možné zboží koupené na dálku do 14 dní vrátit bez udání důvodu
- Nekupovat podezřele levné, ani zbytečně drahé (některé aukce skončí výš než u nového zboží)
- U neověřených prodejců neplatit převodem, ale dobírkou
- Uchovávat doklady o transakci
- Reklamace do 30 dní
- Ověřit si prodejce (viz dále)

UKAZATELE DŮVĚRYHODNOSTI E-SHOPŮ

- Certifikační známky, např.
  - SAOP (Spotřebitelský audit obchodních podmínek) pod SOS (Sdružení obrany spotřebitele)
  - APEK (Certifikát Asociace pro elektronickou komerci) pro kvalitu, obchod či dodání lhůt
  - A další
- V rejstříku certifikovaných obchodů

INFORMACE NA WEBU

- Důvěryhodné poučují zákazníky
- Obvykle kvalitně zpracovaný web na placené doméně a hostingu
- Dostupné údaje:
  - O provozovateli (kontakty, IČO apod.), ideálně se sídlem v ČR
  - O platebních metodách (vč. ceny, obchodních a reklamačních podmínek apod.)
  - O zboží (podrobný popis s jasnou cenou, vč. kompletní dopravy)

PLATEBNÍ METODY

- Na dobírku: při doručení, dražší
- Kartou: rychlejší, vhodné zvláštní kartou (údaje dostupné mnoha) nebo 3-D Secure (jen prostředníku)
- Převodem z účtu: rychle (dle zákona o platebním styku do 24 hodin při příkazu do doby převodů prostředků z banky), možné uspíšit expresní platbou (drahé)
- Platba online: např. PayPal, PaySec, eKonto atd., peněženka pro mikroplatby (bez dalších poplatků a s prostředníkem pro utajení údajů)

E-AUKCE

- Např. Aukro, eBay
- Klíčový počet uživatelů
- Důvěryhodný provozovatel si zakládá na ochranném systému (reputace), přebírá zodpovědnost při problematickém prodeji (např. neodeslané zboží)
- Nutné hlídat finance (cena zboží i odměna portálu), OÚ a vše archivovat

INTERNETOVÉ BANKOVNICTVÍ

- Správa bankovního účtu online
- Předchůddce homebanking s omezeným využitím (přes zvláštní aplikaci)
- Nástupce smartbanking – pružnější, ale problém hl. ve zdrojích aplikací a vytváření bezdrátových sítí (Bluetooth, WiFi)
- Riziko hl. sám uživatel, u banky zabezpečení obvykle na hodně vysoké úrovni

ZÁKLADNÍ BEZPEČNOSTNÍ PRAVIDLA INTERNETBANKINGU

- Hlídání přihlašovacích údajů
- Přihlašování jen na ověřeném zabezpečeném počítači
- Opatrné přihlašování s kontrolou URL a běžností vzhledu (drobnosti) a grafickou klávesnicí
- Nastavení omezení disponibilní částky a výše plateb (nákup, výběr)
- Banky nekontaktují e-mailem (jen výjimečně a kritizováno)
- Pravidelná kontrola účtu, historie přihlášení a transakcí

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

STÁT A ZAMĚSTNANCI STÁTNÍ SPRÁVY

INFORMAČNÍ VÁLKA JAKO NOVÝ A JIŽ EXISTUJÍCÍ PROBLÉM, BUDOUCNOST KONFLIKTŮ NA STÁTNÍ A MEZISTÁTNÍ ÚROVNI

KDY JE STÁTNÍ SPRÁVA CÍLEM?

- Největší správce OÚ
- Množství počítačů a techniky k ovládnutí
- Část či celá může být cílem zesměšnění či útoku od různých skupin (např. změny webových stránek policejní skupiny p. Dastycha hackery ze skupiny CzERT, seznam hacknutých stránek touto skupinou)
- Cílem mohou být i konkrétní zaměstnanci, jako každý jiný
- INFORMAČNÍ VÁLKA

CO TO JE INFORMAČNÍ VÁLKA

- Vždy podoba války podle cíle, který chtěla zasáhnout, dle toho i zbraně
- Konec válek asi ne, ale změna v informační
- Informační válka = bojová činnost využívající informace či ICT nebo proti informacím či ICT
- Různé definice, časté dva přístupy – vylepšení klasických X nová forma války
- Může mít výrazný vliv na vítězství i konvenčně slabší armády
- Lze zasáhnout cíl nehledě na geografii (dříve fronta X týl), tím i stírání rozdílu civilní X vojenské cíle, kvůli menší chráněnosti lze napadnout i civilní infrastrukturu

CO TO JE INFORMAČNÍ VÁLKA (2)

- Cíle informační války: kritické infrastruktury (dodávky energií, vody, informační a komunikační systémy, nouzové služby, zásobování potravinami, státní správa a samospráva…) a kritické informační infrastruktury
- Nízké náklady na zbraně – i menší organizace/osoby X prevence drahá, nutné stále udržovat, i když k ničemu nedojde
- Útok někdy nesnadné rozpoznat – denně tisíce útoků na vojenské cíle bez ambice konfliktu
- Zohledňováno i ve vojenských dokumentech, např. Joint Vision 2020 v USA

TYPY INFORMAČNÍ VÁLKY (DLE LIBICKÉHO)

- Command-and-Control Warfare – zničení vedení či komunikace s ním (i vypnutím el. proudu), vhodné jen poškodit (po zničení nový kanál)
- Intelligence-Based Warfare – zpravodajská válka, shromažďování informací o nepřátelích a chránění o sobě vždy klíčové; např. špionáž, průzkumné akce
- Electronic Warfare – antiradarová, antikomunikační (na úrovni signálů) nebo kryptografie (správně kryptologie)
- Psychological Warfare – manipulace s informacemi, dělení: proti národní morálce, velitelům, vojákům, kultuře; např. i terorismus (zastrašování), vojenské přehlídky (ukázka síly)

TYPY INFORMAČNÍ VÁLKY (DLE LIBICKÉHO) (2)

- Hacker Warfare – výhradně činnost hackerů, oproti cyberwarfare prostředky i fyzické povahy; např. malware, prolamování hesel, DDoS…
- Economic Information Warfare – manipulací získání ekonomické převahy; informační blokáda (např. GPS při válce) X informační imperialismus (ovládnutí trhu)
- Cyberwarfare – čistě v kyberprostoru, dnes jen představa; dělení: informační terorismus (problém v pojmu terorismus), sémantické útoky (falešná data v nepřátelském systému = špatná funkce) simulované boje v kyberprostoru, Gibson warfare (ve virtuálních světech, např. sexuální obtěžování, pomluvy…)

Je Zeitgeist informační válka? - YouTube

MANIPULACE

- Nejen nástroj informační války, časté i v médiích, ale i např. sociální inženýrství
- Nutný správný výběr komunikačních kanálů, záleží na cíli
  - Tradiční média (tisk, televize) pasivní – ideální pro ty, kteří je ovládají (stát)
  - Internet obousměrný – rychlá a levná, i malé skupiny (IRA, Al Qaeda, neonacisté…), monitorování státem nákladné až nemožné, po zablokování či zničení snadné migrovat

MANIPULACE (2)

- Př. ve válce ve Vietnamu manipulace médii – pobouření americké veřejnosti televizními záběry – stažení vojsk
- Většinou každý stát svá média využije pro svůj prospěch, někdy i částečně až úplně nepravdivými informacemi
- Součástí mnoho technik, např.:
  - Dezinformace (dále),
  - Obrazová válka – fotky a video stále vyvolávají pocit pravdy X selekce, naaranžování, korekce…, př. fotka oslav 2. výročí komunistické revoluce (1919), z politických důvodů odstraňováni nepohodlní, v 1967 zbyl jen Lenin
  - Propaganda – nejčastěji masovými sdělovacími prostředky přesvědčování veřejnosti o správnosti vlastního konání nebo ideologie

TECHNIKY MANIPULACE (DLE BOHÁČKOVÁ, S. 56-59)

- Účelová selekce informací
- Řazení informací
- Využití emocí
- Výběr komentátorů
- Kontext sdělení
- Nesrozumitelné zprávy
- Podprahové techniky
- Kombinace výše uvedených

METODY INFORMAČNÍ VÁLKY - DEZINFORMACE

- „Záměrně nepravdivá (falešná, lživá, nesprávná, zkreslená) informace sdělovaná s cílem uvést v omyl a ovlivnit příjemce tím, že ji bude považovat za pravdivou a důvěryhodnou. Rozlišují se dezinformace pasivní (zatajení, zadržení, zpoždění informace) a aktivní (tvorba nepravdivé informace, modifikace původní informace či jejího kontextu).“ (TDKIV)
- Velmi stará a častá vojenská technika, zmatení nepřítele pro získání strategické výhody
- Za studené války zvláštní úřady v obou blocích
- Př. V 80. letech KGB šířila informaci, že virus HIV vznikl v laboratořích USA za účelem záměrné likvidace černošské populace; vědecky podkládáno, zveřejňováno v tisku, cílem diskreditace USA hl. v zemích 3. světa

POUŽITÁ LITERATURA

- BARRETT, Daniel J. *Bandité na informační dálnici*. Vyd. 1. Brno: Computer Press, 1999, 235 s. ISBN 80-722-6167-3.
- BASTL, Martin. Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví. Brno, 2007. 153 s. Disertační práce.
- BITTMAN, Ladislav. *Mezinárodní dezinformace a černá propaganda, aktivní opatření a tajné akce*. 1. vyd. Praha: Mladá fronta, 2000, 358 s. ISBN 80-204-0843-6.
- BOHÁČKOVÁ, Gabriela. Kvalita a objektivita informací v médiích: pravda versus manipulace a dezinformace. Brno, 2006. 120 s. Diplomová práce. Masarykova univerzita, Filozofická fakulta, Ústav české literatury a knihovnictví.
- Europe"s Information Society Thematic Portal [online]. 2009 [cit. 2010-06-26]. Critical Information Infrastructure Protection – a new initiative in 2009. Dostupné z: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm
- HAENI, Reto E. Information Warfare: an introduction [online]. Washington DC: The George Washington University, 1997 [cit. 2013-04-08]. Dostupné z: http://www.trinity.edu/rjensen/infowar.pdf
- JANCZEWSKI, Lech a Andrew M COLARIK. *Managerial guide for handling cyber-terrorism and information warfare*. Hershey PA: Idea Group Publishing, c2005, xiv, 229 p. ISBN 15-914-0550-5.
- JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

POUŽITÁ LITERATURA (2)

- *Joint Vision 2020* [online]. 2000 [cit. 2013-04-08]. Dostupné z: http://www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/joint_vision_2020.pdf
- LIBICKI, Martin. *What Is Information Warfare?* [online]. 1995 [cit. 2013-04-08]. Dostupné z: http://www.afcea.org.ar/publicaciones/libicki.htm
- Ministerstvo vnitra České republiky [online]. 2010 [cit. 2010-06-25]. Pojmy. Dostupné z WWW: http://www.mvcr.cz/clanek/kritickainfrastruktura.aspx
- MLEZIVA, Emil. *Diktatura informací: jak s námi informace manipulují*. 1. vyd. Plzeň: Aleš Čeněk, 2004, 133 s. ISBN 80-868-9812-1.
- MOTEFF, John; COPELAND, Claudia; FISCHER, John. *Critical Infrastructures: What Makes an Infrastructure Critical?* [online]. 2003 [cit. 2013-04-08]. Dostupné z: http://www.fas.org/irp/crs/RL31556.pdf
- POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, 309 s. Vysokoškolská učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.
- UHRÍN, Tibor. *Portál CI* [online]. 24.1.2011 [cit. 2013-04-08]. Jak používat volně dostupné nástroje k základnímu sledování konkurenta: nástin problematiky (v ČR) a příklady. Dostupné z: http://www.portalci.cz/ci-v-praxi/jak-pouzivat-volne-dostupne-nastroje-k-zakladnimu-sledovani-konkurenta-nastin-problematiky-v-cr-a-priklady

Děkuji za pozornost.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ