



# Dokumentová úložiště vs. informační bezpečnost

Ing. Jan Bareš, CISA 5.10.2009



# Agenda

- Legislativa
- Úvod do problematiky bezpečnosti
- Co je „bezpečné úložiště“
- Realizace bezpečnosti na úložišti
- Širší pohled
- Doporučení

# Zákony

- Tlak na elektronizaci státní správy
- Předpisy bezpečnost neřeší
- Všichni očekávají, že bezpečnost „bude v ceně“
  
- Funkční aspekt je nyní prioritou
- Bezpečnost ?
  - Bude se „dolepovat“ ?
  - Bude vůbec řešena ?

# Bezpečnost

- Dostupnost
  - Jsem schopen se k informaci dostat ?
- Důvěrnost
  - Informace se nesmí dostat do nepovolaných rukou
- Integrita
  - Je informace původní, celá, nezměněná ?
- Autentičnost
  - Je skutečný původ dokumentu takový, jak je deklarován ?
- Vše budeme zvažovat v horizontu dlouhodobého provozu

# Pohled bezpečáka

- Nemáme NOVÁ rizika
- Existující rizika mění svůj význam
- Řešme bezpečnost jako celek
  
- Spisová služba je nositelem bezpečnosti
- Stejně jako spisová služba vystupují i ostatní systémy
- Nesmíme zapomenout na otázku elektronických podpisů
  
- Standardizace bezpečnosti existuje – lze ji využít

# Proč digitální úložiště?

- Některé dokumenty jsou ukládány ze zákona
- Mnoho informací nemá jinou než datovou podobu
- Státní správa přechází na elektronické vedení agendy povinně
- Mnoho dokumentů ve fyzických archivech vzniká konverzí (vytištěním) datového obsahu  
Přitom zaniká část autenticity informace, která je pouze digitální
- Zjednodušeně: Digitální doba vyžaduje digitální ukládání

# Bezpečné úložiště

- Otázka bezpečného vývoje aplikací
- Certifikace aplikace
- Audit
  - Procesu vývoje
  - Procesu implementace
  - Provozování
  - Dekompozice a zániku
- Garance vzniku a nepozměnitelnosti důkazního materiálu
- Národní standard pro elektronické spisové služby (MoReq2)

# Disky? Úložiště? Archiv?

- Archiv je soustava definovaná zákonem
- Na vedení archivu klade zákon jasné podmínky
- Ne každé úložiště dat je archiv
- I když úložiště není archiv, nesmí být podkopána jeho důvěryhodnost
  
- Aspekty bezpečného úložiště
  - Data jsou write only
  - Nejen dokument, ale i metadata
  - Zajištění integrity a autenticity na dlouhou dobu
  - Aplikační nadstavba pro řízení provozu
  
- **Diskové pole s velkou kapacitou a redundancí není bezpečné úložiště!**

# Zajištění bezpečného

- Datové centrum je propojeno s více typy sítí
  - Veřejné (Internet)
  - Samotné DC (zónování?)
  - Privátní síť (LAN úřadu)
  - Poloveřejné síť (KIVS)
- Více typů přístupu
  - Úředník úřadu
  - Vzdálený úředník
  - Správce DC
  - Správce aplikace
- **Potřeba vytvořit, implementovat a vynutit řízení datového provozu a přístupových práv**

# Dostupnost, dostupnost ...

- Dostupnost ve všech významech
  - Technologií (servery, LAN)
  - Přístupových cest (linky do externích sítí)
  - Aplikační (odolnost aplikace proti nestandardním stavům)
- Obnova provozu
  - Recovery point
  - Recovery time
- **Je nutno řešit komplexně**

# Datové úložiště je nejen IT

- Fyzická bezpečnost
  - Bezpečné prostory
  - Řízení fyzického přístupu
  - Nedatové sítě (vzduch, voda, teplo, energie, hašení atd.)
  - Monitoring (kamery, ostraha)
- Ostatní otázky
  - Oddělení a zónování prostor
  - Přepisová základna
  - Trénink, kontrola, audit
- **Je nutno řešit komplexně**

# Doporučení

Zde uvedená doporučení nejsou univerzální návod  
Jde především o otázky k zamyšlení

- Bezpečnost nemusíme stavět na zelené louce, použijme již hotové
- Normy řady ISO27000 + ISMS best practice
- Zajistit základní přístupovou bezpečnost (HW+SW)
- Zajistit redundanci
- Prověřit (vybudovat) procesní a předpisovou základnu
- Řešit důvěryhodné úložiště
  
- **Nenechat bezpečnost „na potom“**  
Bylo by to drahé, riskantní, a časem i zbytečné

# Dotazy a závěr

Kontakt  
Ing. Jan Bareš  
[Jan.Bares@Corpus.cz](mailto:Jan.Bares@Corpus.cz)