# Dokumentová úložiště vs. informační bezpečnost

Ing. Jan Bareš, CISA 20.10.2009

CORPUS SOLUTIONS

# Agenda

- Úvod do problematiky bezpečnosti
- Důvěryhodnost elektronických dokumentů
- Spisová služba a důvěryhodnost
- Realizace bezpečnosti na úložišti

- Doporučení

# Zákony

- Tlak na elektronizaci státní správy
- Předpisy bezpečnost neřeší
- Všichni očekávají, že bezpečnost „bude v ceně“

- Funkční aspekt je nyní prioritou
- Bezpečnost ?
  - Bez bezpečnosti není důvěryhodnost
  - Bezpečnost v širším smyslu je podmínkou platnosti
  - 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

# Proč digitální úložiště?

- Některé dokumenty je nutno ukládat 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

# Základní otázky důvěryhodnosti

- Původ
  - Kdo dokument vytvořil
  - Jsme schopni prokázat autora a čas vzniku?
- Transport
  - Je doručena původní podoba dokumentu?
  - Nedostal se také do nepovolaných rukou?
- Ověření
  - Prověření pravosti před převzetím k uložení
- Uložení
  - Dlouhodobé zajištění platnosti ověření pravosti

# Problémy elektronických dokumentů

- Platnost certifikátu je dočasná
- Datová zpráva – podpis „na obálce“
- Obsažený dokument
  - Digitální podpis
  - Časová razítko
- Certifikát pro podpis je pro osobu
  - Jak validujeme organizaci?
- Konverze ze zákona (na papír) ztrácí data
  - Pouze sériové číslo certifikátu

# Fikce pravosti

- §69a odst. 8 ArchZ:
- Neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán platným uznávaným elektronickým podpisem nebo označen platnou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna, osoby odpovědné za převedení z dokumentu v analogové podobě nebo změnu formátu dokumentu v digitální podobě nebo osoby odpovědné za provedení autorizované konverze dokumentů a opatřen kvalifikovaným časovým razítkem.
- Dopady
  - Nestačí zpochybnit – musí se prokazovat
  - Není soudní výklad a praxe
- Doporučení – paranoia je na místě

# Spisová služba a důvěryhodné uložení

- Oběh dokumentu s digitálním podpisem není dostatečný
- Nutno pracovat s metadaty
- Elektronický podpis validuje pouze transport
  - Je aplikace vytvořena důvěryhodně?
  - Je aplikace provozována důvěryhodně?
- Národní standard pro spisové služby – eRMS; Moreq2

- Spisovna
- Skartační řád
- Archivace

# Alternativa k spisové službě

- Ne každý je povinen vést SS ze zákona podle eRMS
  - Především komerční subjekty
  - Fyzické osoby
- Důvěryhodně uložit + pracovat s „kopií“
  - Ukládat a ověřovat hned při příjmu
  - Interní pravidla uznávání pravosti

- Úložiště
  - Jako služba
  - Vlastní

# 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)

# 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
- Národní standard eRMS
- Normy řady ISO27000 + ISMS best practice
- Zajistit základní přístupovou bezpečnost (HW+SW)
- Zajistit redundanci
- Prověřit (vybudovat) procesní a předpisovou základnu

- **Nenechat bezpečnost „na potom“**
  Bylo by to drahé, riskantní, a časem i zbytečné

# Dotazy a závěr

Kontakt

Ing. Jan Bareš

Jan.Bares@Corpus.cz