BRK-04-2016-02P

Kybernetická bezpečnost – implementace procesního rámce pro řízení informační bezpečnosti

pro: jednání bezpečnostní rady kraje č. 04/2016 dne 13. 10. 2016
zpracoval(a): D. Marek
předkládá: Z. Kadlec

počet stran: 2
počet příloh: 1CD

Popis problému:

Na základě požadavků zákona 181/2014 Sb. o kybernetické bezpečnosti, schválené Strategii ICT Kraje Vysočina a rozhodnutí vedení Krajského úřadu Kraje Vysočina dochází v současné době k implementaci procesního rámce - systému řízení bezpečnosti informací (ISMS). ISMS je popsán v normách ČSN ISO/IEC 2700x a slouží k zavedení procesních a technických opatření za účelem zajištění odpovídající úrovně informační bezpečnosti.

Výsledkem zavedení systému bude systematické zabezpečení informací, zamezení zneužití a ztráty informací, zefektivnění informačních toků prostředí kraje a jeho orgánů, ochrana osobních údajů a zamezení neoprávněného nakládání s osobními údaji, zajištění souladu činností s trestním zákoníkem. Zavedení moderního a komplexního managementu zajistí trvalé zlepšování podmínek bezpečnosti dat a informací, zajištění včasné dostupnosti dat a informací, zamezení zneužití nebo zcizení dat a informací, zavedení dodržování zákonných požadavků v oblasti bezpečnosti a ochrany dat, informací a osobních údajů, zajištění průkaznosti plnění požadavků legislativy a získání právně uznatelných důkazů pro případ potřeby, snížení rizika vzniku havárií a stavů ztráty nebo znehodnocení dat a informací, zamezení nechtěné nebo neúmyslné modifikace dat a informací, snížení rizika sankcí vyplývajících z nedodržování legislativy a regresů spojených únikem dat, informací a osobních údajů, vyřešení kompetence pracovníků, odpovědností a pravomocí v oblasti bezpečnosti dat a informací a v neposlední míře přispěje i zvýšení důvěryhodnosti a dobrého jména Kraje Vysočina.

Průběh zavedení systému ISO/IEC 27001 je následující:

- vstupní analýza (zmapování stávajících procesů, vymezení systému a jeho procesů)
- stanovení úrovně bezpečnosti
- stanovení rozsahu aplikovatelnosti
- určení způsobu řízení rizik v oblasti informací
- implementace definovaných postupů do praxe
- standardizace postupů formou dokumentace
- zmapování relevantních procesů a to v tomto rozsahu:
  - popis procesů, jejich dokumentace a zachycení vzájemného působení a ovlivňování
  - reengineering a vhodné přepracování málo výkonných míst procesů
  - zpracování dokumentace procesů, map procesů a grafického záznamu vazeb
  - zmapování legislativních a technických požadavků na realizaci procesů
  - stanovení vstupů, výstupů a zdrojů potřebných pro činnost procesu
  - personální řešení, řízení odpovědností a pravomocí
- provedení interního auditu k ověření implementace postupů do praxe
- korektura dokumentace na základě zjištění z interního auditu
- zaškolení pracovníků
- výběr certifikační společnosti a podání přihlášky k certifikačnímu auditu
- certifikační audit (1. a 2. stupeň, případně následný audit)

- opakovaný dohledový audit.

Očekávání úřadu do implementace ISM jsou následující

- organizace bezpečnosti
  - určení zodpovědností a pravomocí
  - provádění analýzy rizik
- řízení vztahů s dodavateli
  - definice bezpečnostních požadavků na dodávané informační systémy
- řízení aktiv
  - identifikace a ohodnocení aktiv
  - zavedení pravidel pro používání mobilních zařízení, paměťových médií, zaměstnaneckých a čipových karet
  - zavedení pravidel na manipulaci s informacemi
- bezpečnost lidských zdrojů
  - zavedení systému vzdělávání zaměstnanců v oblasti bezpečnosti
- fyzická bezpečnost
  - zabezpečení důležitých místností - serverovny, spisovny, kanceláře
- řízení přístupů
  - schvalování a evidence přístupů
  - přidělování přístupů na základě principu „potřeba znát“ a „potřeba použít“
  - používání bezpečných hesel a
  - včasné odebírání nepotřebných přístupů
- kryptografie
  - používání bezpečných kryptografických prostředků a jejich ochrana
- bezpečnost provozu
  - evidence změn v IS
  - dokumentace provozních postupů
  - plánování kapacit
  - provádění pravidelných a obnovitelných záloh dat
  - řešení technických zranitelností
  - zaznamenávání a vyhodnocování vzniklých událostí
  - provádění bezpečnostních auditů
- řízení incidentů
  - efektivní řešení bezpečnostních incidentů a jejich evidence

Návrh řešení, zdůvodnění:

Podrobnější popis a rekapitulace současného stavu implementace ISMS jsou uvedeny v příloze BRK-04-2016-02P, př.1

Stanoviska:

Stanoviska nebyla vyžádána.

Návrh usnesení:

bezpečnostní rada kraje
bere na vědomí

Informaci o průběhu implementace procesního rámce pro řízení informační bezpečnosti dle materiálu BRK-04-2016-02P a BRK-04-2016-02P, př. 1

odpovědnost: Z. Kadlec
termín: 13. 10.2016