POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY
FAKULTA BEZPEČNOSTNÍHO MANAGEMENTU

Některé aspekty kybernetické kriminality

Doc. RNDr. Josef POŽÁR, CSc. - děkan

12. 4. 2011

Tato prezentace byla zpracována v rámci Projektu vědeckovýzkumného úkolu č. 4/4 „Informační bezpečnost a kybernetická kriminalita v organizaci“, který je součástí Integrovaného výzkumného úkolu na léta 2010-2015, realizovaný Fakultou bezpečnostního managementu Policejní akademie České republiky v Praze.

1. Kybernetická kriminalita

Kybernetická kriminalita

- Trestné činy proti počítačům (sítím) a pomocí počítače - trestný čin proti integritě, dostupnosti a důvěrnosti (utajení) ICT.
- Jsou to veškeré aktivity proti neautorizovanému čtení, modifikaci zneužití dat (informací) – počítačová defraudace s cílem získat výhodu, peníze apod.
- Trestně právní kvalifikace a důsledky.

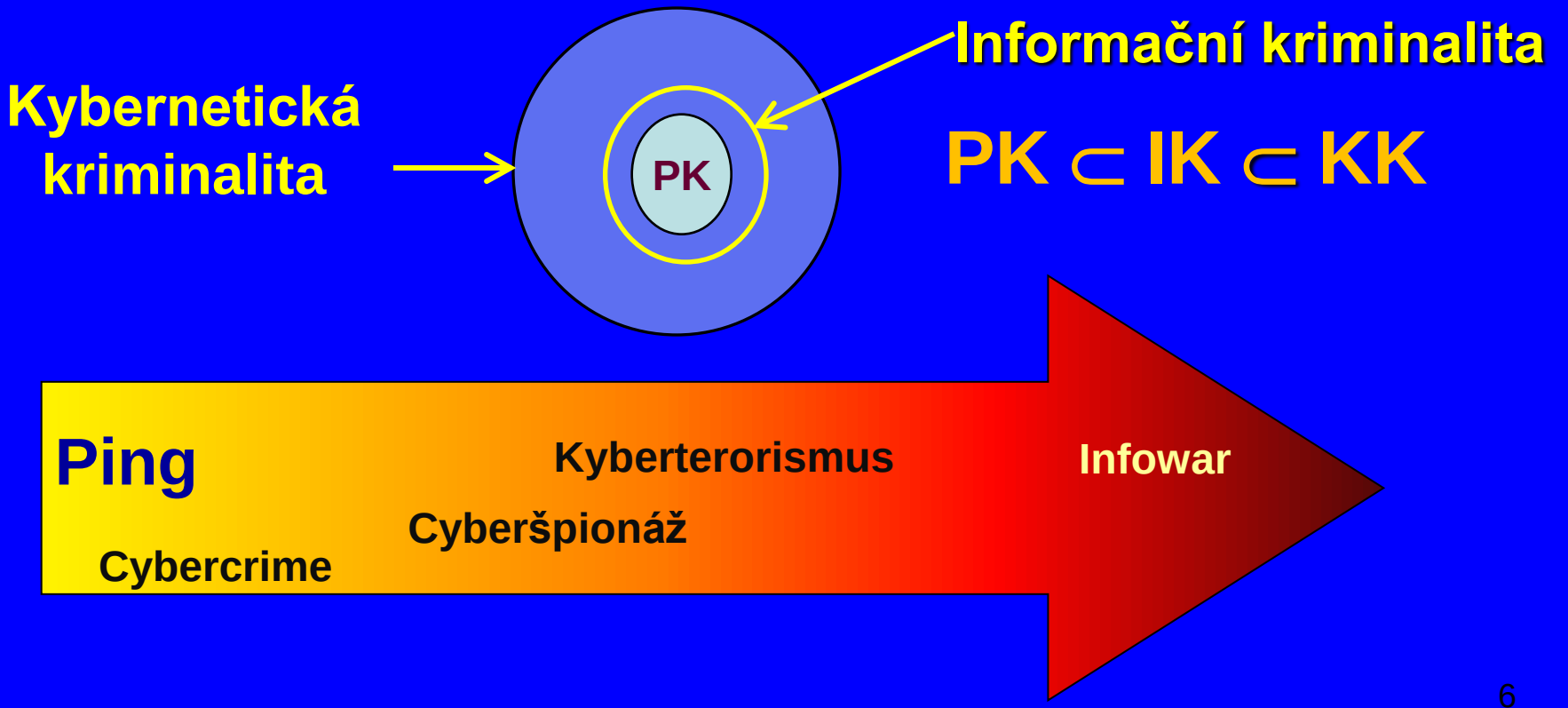
Porovnání klasického a kybernetického zločinu

Parametr	Průměrné ozbrojené přepadení	Průměrný kybernetický útok
Riziko	Pachatel riskuje zranění	Bez rizika fyzického zranění
Zisk	Průměrně 3-5000 USD	Cca 50-500 000 USD
Pravděpodobnost dopadení	50-60% šance dopadení	10% šance dopadení
Pravděpodobnost odsouzení	95% šance odsouzení při dopadení	15% dopadených soudně stíháno, z toho 50% odsouzeno
Trest	5-6 let v průměru, pokud pachatel nikoho nezabil	2-4 roky v průměru

Zdroj: Kybernetická kriminalita, Václav Jirovský

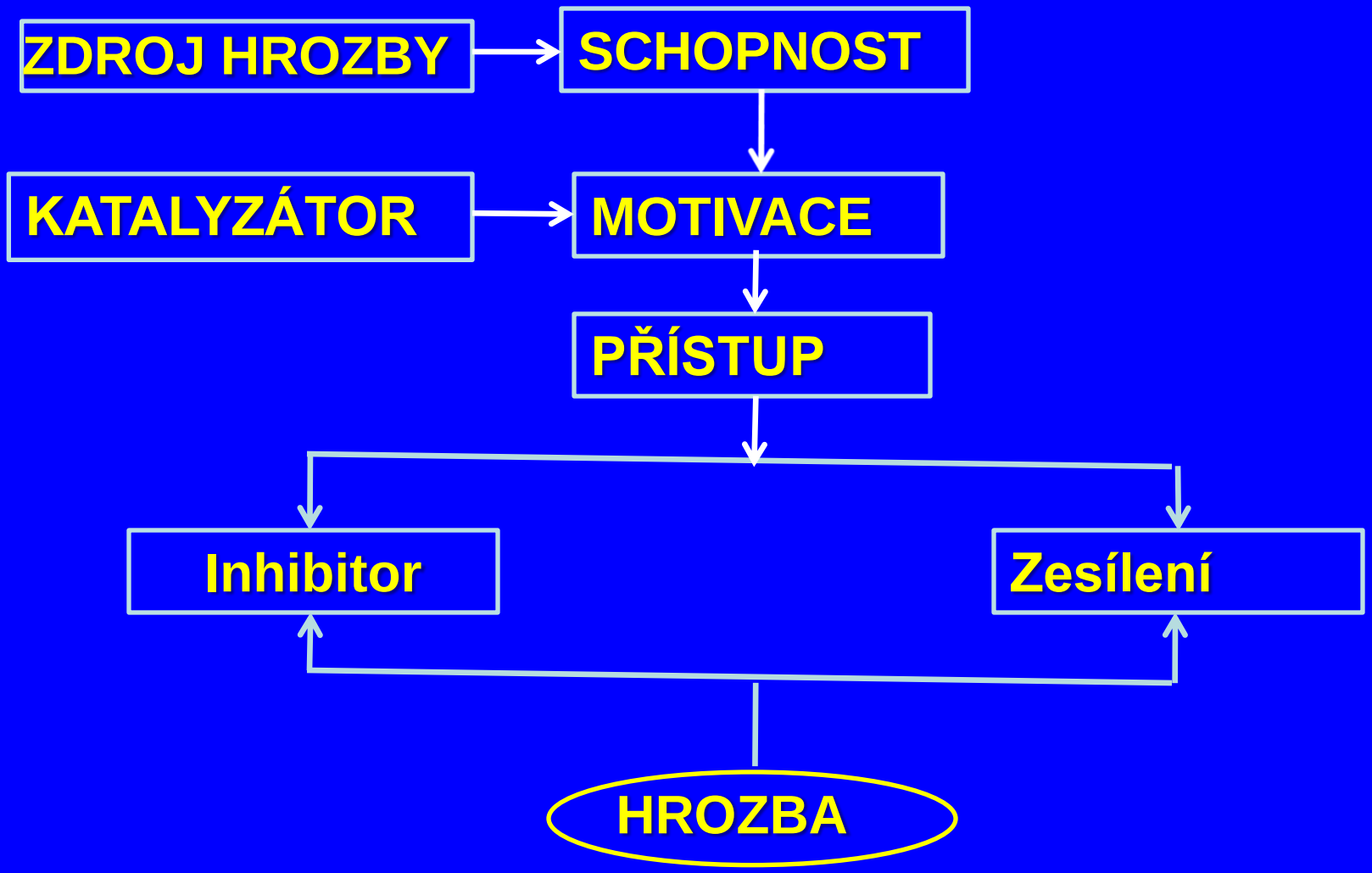
Kybernetická kriminalita

Počítačová, informační a kybernetická kriminalita



Kybernetická kriminalita

Vazby a komponety hrozeb KK



Jones, Andrew. *Identification of a Method for the Calculation of Threat in an Information Environment*. Unpublished, April 2002

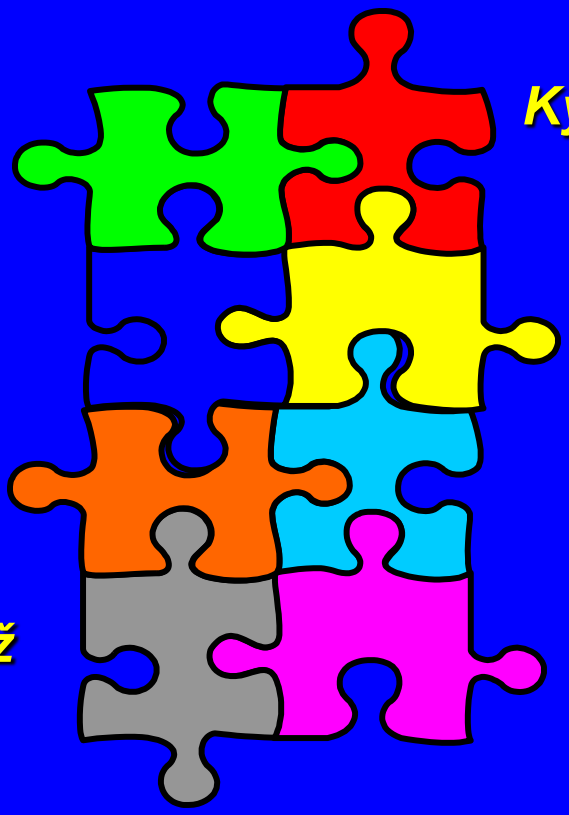
2. Typy útoků kybernetické kriminality

Typy kybernetické kriminality

Kybernetický kontraband

Kybernetické pronásledování

Kybernetický neautorizovaný vstup



Kyberterorismus

Kybernetický podvod

Kybernetická pornografie

Kybernetické praní špinavých peněz

Kybernetická krádež

Kybernetický vandalismus

Kybernetická pomluva

Hrozby (threats)	Prostředky (means)	Cíle (targets)	Konečné cíle (ends)
Teroristické organizace	Vraždy	Státní organizace	Asymetrický konflikt
Teroristické organizace	Kybernetický útok	Bankovnictví a finance kritická infrastruktura	Bezpečnostní výhoda
Pracovníci informační války	Informační operace	Obchod	Ekonomická výhoda
Státní terorismus	Infowar	Obyvatelstvo, vlády	Politická změna
Počítačoví hackeři	Logické bomby	Kritická infrastruktura	Politický vliv a zisk
Počítačoví hackeři	Kybernetický útok	Firmy, finance	Finanční zisk
Státem sponzorovaný terorismus	Přímá akce	Kritická infrastruktura	Politická změna

incidenty

útoky

události

Útočníci	Nástroje	Zranitelnost	Akce	Cíle	Důsledek	Účel
hackeři	fyzický útok	návrhy	zkoušky	účty	vniknutí	změny statusu
špioni	výměna informací	implemen-tace	scaning	procesy	prozrazení informací	politický zisk
razie	skripty	kofigurace	záplavy	data	zničení informací	finanční zisk
profesionální zločinci	anonymní uživatel		autenti-zace	kompo-nenty	DoS	
vandalové	toolkit		bypass	počítač	DDoS	
cestovatelé	distribuční nástroje		čtení	sítě	krádež zdrojů	
	datové zdroje		kopie	výměny dat		
			krádež			
			výmaz			

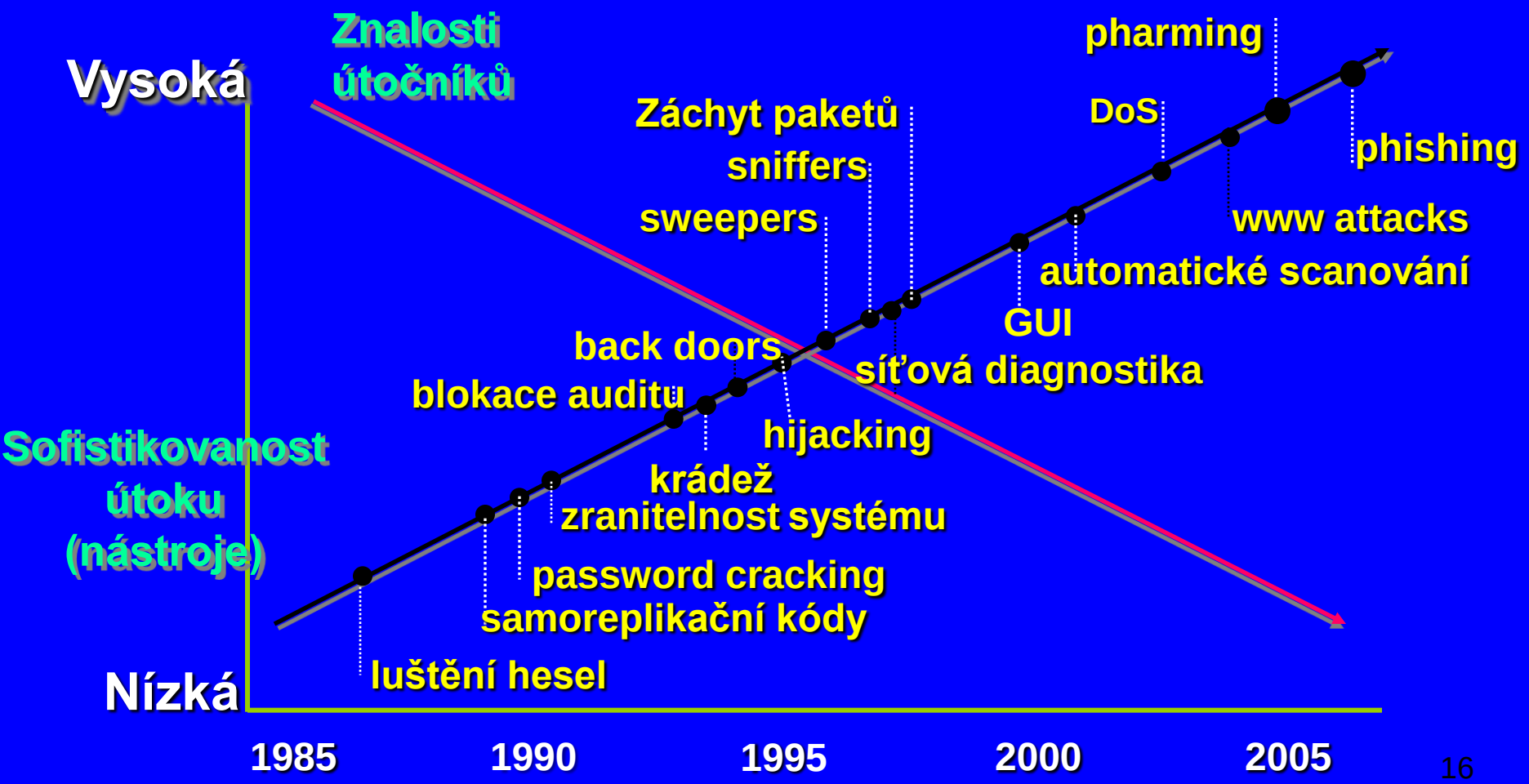
3. Pachatelé kybernetické kriminality

Pachatelé kybernetické kriminality

- Kiddiots/skript - Kiddies - *nejnižší úroveň*
- Tvůrce virů
- Příležitostný hacker
- Profesionální hacker
- Phisher
- Nájemný kybernetický zločinec – *nejvyšší cena*
- Organizované skupiny pachatelů kybernetické kriminality

Pachatelé kybernetické kriminality

Sofistikovanost útoku a znalosti útočníků

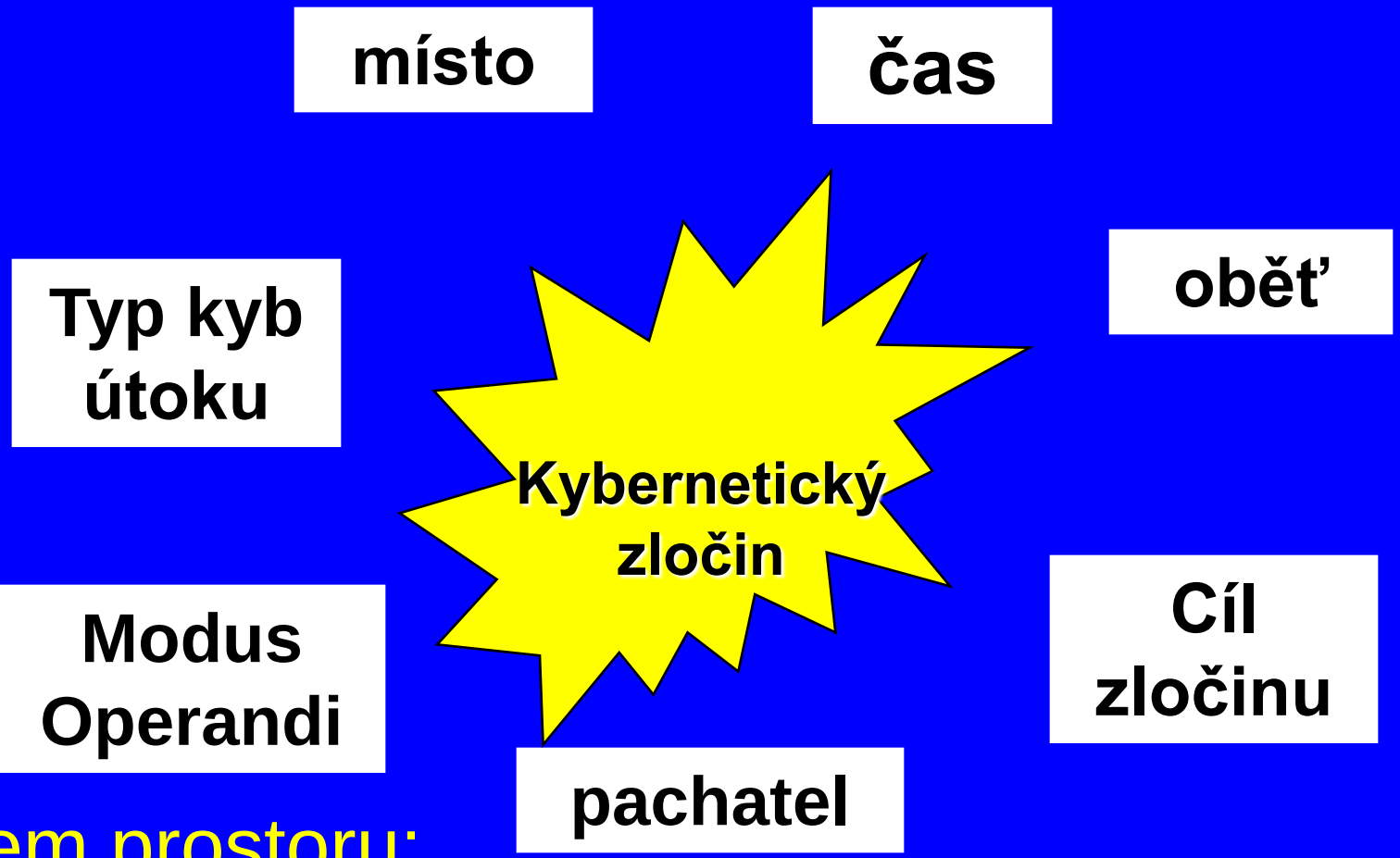


Cyberthreat Hype Cycle

IT Wisdom

Entire contents © 2005 Gartner, Inc. All rights reserved.

Gartner



Problem prostoru:
mapa příznaků
a vymezení objektu trestného činu

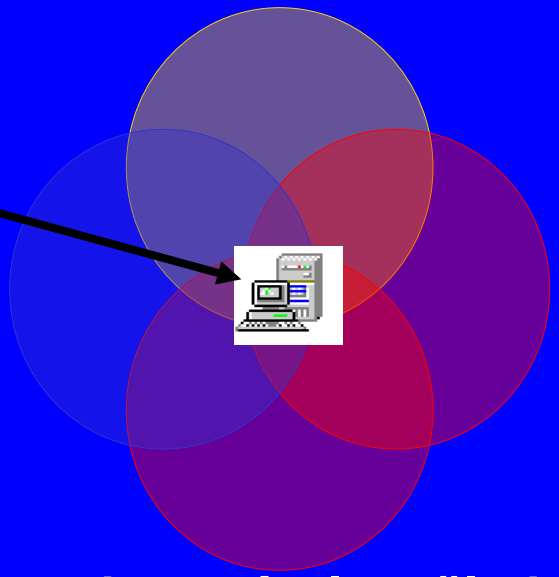
Kategorie otázek vyšetřování kyber. kriminality

- What (the data attributes)
- Why (the motivation)
- How (the procedures)
- Who (the people)
- Where (the location)
- When (the time)
- Wherewith (the means)

Charakteristika digitálního místa činu

Co je zde, ale nemělo být?

Co je zde?



Co zde není?

Co zde není, ale mělo být? (tj. data, zbytky dat, registry)

Co bylo změněno a je různé, ale ještě je zde? (tj. skrytá data, steganografie)

Čím bylo pohnuté, ale dosud zde je?

4. Trendy kybernetické kriminality

Trendy kybernetické kriminality

- Útočníci povedou sofistikovanější útoky za účelem finančního zisku.
- Nárůst hrozeb elektronickému obchodu.
- Zvyšuje se počet útoků proti webovým aplikacím.
- Zvýšení útoků pomocí červů (Slammer).
- Zvyšující se počet útoků na slabá místa systémů.
- Zvyšující se počet škodlivých kódů.

Programová bezpečnost

- Nové delikty lze páchat pouze on-line.
- Útoky pomocí škodlivých kódů, virů pod. za účelem obohacení, zisku.
- Rostoucí ohrožení mobilních komunikačních systémů a zařízení (virus Cabir).
- Zneužívání sítí Wi-Fi.
- Masové rozšíření spammingu pomocí trojských koní a botů.
- Pokročilé webové hrozby (Java scripty aj.).
- Mobilní platformy.

- Rozšiřování tzv. phishingu, spywaru a hijackeringu (přesměrování prohlížeče na placené stránky).
- Spamy, adware, viry aj.

Odcizení identity (identity theft)

- Krádež dokumentů a platebních karet.
- Odcizení hesel.
- Kybernetický útok na data a protokoly (DoS, DDoS).

Komunikační bezpečnost

- Odposlech a modifikace dat.
- Sdílení dat a programů.
- Technologická složitost.
- Neznámý bezpečnostní perimetr.
- Množství zranitelných míst.
- Neznámá přenosová cesta.
- Nárůst počtu robotických sítí.

5. Závěr

Výzkum

- V rámci bezpečnostního výzkumu Ministerstva vnitra úspěšně probíhá projekt „Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů ČR“. Naplánován do roku 2010, je žádoucí v projektu pokračovat i po roce 2010. Některá témata výzkumu.
- Problematika CSIRT (Computer Security Incident Response Team – středisko koordinace reakce na kybernetické incidenty) (zvláště budování standardů a hierarchie řešení bezpečnostní problematiky v sítích).

- Bezpečnostní a spolehlivostní analýza rozsáhlých sítí.
- Standardizace programového vybavení pro forenzní analýzu.
- Zkoumání sociálně-psychologických faktorů kybernetické kriminality.
- Stav, úroveň, struktura a dynamika ohrožení ČR kybernetickou kriminalitou a kyberterorismem.

Vzdělávání a výcvik

- Vysokoškolské vzdělávání Univerzitní – veřejné VŠ – obor informatika.
- PA ČR v Praze:
  - Ochrana počítačových dat.
  - Bezpečnost informací.
  - Manažerská informatika.
  - Kriminalistická technika, taktika a metodika aj.
- Specializační kurzy pro policisty, vyšetřovatele, experty apod.

Doporučení

- Zintenzivnit mezinárodní spolupráci Policejních sborů.
- Harmonizovat právní normy – jednotná legislativa alespoň v EU.
- Potřeba vzdělávání manažerů podniku v IT.
- Výchova X útoky zevnitř podniku

pozar@polac.cz