



Od teorie k praxi víceúrovňové bezpečnosti

Ing. Milan KNÝ, CSc. – katedra managementu a informatiky

Doc. RNDr. Josef POŽÁR, CSc. – děkan

21. 6. 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.

Bezpečnostní management

- se jeví jako **téma moderního managementu**, které se zabývá tvorbou, udržením a obnovením optimální bezpečnostní situace objektů,
- stává se samostatnou **speciální praktickou vědní disciplínou** jako jedna z množiny **bezpečnostních věd**,
- představuje **činnosti, procesy a funkce**, kterými (bezpečnostní) manažeři čelí hrozbám, jejich odvracení, zmírnění, eliminaci a recidivám.

Systémová bezpečnost

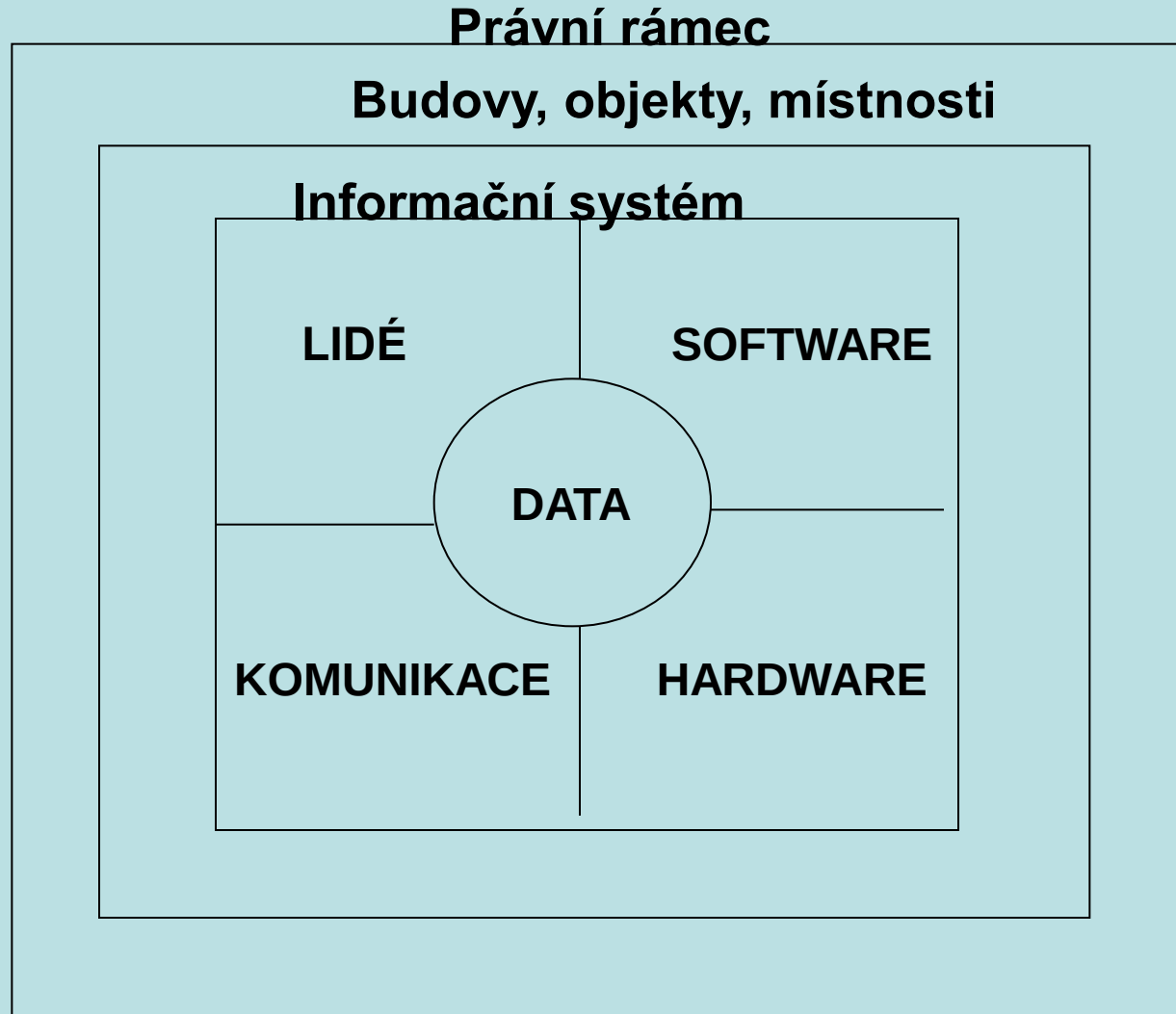
Systémový přístup k řešení bezpečnosti vede manažery k celistvému myšlení, provázanosti prvků, modelové relevanci i k účelové redundanci.

- Systémová bezpečnost je řízena bezpečnostním managementem v rámci funkční vrstvy nebo napříč vrstev v modelovém komplexu.**
- Systémové řešení je ideál a důvod konvergence (k harmonii, funkční ucelenosti).**

Informační bezpečnost

- Je to ochrana objektů, entit v organizacích, která je orientována se zvláštním zřetelem na ochranu dat, bezpečnému zacházení s informacemi prostřednictvím informačních procesů a informačních a komunikačních technologií.
- Informační bezpečnost je jedna z významných součástí systémové bezpečnosti a odráží mj. také fyzickou (energeticko-fyzikální a personální) bezpečnost.

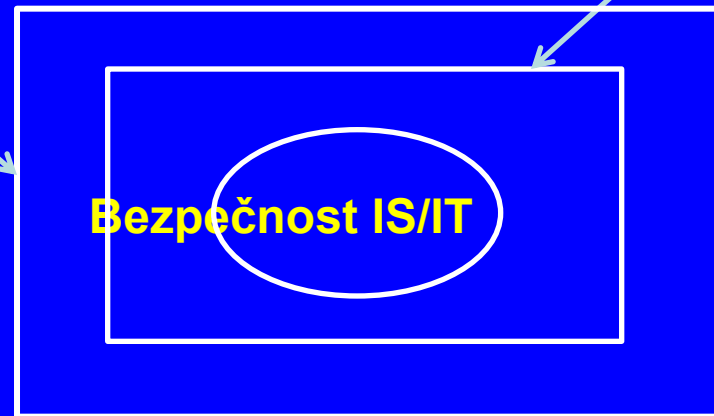
Informační bezpečnost



Vztah úrovní bezpečnosti v organizaci

Bezpečnost organizace

Informační bezpečnost

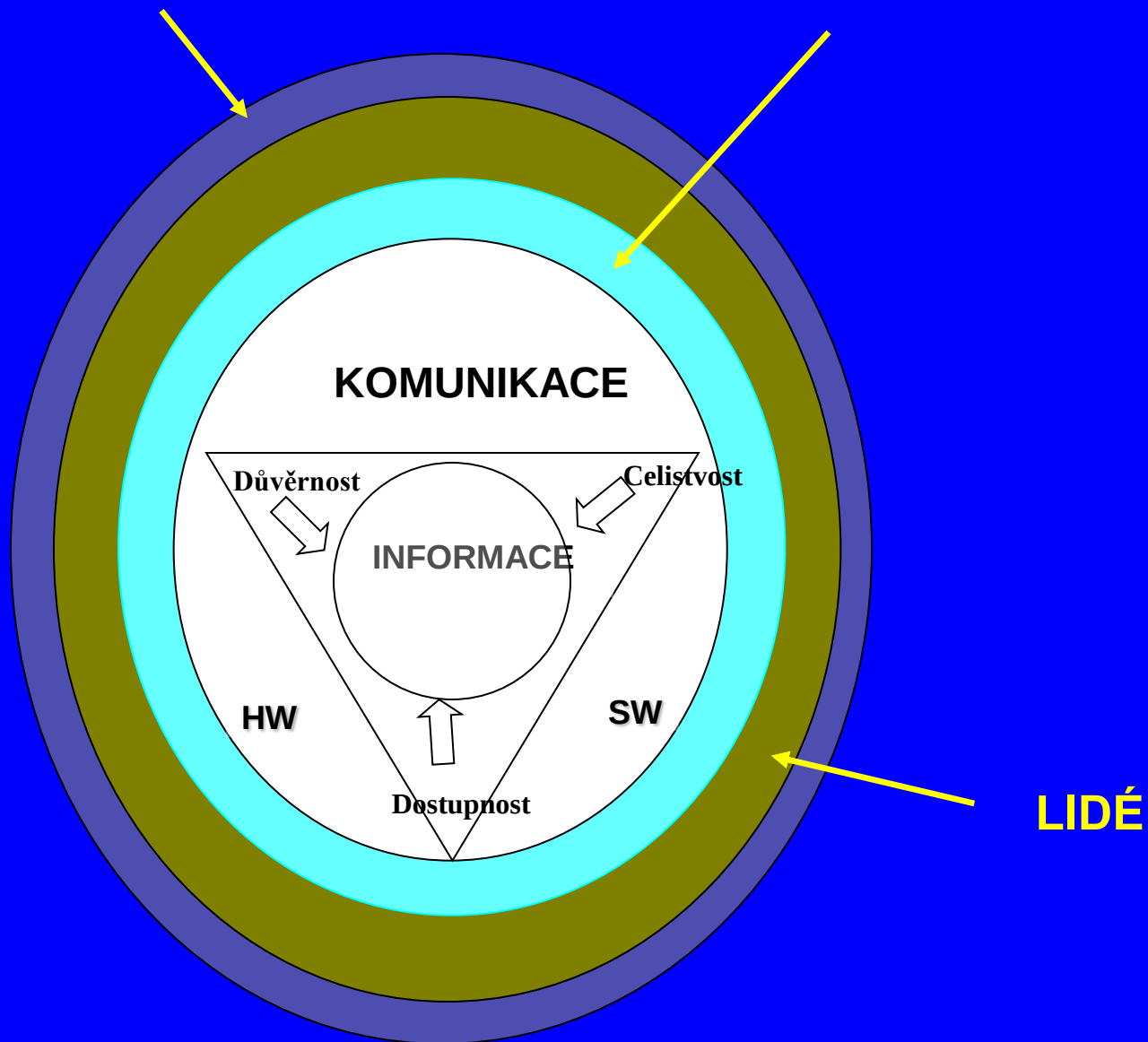


Úrovně informační bezpečnosti

- **Personální bezpečnost**
- **Fyzická bezpečnost**
- **Administrativní a režimová bezpečnost**
- **Hardwarová bezpečnost**
- **Softwarová bezpečnost**
- **Datová bezpečnost**
- **Komunikační (síťová) bezpečnost aj.**

PROCEDURY

FYZICKÁ BEZPEČNOST



Informační management

- vědní disciplína nebo skupina manažerů - specialistů, kteří ovlivňují kvalitu uspokojování informačních potřeb firmy (organizace), tj. také spolehlivost a bezpečnost informačních a komunikačních systémů,
- informační manažer, kompetence nebo vedoucí funkce pro informatizaci, koncepci informačních systémů a služeb, CIO – Chief Information Office.

Víceúrovňová bezpečnost

- Úrovně, respektive vrstvy či stupně zabezpečovacího procesu představující nikdy nekončící postup optimalizace bezpečnosti s trvale existujícím reziduem rizika.
- Hierarchie či následnost nástrojů k zmírňování známých rizik má metaforicky podobu à la: *geologické vrstvy sedimentu nebo slupky strukturovaných obalů např. cibule k ochraně jádra plodu. Jako další metaforické termíny se užívají brány, detektory (anti-virové) ochrany, politiky ap.*
- **Princip víceúrovňovosti** znamená násobnost užití více nástrojů v sekvenci účinku, *když principu je systémově použito i v dílčím subsystému např. v rámci konkrétního informačního systému (vymezeného SW-HW-infrastruktura); příklad: oblast tisk.*

2. Příklad vrstev či úrovní jako nástroje ochrany

- **Antivirový SW (s vazbou také na gateway)**
- **Firewall**
- **Detekce narušení sítě, stanice, serverů**
- **Hodnocení zranitelnosti infrastruktury**

INICIACE HACKERŮ

a

VNITŘNÍ INCIDENTY

BEZPEČNOSTNÍ OPATŘENÍ

**SÍŤ BEZPEČNOSTNÍCH
NÁSTROJŮ**

NARUŠENÍ

**Rozšíření o další vrstvu
SEBE-ZDOKONALENÍ VRSTVY**

Další penetrace
IS

**CHRÁNĚNÁ
část I**

**KONZOLIDACE
BEZPEČNOSTNÍ POLITIKOU**

Dodatečné
NÁKLADY*

**CHRÁNĚNÁ
část II**

**Taková ekonomická síla ochrany, aby se útočníkovi,
vzhledem k hodnotě, dat prolomení nevyplatilo*

kny@polac.cz
pozar@polac.cz