Zabezpečení aktiv v aplikačních systémech

ISSS 2015

Hradec Králové, 14. 4. 2015

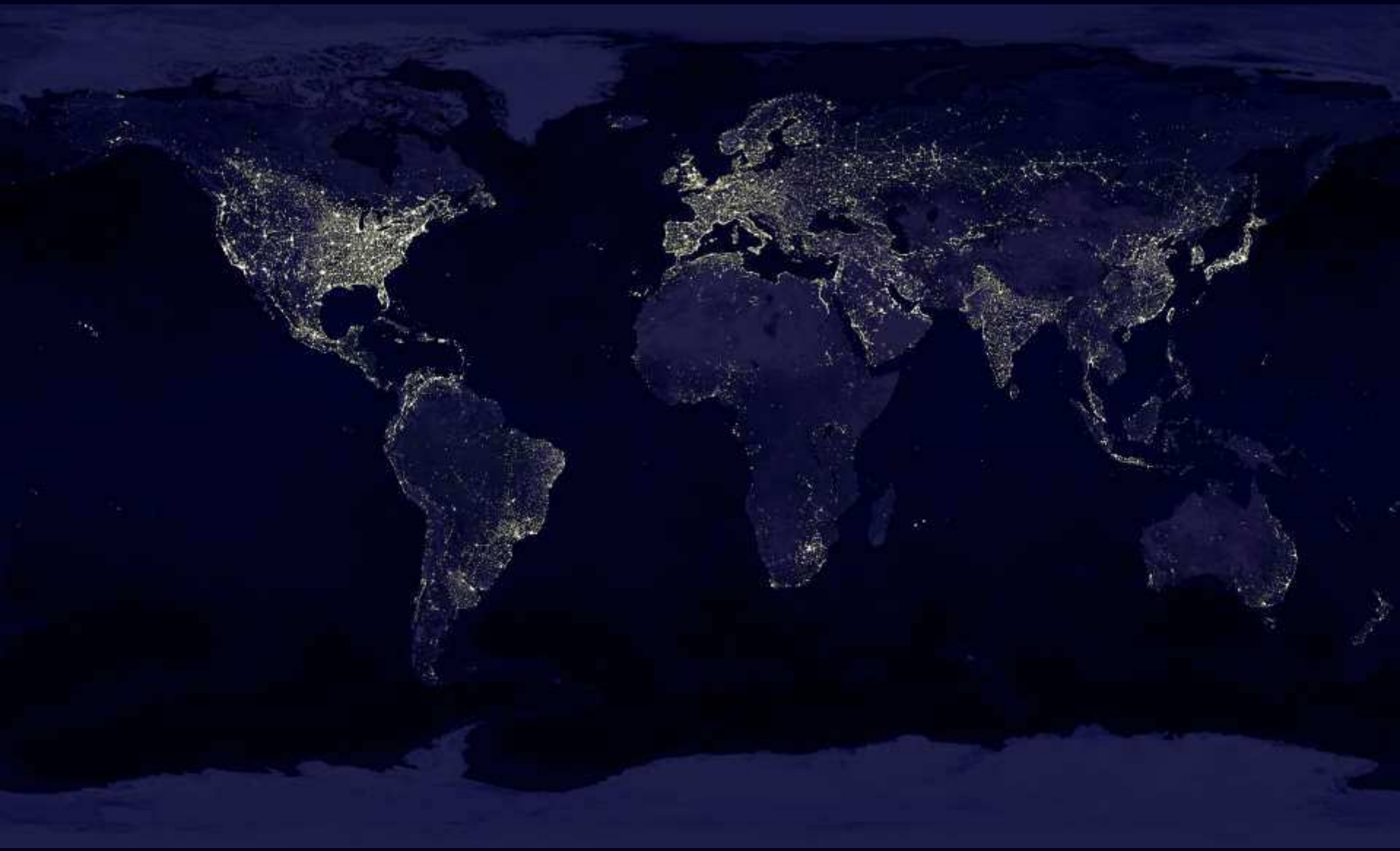
Igor Štverka

Legislativa ČR

- **Zákon o Kybernetické bezpečnosti**
  - Zákon č. 181/2014 Sb.
  - Prováděcí předpisy (www.govcert.cz)
- **Zákon o ochraně osobních údajů**
- **Zákon o elektronickém podpisu**
- **Zákon o ochraně utajovaných informací a bezpečnostní způsobilosti**

Kybernetická bezpečnost a ZoKB

- Inspirace ISO 2700x :
  - Bezpečnostní pravidla
  - Organizace informační bezpečnosti
  - Klasifikace a inventarizace **aktiv**
  - Zabezpečení vůči zaměstnancům
  - Fyzické zabezpečení výpočetního centra
  - Bezpečnost komunikací a provozu IT
  - Přístupová práva k sítím, systémům, aplikacím, funkcím a datům
  - Implementace zabezpečení do aplikací
  - Předvídání a řešení incidentů
  - Zabezpečení kontinuity chodu kritických systémů
  - Zabezpeční konformity s nastavenými požadavky, audit



Co je on-line?

osobní údaje

vztahy a vazby

obchodní tajemství

regulace a dohled

software

peníze

zaměstnanci

důvěryhodnost

akcie

strategické plány

AKTIVA !

duševní vlastnictví

krizové řízení

technické prostředky

budovy

přístupové klíče

výsledky výzkumu

společenský vliv

KDO je on-line?

Kdo jde po našich AKTIVECH ?

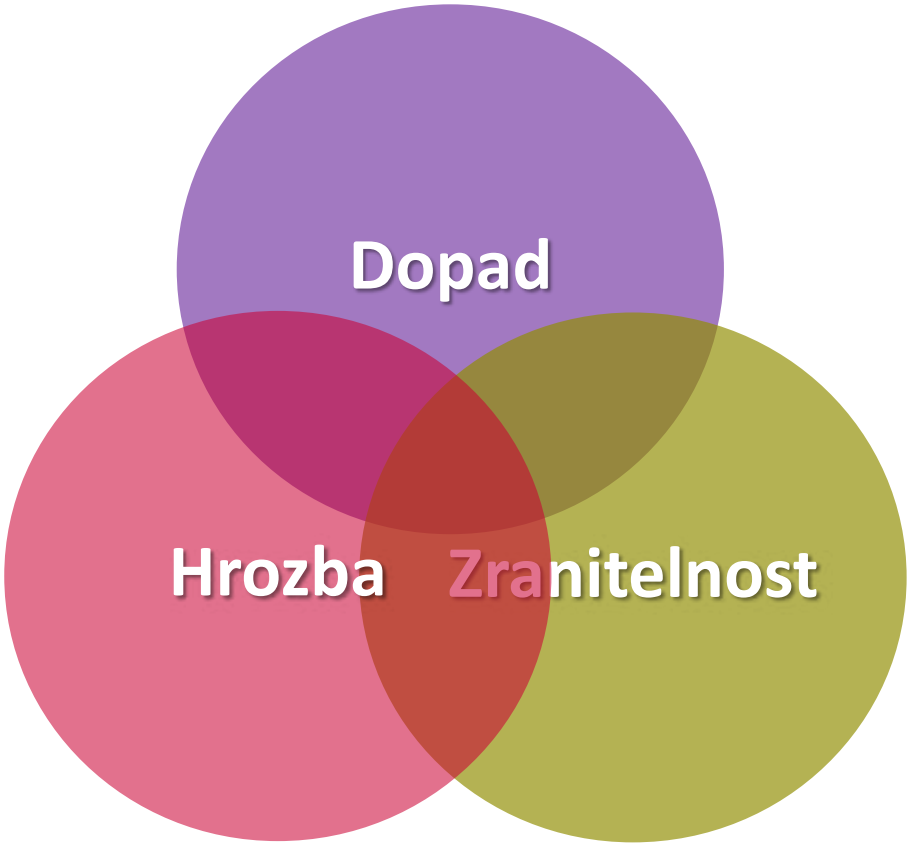
Typy „aktiv“ dle ZoKB

- **Primární aktiva**
  - zpracovávané informace
  - poskytované služby
- **Podpůrná aktiva**
  - zaměstnanci
  - dodavatelé (provoz, rozvoj, správa, bezpečnost IS)
  - technická aktiva
    - technické vybavení
    - komunikační prostředky
    - programové vybavení
    - objekty ve kterých jsou IS/KS umístěny

Osoby se vztahem k aktivům

- **Správce IS/KS**
  - orgán nebo osoba, které určují účel a podmínky provozu IS/KS
  - **Garant aktiva**
    - fyzická osoba pověřená správcem k zajištění rozvoje, použití a bezpečnosti aktiva
  - **Administrátor aktiva**
    - fyzická osoba pověřená garantem aktiva zajišťující správu, provoz, použití, údržbu a bezpečnost technického aktiva
  - **Uživatel aktiva**
    - fyzická nebo právnická osoba anebo orgán veřejné moci, která využívá primární aktiva

Tři komponenty rizikovosti aktiv



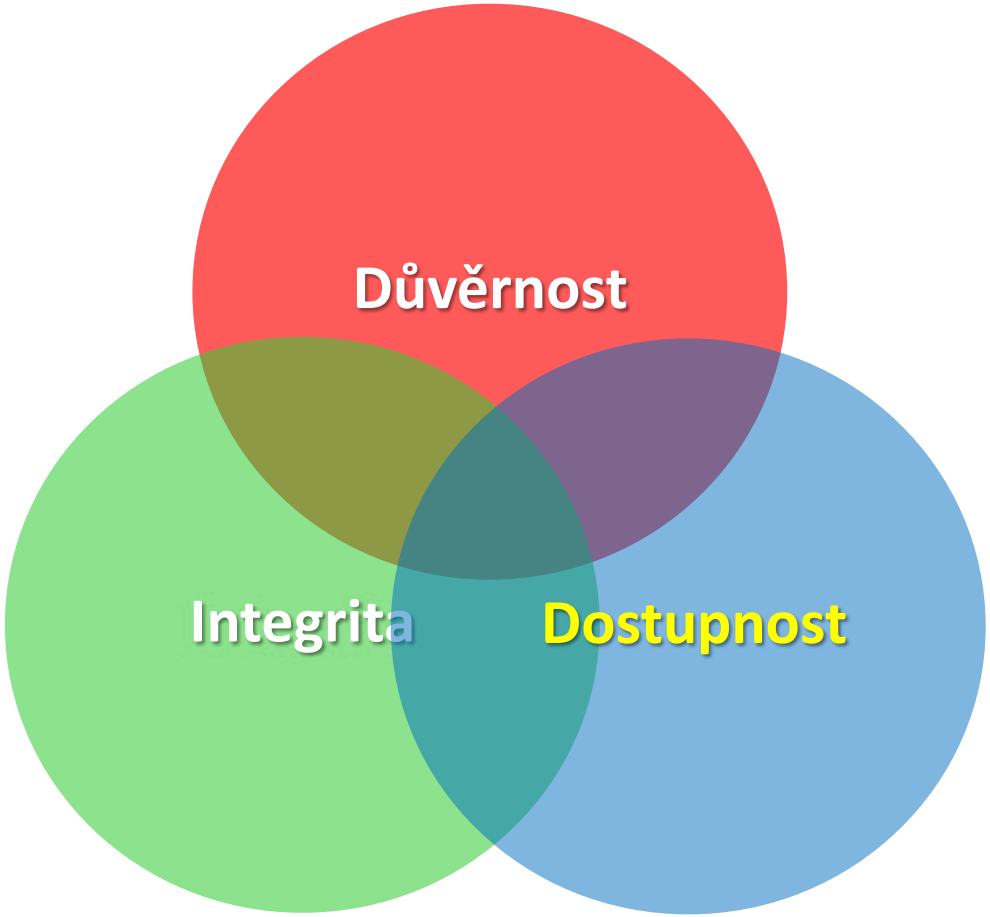
Riziko = Dopad x Hrozba x Zranitelnost

Příloha č. 2 k vyhlášce č. 316/2014 Sb.

Ohodnocení rizikovosti aktiv

Aktiva	Dopad	Hrozba	Zranitelnost
Zpracovávané informace			
Poskytované služby			
Zaměstnanci			
Dodavatelé			
Technické vybavení			
Komunikační prostředky			
Programové vybavení			
Objekty umístění IS/KS			

Tři protichůdné nároky na zabezpečení aktiv



Příloha č. 1 k vyhlášce č. 316/2014 Sb.

Ohodnocení nároků na zabezpečení

Aktiva	Důvěrnost	Integrita	Dostupnost
Zpracovávané informace			
Poskytované služby			
Zaměstnanci			
Dodavatelé			
Technické vybavení			
Komunikační prostředky			
Programové vybavení			
Objekty umístění IS/KS			

Cyber Security GINIS®

Komplexní zabezpečení primárních aktiv v aplikačních systémech

Modul GINIS®		Podporuje IS		Potenciální přínos pro zabezpečení aktiv*		
		GINIS®	ostatní	Důvěrnost	Integrita	Dostupnost
IDM	Identity Management	ANO	ANO	●●●		
GDU	Garantované dlouhodobé úložiště	ANO	ANO	●●	●●	●●
GDA	Důvěryhodný archiv	ANO	ANO	●●	●●●	●●●
AIB	Aplikační internetová brána	ANO	ANO	●●●		
DKS	Dokumentový konverzní server	ANO	ANO		●●	
WSDMS	Úložiště dokumentů	ANO	ANO	●●	●●	●●●
GSP	GORDIC Support Portál	ANO	ANO	●	●	●
ZUD	Zpracování událostí	ANO		●●	●	●●
RAK	Registr autorizovaných konverzí	ANO		●●	●●	
EPK	Elektronická podpisová kniha	ANO			●●●	
DAA	DRMS Administrativní audit	ANO		●	●●	●
SEM	Security Monitor GINIG	ANO		●●	●	●●
DSG	Dohledový systém GINIS	ANO			●	●●
eConnector	Konektory na bezpečná úložiště	ANO		●●●	●●	●●●
SSL	Individuální přístup k dokumentům	ANO		●●●	●	
ADM	Záznam činností administrátora	ANO		●●●	●	●

*) Potenciální přínos pro zabezpečení aktiv: ●●● kritický / ●● podstatný / ● podpůrný

Životní cyklus kybernetické bezpečnosti

PDCA

Reálný provoz!

Přístup GORDIC ke kybernetické bezpečnosti

- Popularizace: www.KyBez.cz
- Cyber Security GINIS®
- Individuální interaktivní semináře
- Školení
- Bezpečnostní audit /CISA/
- Studie kybernetické bezpečnosti
- *Zpracování analýz a projektů*
- *Realizace*
- *Provoz*
- *Dohled*

Partneři

Individuální interaktivní seminář

- Kybernetická bezpečnost úřadu:
  Jednodenní seminář se školením a interaktivním workshopem v místě zákazníka
  - Princip důvěrnosti a exkluzivity
  - Orientace v tématu a praktický vstup do řešení v rámci konkrétní organizace
  - Obsah školení:
    - Kybernetická bezpečnost pro veřejný sektor
    - Bezpečnost pro projektové celky
    - Ochrana informačních aktiv a základy informační bezpečnosti
  - Workshop:
    - kontrolní seznam (check-list)
    - přehled kritických oblastí, orientační nastavení priorit
    - přehled alternativ možných postupů a opatření.

Školení klybernetické bezpečnosti

- Úvod do informační bezpečnosti
  - Kybernetická bezpečnost pro veřejný sektor
  - Bezpečnost pro projektové celky
  - Ochrana informačních aktiv a základy informační bezpečnosti
- Technická opatření
  - Základy šifrování
  - Síťová infrastruktura a bezpečnost
  - Bezpečnost databází
  - Práce s logy, analýza a reportování incidentů
- Organizační opatření
  - Životní cyklus informací ve vztahu k bezpečnosti
  - Oborové bezpečnostní standardy
  - Zachování provozu a havarijní scénáře
  - Řízení bezpečnosti a nápravná opatření
- Cyber Security GINIS®
  - Řízení bezpečnosti v systému GINIS
  - Optimalizace a dobrá praxe v zabezpečení systému

Co znamená KB pro zákazníky GORDIC?

- GINIS® vyvíjen s důrazem na bezpečnost provozu
  - Instalace v silových rezortech
  - **Cyber Security GINIS®**
- Standardy – GORDIC je držitelem certifikátů:
  - ISO 9000 (řízení jakosti)
  - ISO 20000 (poskytování ICT služeb)
  - ISO 27001 (řízení bezpečnosti informací)
- Podpora zákazníků v zavádění ISMS
  - Odborné poradenství (CISA, CISM, CRISC)
  - Inovace v produktech
  - Řešení se specializovanými partnery

16.4.2015

Další informace (otázky, upřesnění)

Děkujeme za pozornost

www.gordic.cz

Informace v této prezentaci nemají charakter obchodní nabídky. Pro GORDIC spol. s r. o. z této prezentace nevyplývají žádné závazky a/nebo povinnosti.