Taxonomie kybernetických hrozeb

Václav Jirovský
Dopravní fakulta
České vysoké učení technické, Praha
Česká republika

EUROPEN 2008, Rožmberk nad Vltavou

Co zahrnuje taxonomie

- taxonomie = klasifikace, kategorizace
- jsou používány některé významné vlastnosti
  - specifikace významných vlastností
  - vytvoření taxonomického systému
- taxonomie kybernetických hrozeb (terorismus, kriminalita)
  - podle účastníků, efektu a cílů
    - populace, třídy kyberterorismu, účastníci
  - podle charakteru hrozby
    - základní hrozby, aktivační hrozby, podkladové hrozby
  - podle technologických vlastností (síťový model)
    - umístění v OSI/ISO architektuře, interaktivita etc.

Taxonomie podle účastníků, efektů a cílů

Populace kyberprostoru

- **virtuální osobnosti**
  - projekce reálné osobnosti člověka do kyberprostoru (život pod přezdívkou, náchylnost k internetu)
- **virtuální komunity**
  - globální seskupení virtuálních osobností bez omezení hranicemi států, svázaných společnými myšlenkami, vírou, politickým názorem, zkušenostmi, zájmem etc.
    - častá je politická nebo náboženská motivace
    - skupiny patřící ke stejnému hnutí ve světě
- **virtuální korporace**
  - virtuální organizace v kyberprostoru zaměřená na stejný tržní segment
  - volná organizace nebo smluvní vazba

Rozdělení terorismu v kyberprostoru

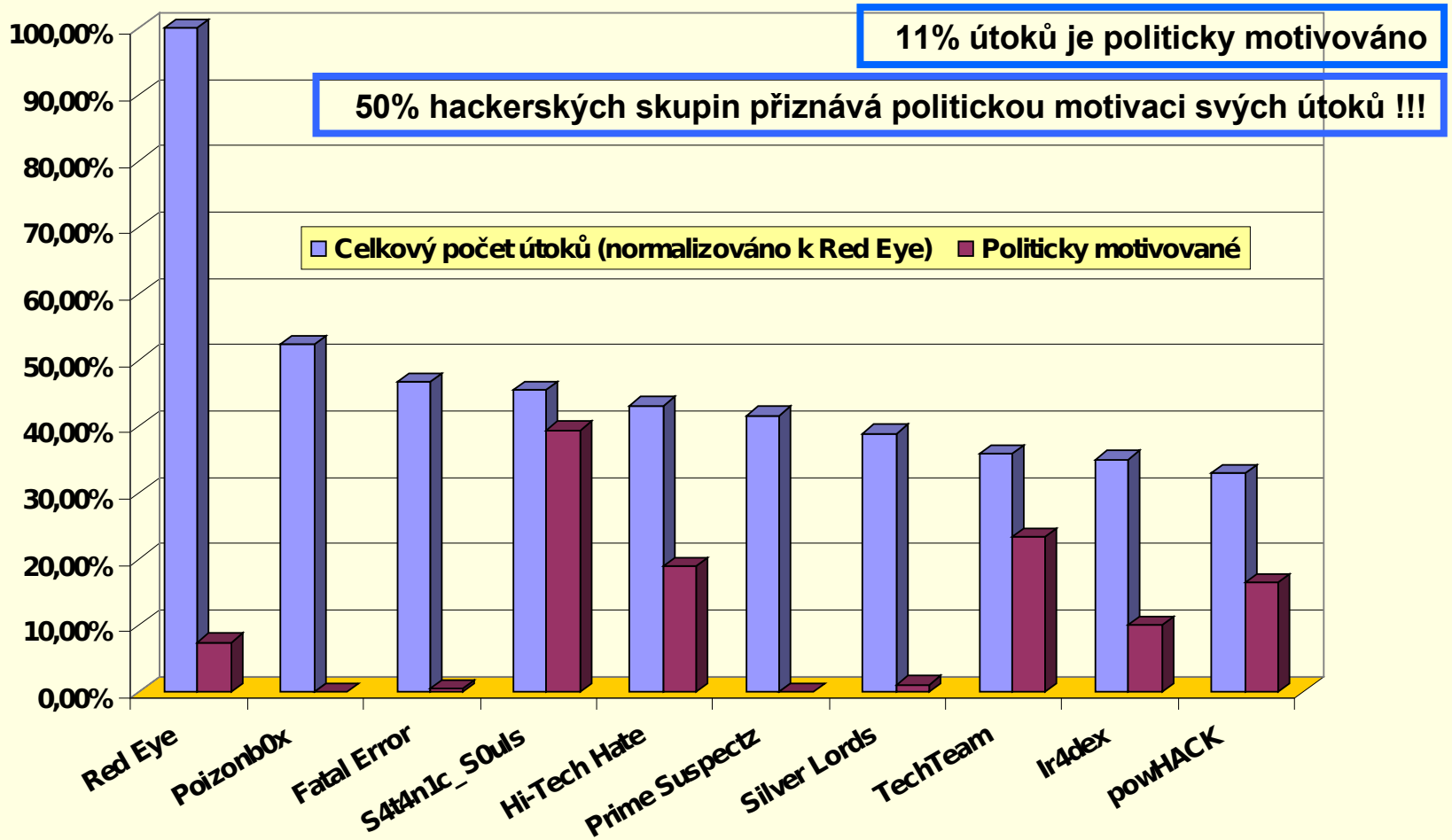
- politický terorismus
  - kyberprostor je užíván nejenom jako bitevní pole, ale i pro koordinaci akcí a pro komunikaci teroristických skupin
  - separatismus
  - sektářský terorismus (kulty)
  - revoluční terorismus (buřičský, štvavý)
  - náboženský terorismus, zvl. fundamentalismus
- psychotický terorismus
  - personální (individuální) terorismus
  - pocit satisfakce u mentálně nemocného jedince
- kriminální terorismus
  - nezahrnuje kriminální chování v kyberprostoru
  - individuální aktivity – např. cyberstalking, cyberbullying
  - aktivity organizovaného zločinu, např. kybernetické výpalné

často doprovází tradiční formy terorismu

Kdo jsou útočníci?

- hackerské skupiny najaté pro uskutečnění útoku
  - skupiny H4H
  - založené na regulérním obchodním vztahu (objednávka/faktura)
- zvláštní jednotky teroristických buněk, zvláštní vojenské jednotky
  - útok se dá obtížně odlišit od útoků H4H
  - vysoká kvalita útoků, specifické strategie, specifické cíle
- ideologičtí sympatizanti
  - prezentují vyjádření svých sympatií k ideologickému hnutí (nejčastěji formou defacementů)
  - pracují odděleně a samostatně, latentní hrozba skrytá v možnosti jejich účelového spojení
- hledači vzrušení
  - individuální útočníci přitahovaní reálným konfliktem nebo konfliktem v kyberprostoru,
  - nejsou vedeni žádnou ideologií, náboženstvím nebo jiným filosofickým zázemím,
  - hlavním motivem je jejich exhibicionismus

Politická motivace kybernetických útoků



Nepřímý kyberterorismus

- terorismus spojený s IT bez přímého vztahu k existující IT infrastruktuře
  - je příznačně svázán s vývojem „informačního věku“, informatikou a telekomunikacemi
  - pocit svobody podporovaný vnímáním volnosti na internetu
  - založen na obecně nízké úrovni úsudku o kvalitě předávané informace
- používající sítě IT jako nástroj
  - mediální terorismus
  - hacktivismus
- zneužití procesů a výkonu IT
  - procesní terorismus
  - IT governance

Taxonomie podle charakteru hrozby

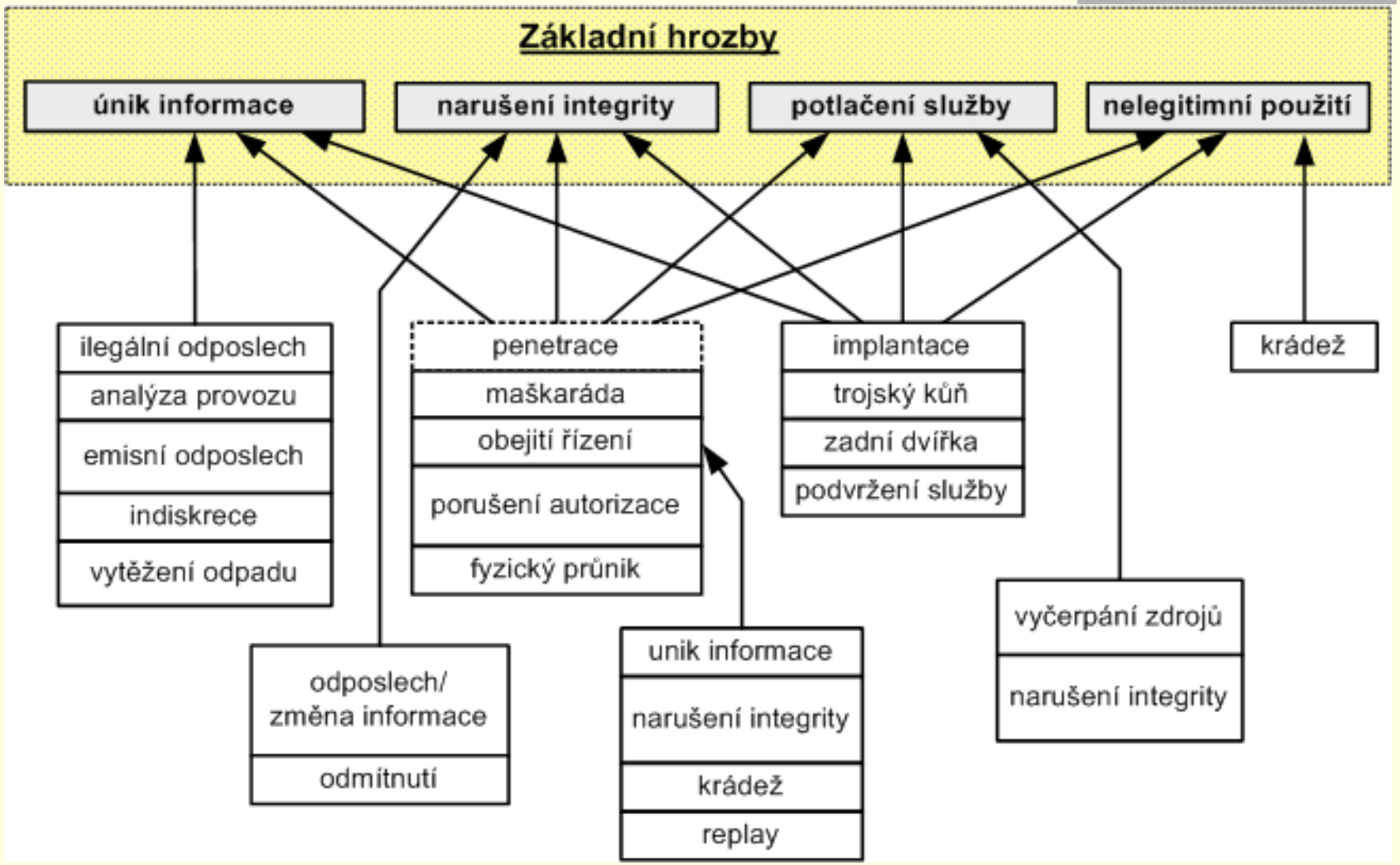
Charakter hrozby

- základní hrozby
  - únik informace
    - je získána utajovaná informace
  - narušení integrity
    - vliv na konzistenci dat nebo možná modifikace uložené informace
  - potlačení služby
    - také jako potlačení přístupu ke službě
  - nelegitimní použití
    - neautorizovaný přístup, krádež
- odrážejí čtyři hlavní hlediska bezpečnosti informačního systému

Aktivační a podkladové hrozby

- aktivační hrozby vedou k bezprostřednímu vytvořené některé ze základních hrozeb
  - penetrační hrozby
    - maškaráda
    - obejití řízení
    - narušení autorizace
  - implantační hrozby
    - trojský kůň
    - backdoors
- podkladové hrozby mohou vést k realizaci několika základních hrozeb

Vzájemná závislost hrozeb



Taxonomie založená na síťovém modelu

Taxonomie - síťový model (1)

- založena na síťových charakteristikách útoku*

3) charakter útoku
   i. pasivní
   ii. aktivní
4) účel útoku
   i. kompromitace dat
   ii. narušení integrity dat
   iii. degradace systému
5) spouštěcí událost
   i. specifický signál vydaný cílem
   ii. specifická událost uvnitř cílového systému
   iii. bezpodmínečné spuštění

*vychází z „Attack from Internet“, zone-h, 2004

Taxonomie - síťový model (2)

1) požadavek na zpětnou vazbu
   i. zpětná vazba je součástí útoku
   ii. zpětná vazba není nutná
2) pozice útočníka vzhledem k cíli
   i. intrasegmentová
   ii. intersegmentová
3) použitá vrstva ISO/OSI
   i. fyzická
   ii. linková, síťová nebo transportní
   iii. aplikační vrstva
4) pozice útočníka vůči cílovému systému
   i. uvnitř systému (insider)
   ii. mimo systém

SHRNUTÍ

Shrnutí

- taxonomie podle účastníků, efektu a cílů
  - popisuje spíše sociální a psychologický pohled na kybernetickou hrozbu,
  - vhodná pro vytvoření profilu útočníka
- taxonomie podle charakteru hrozby
  - popisuje technologii útoku
  - vhodná pro nastavení bezpečnostní politiky
- taxonomie založená na síťovém modelu
  - popisuje architektonický pohled na útok
  - vhodná pro nastavení IDS systémů nebo podobných opatření
- uvedené taxonomie nejsou jediné!