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

BEZPEČNOST V IP FIRMY A STÁTU

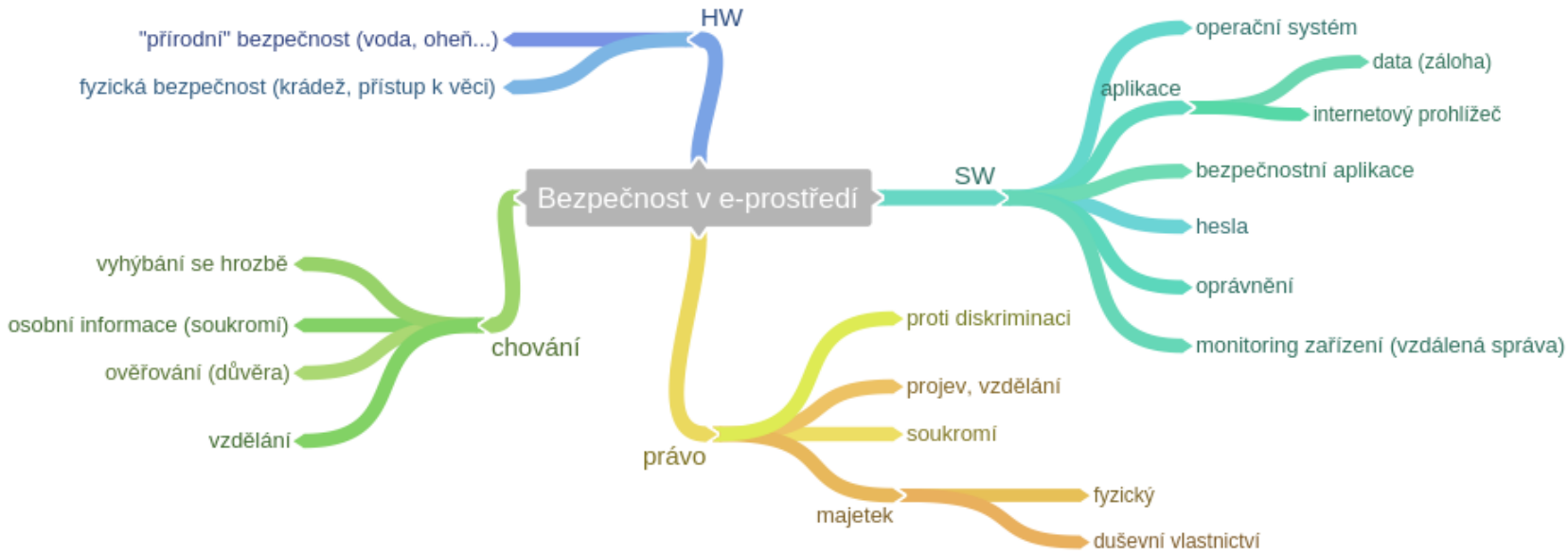
INFORMAČNÍ BEZPEČNOST

KISK FF MU

KOMBI PREZENTACE

- Co jste četli? (publikace)

POSTERY



MOŽNOSTI BĚŽNÉHO VYBAVENÍ

- (automatické) aktualizace všeho SW, vč. OS
- Nastavení, hl. prohlížeče (soukromí, zóny obsahu, Cookies, ActiveX, vyskakovací okna…)
- Uživatelské účty – bezpečná hesla + vhodná oprávnění
- Bezpečné přihlášení (Ctrl+Alt+Del)
- Zaheslovaný spořič, max. po 10 minutách

BEZPEČNOSTNÍ APLIKACE

- Dnes by mělo být běžné vybavení
  - Antivir
  - Antirootkit
  - Antispyware
  - Firewall
  - Antispam
- (rodičovská ochrana)
- Antispam (hl. pro e-maily)
- Antiphishingové nástroje (v balíku, plugin, protokol pro vyhledávač…)

TECHNO OCHRANA - FILTROVÁNÍ

- SWOT analýza
  - 4 skupiny: BlackList, WhiteList, Indikátory, manuální
  - Výhody a nevýhody
  - Proti čemu (ne)pomůže
  - Jaký typ NNO řeší
  - …

ANONYMIZÉRY

- Pohyb po internetu s omezením sdělování informací
- Někteří provozovatelé se zavazují nezaznamenávat žádné aktivity uživatele
- Nutné doplnit vhodným chováním
- Anonymní prohlížení X proxi X Onion Routing

	Cloak (web proxy)	TOR	JonDonym
IP adresa	✗	✓	✓
poskytovatel připojení	✓	✓	✓
geografická lokace	✓	✓	✓
otisk prohlížeče	✗	✓	✓
Java	✗	✓	✓
Flash	✗	✓	✓
historie	✓	✓	✓
cookies	✓	✓	✓
e-tags	✓	✗	✓
Referer	✗	✗	✓
Výsledek	50%	80%	100%

Skoček, 2012

	Ghostery	DNT +	TrackerBlock	TrackMeNot
cookies	✓	✓	✓	✗
pixelové tagy	✓	✓	✗	✗
web bug	✓	✓	✗	✗
Flash	✓	✓	✗	✗
vložené objekty (pluginy)	✓	✓	✗	✗
HTML5	✗	✗	✓	✗
opt-out	✗	✓	✓	✗
hlavička DNT	✗	✓	✓	✗
vyhledávání	✗	✗	✗	✓
Java	✓	✓	✗	✗
Celkem	50%	70%	40%	10%

Skoček, 2012

TECHNOLOGICKÁ OCHRANA

- Nezamezí, ale omezí
- Doplněk prevence – vzdělání, chování

- Když vzdělávání, co vaše texty?

IS ORGANIZACÍ

- Tlak na zpřístupnění dokumentů + odkudkoli + BYOD
- Zabezpečení nikdy 100%, ale pro omezení rizik jsou řešení, vhodnější aplikovat než odepsat e-IS
- **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)

KLASIFIKACE HROZEB

RISK MANAGEMENT

- Risk Assessment = vyrovnání pravděpodobnosti a důsledků problémů s cenou za bezpečí
- ALE (Annual Loss Expectancy)

p = pravděpodobnost výskytu ohrožení

C = ztráta při útoku

i = pořadí ohrožení

n = celkový počet ohrožení

$$ALE = \sum_{i=1}^{n} P_i * c_i,$$

- Součást informačního auditu

PŘÍKLAD – NARUŠENÍ UTAJENÍ (KRÁDEŽ DAT KONKURENCÍ)

- Lidská hrozba úmyslná i ne (SI), 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

- Více k CI v ČR – doporučuji článek T. Uhrína

ÚKOL

- Individuálně nebo skupiny
- Vyberte si známou organizaci (např. KISK)
- Popište vlastní příklad – vymezení hrozby + zhodnocení možných protiopatření z hlediska riskmanagementu

POMŮCKY ZABEZPEČENÍ

- ISO normy (řízení a hodnocení bezpečnosti, zvláštní na IT)
- Hodnocení důvěryhodnosti systému (TCSEC, ITSEC…)
- Metodiky a softwarová řešení (CRAMM, Cobra, DRAMBORA…)

ŘEŠENÍ BEZPEČNOSTI (DLE NOREM)

1. Cíle a strategie
2. Analýza rizik
3. Bezpečnostní politika
4. Bezpečnostní standardy
5. Implementace IB
6. Monitoring a audit

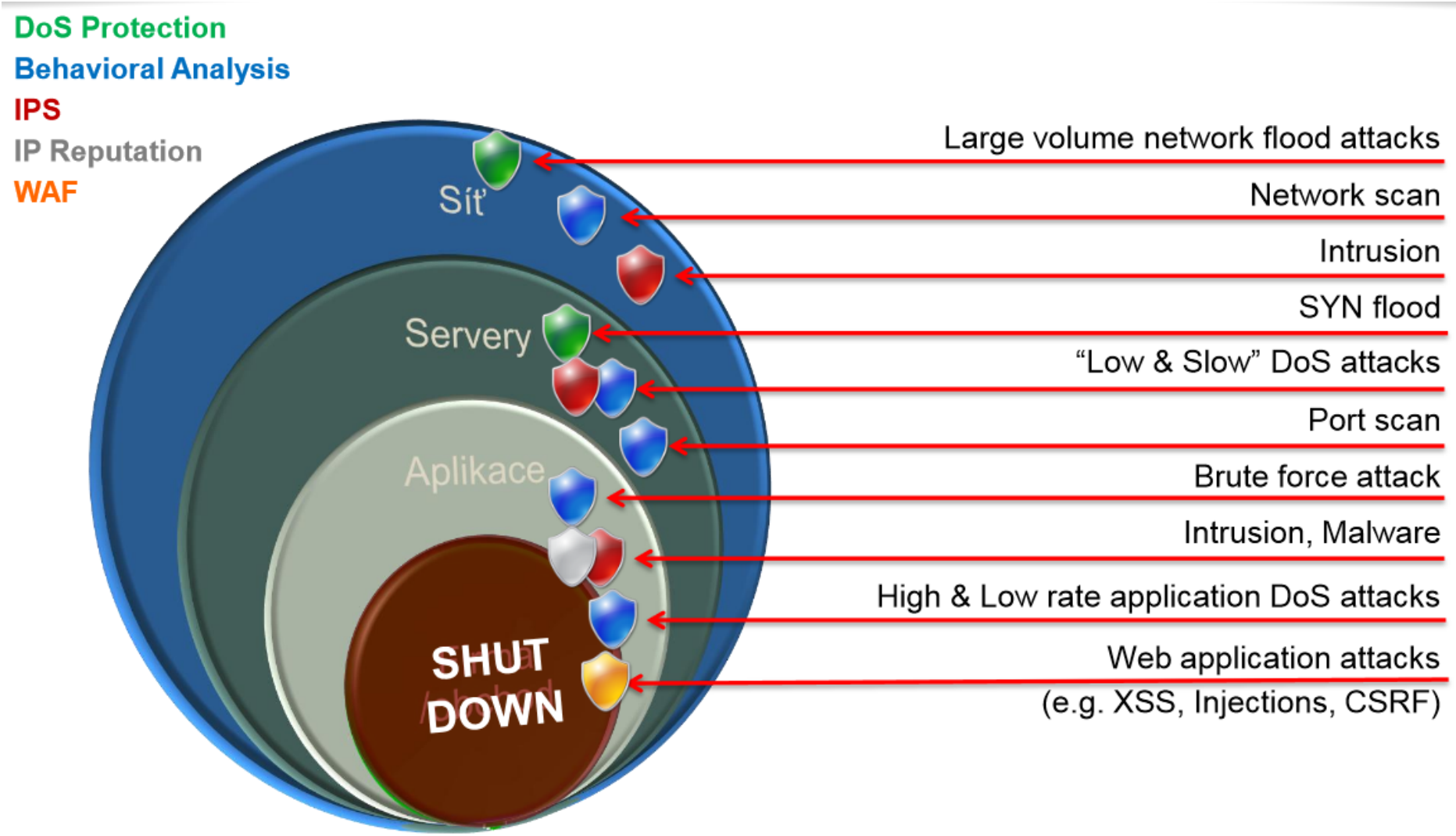
ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

- Účinný od 1. 1. 2015
- Hl. pro IS státu + podstatné pro obyvatele (infrastruktura), vč. soukromých firem
- Opatření specifikována ve vyhlášce č. 316/2014 Sb., o kybernetické bezpečnosti
- Část subjektů povinna hlásit bezpečnostní incidenty (národní CERT, NBÚ) – povinnost mlčenlivosti
- NBÚ vydává varování na webu + ukládá reaktivní a ochranná opatření
- Součástí NBÚ je vládní CERT

OBSAH BEZPEČNOSTNÍ POLITIKY DLE VYHLÁŠKY O KYBERNETICKÉ BEZPEČNOSTI

- systém řízení bezpečnosti informací,
- organizační bezpečnost,
- řízení vztahů s dodavateli,
- klasifikace aktiv,
- bezpečnost lidských zdrojů,
- řízení provozu a komunikací,
- řízení přístupu,
- bezpečné chování uživatelů,
- zálohování a obnova,
- bezpečné předávání a výměna informací,
- řízení technických zranitelností,
- bezpečné používání mobilních zařízení,
- poskytování a nabývání licencí programového vybavení a informací,
- dlouhodobé ukládání a archivace informací,
- ochrana osobních údajů,
- fyzická bezpečnost,
- bezpečnost komunikační sítě,
- ochrana před škodlivým kódem,
- nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí,
- využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí a
- používání kryptografické ochrany.

ÚROVNĚ ZABEZPEČENÍ A ÚTOKŮ NA DOSTUPNOST DLE RADWARE

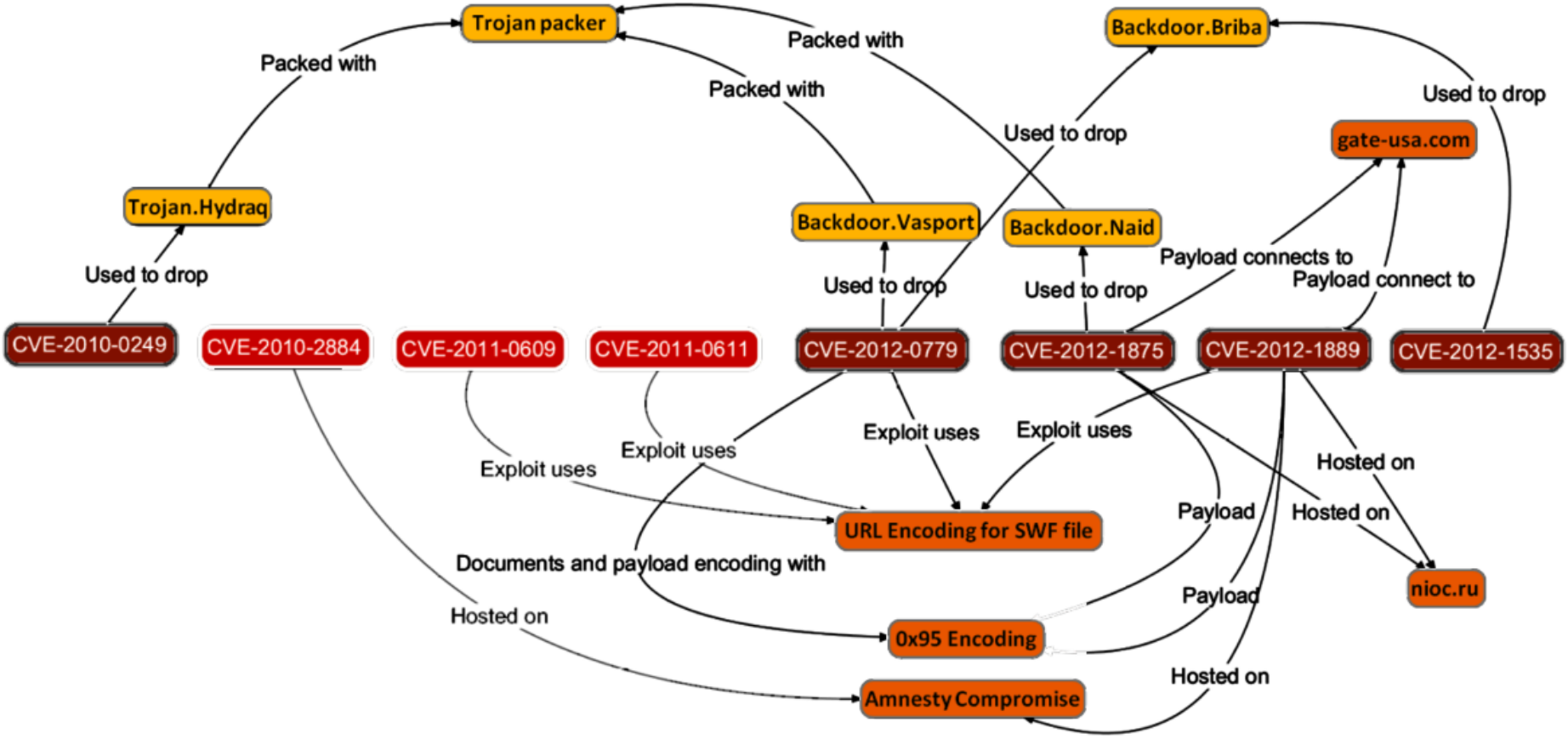


PŘÍKLAD – NARUŠENÍ DOSTUPNOSTI (DOS)

- 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

- Význam útoku roste, stále typičtější multi-vektorové

APT DLE RADWARE



UTM – MOŽNÉ FUNKCE (SOPHOS)

- (NextGen) Firewall
- IPS/IDS
- VPN Gateway (klíčové SSL, IPsec, šifrování, certifikační autority)
- Email Protection (Antivirus, Antispam, Antiphishing, šifrování a podepisování, centrální management klíčů…)
- Web Protection (Antivirus, URL filtr, reputace stránek, přístupové politiky, WAN link balancování)
- Wi-Fi zabezpečení, správa Hotspotů
- Endpoint Protection (antimalware, Host IPS, Device and Port control)

POUŽITÁ LITERATURA

- BARRETT, Daniel J. Bandité na informační dálnici. Vyd. 1. Brno: Computer Press, 1999, 235 s. ISBN 80-722-6167-3.
- 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.
- LASEK, Petr. DoS/DDoS ochrana. RADWARE. *IT Security Workshop* [online]. 18.03.2014 [cit. 2014-04-08]. Dostupné z: http://www.itsw.cz/files/prezentace_itsw14/1_radware_ddos_ochrana.pdf
- Občanský zákoník
- POŽÁR, Josef. Informační bezpečnost. Plzeň: Aleš Čeněk, 2005, 309 s. Vysokoškolská učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.
- ROSIČKA, Jindřich. UTM – Unified threat management. SOPHOS. *IT Security Workshop* [online]. 18.03.2014 [cit. 2014-04-08]. Dostupné z: http://www.itsw.cz/files/prezentace_itsw14/8_is4tech_ict_security_utm0_38.pdf
- 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

KDY JE STÁTNÍ SPRÁVA CÍLEM?

- Největší správce OÚ (bezpečnost, důvěryhodnost IS => eGov)
- Množství počítačů a techniky k ovládnutí
- Část či celá zesměšnění či útok od různých skupin (např. změny webových stránek CzERT, seznam hacknutých stránek)
- (H)acktivismus
- Cílem i konkrétní zaměstnanci, jako jiný
- INFORMAČNÍ VÁLKA

CO JE INFORMAČNÍ VÁLKA

- Informační válka = bojová činnost využívající informace či ICT nebo proti informacím či ICT
- Cíle: kritické infrastruktury = informační a komunikační systémy, dodávky energií, vody, nouzové služby, zásobování potravinami, státní správa a samospráva… - nejen vojenské cíle + bez ohledu na geografii
- (Relativně) nízké náklady X prevence velmi drahá, nutné stále udržovat, i když k ničemu nedojde
- Útok někdy těžké rozpoznat – denně tisíce útoků bez ambice

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

- Viz argumentace a argumentační fauly
- Nutný správný výběr komunikačních kanálů, záleží na cíli
  - Tradiční média pasivní – nutné ovládat
  - Internet obousměrný – rychlá a levná, i malé skupiny, monitorování nákladné až nemožné, snadné migrovat
- Součástí mnoho technik, např.:
  - Dezinformace,
  - Obrazová válka,
  - Propaganda

PŘÍKLADY MANIPULACE

- Nesrozumitelná odbornost: „In fact, few hackers worldwide would disagree with the essential unification of voice-over-IP and public-private key pair.“
- Účelový výběr informací: nehodící se zamlčeno
- Výběr komentátorů: „Když to řekli ViralBrothers, tak to je určitě pravda.“
- Řazení informací: pamatován hl. začátek a konec, směrování rozhovoru, umístění článku na stránce…

CÍLE V MÉDIÍCH

- Informování, učení, ovlivňování a zábava
- Různé cíle tvůrců => důležité srovnání z více zdrojů!
- Kdo tvoří zprávy?
  - PR agentury, tiskové agentury…
  - Vlastník, lobbing => politika, finance, osobní důvody…
  - Občanská žurnalistika => menší vliv zájmových skupin

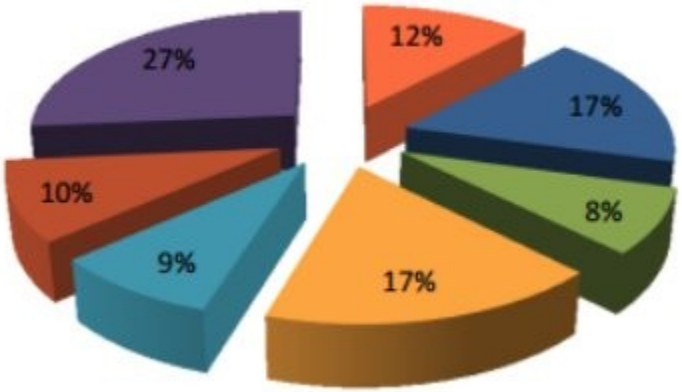
REKLAMA

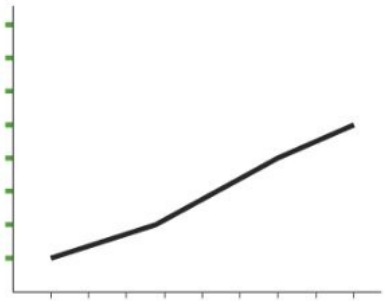
- Jeden z finančních zdrojů
- Zobrazená X začleněná (product placement) => vliv emocí (oblíbený herec, film…)

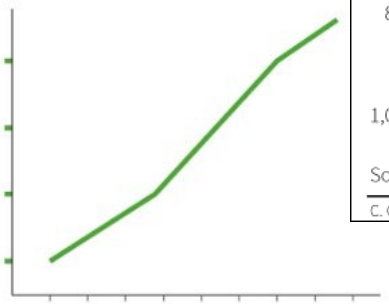
Zdroj: http://www.brandchannel.com/wp-content/uploads/2015/10/big-bang-theory-600.jpg

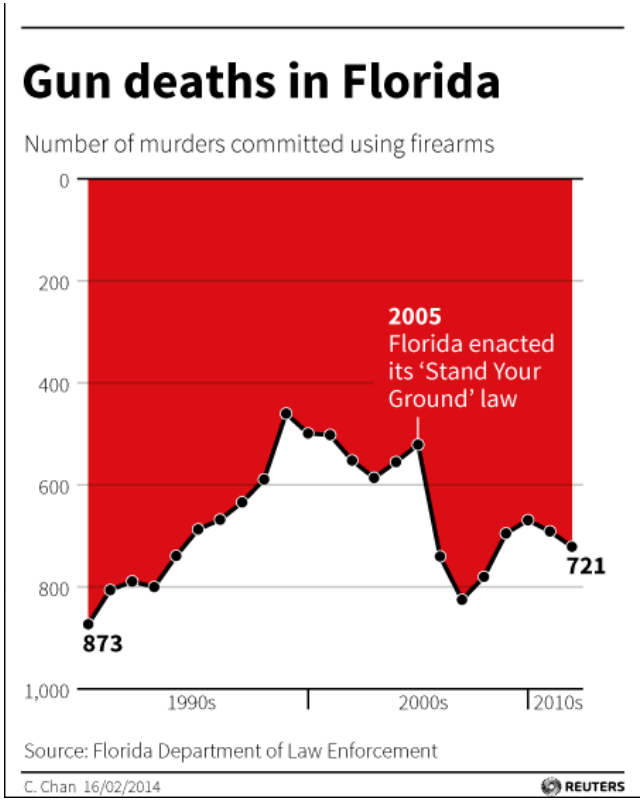
Zdroj: http://www.mediar.cz/prima-nasazuje-novy-serial-ohnivy-kure/

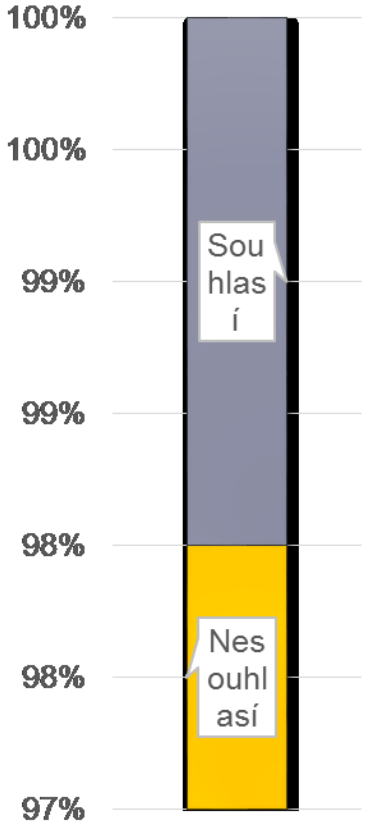
PŘÍKLADY MANIPULACE V GRAFECH











PŘÍKLADY OBRAZOVÉ MANIPULACE

- Ilustrační obrázky, např. inkubátor s čitelnou značkou u článku o onemocnění dítěte (v nespecifikovaném) inkubátoru
- Úprava foto/video, např. politicky nepohodlní z oslav 2. výročí komunistické revoluce (1919)

Ale: pobouření televizními záběry války ve Vietnamu

ÚKOL

- Zkuste najít příklad možné manipulace
  - Média
  - Vyjádření politika
  - Video
  - Infografika
  - Webové stránky
- Kde a co (byste zkusili)

POUŽITÁ LITERATURA

- 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.

POUŽITÁ LITERATURA (2)

- 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.
- 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

ZDROJE OBRÁZKŮ

- https://www.youtube.com/watch?v=i7xdnlxTVXU
- https://is.muni.cz/th/362075/ff_m/tvorba-efektivnich-grafu.pdf
- https://commons.wikimedia.org/wiki/File:Soviet_censorship_with_Stalin2.jpg

DĚKUJI ZA POZORNOST.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ