Systém řízení bezpečnosti informací na Krajském úřadě

Dominik Marek

Kraj Vysočina

Dopady ZKB

- Kraj Vysočina je správcem VIS dle ZKB (181/2014 Sb.)
  - podle doporučení Asociace krajů
  - podle usnesení Rady Kraje 0110/03/2016/RK
    - www stránky
    - poštovní systém
    - ekonomický systém
    - spisová služba
- VIS jsou nahlášeny na NBÚ od ledna 2016
- Zavedení bezpečnostních opatření
  - do ledna 2017
  - dle ČSN ISO/IEC 27001:2013

Zavedení systému řízení bezpečnosti informací (ISMS)

- Cíl
  - certifikace celého úřadu
  - splnění podmínek ZKB
  - zvýšení úrovně informační bezpečnosti
  - řešení bezpečnosti informací systémovým způsobem

- Schválená Pravidla Rady Kraje Vysočina č. 06/2015
  - Stanovena bezpečnostní politika Kraje Vysočina v oblasti systému řízení informační bezpečnosti

- Směrnice, kterou se stanoví Bezpečnostní politika Kraje Vysočina
  - základní stavební kámen ISMS
  - dokument obsahující bezpečnostní opatření (vychází z normy)

Stav implementace ISMS

Číslo úkolu	Popis	Návrh	Implementace	Co chybí
1	Ustavení ISMS v organizaci	100%	50%	Schválení směrnice, ustanovení rolí , zapsání rolí do pracovních náplní
2	Návrh a implementace Celkové Bezpečnostní politiky organizace	100%	100%	x
3	Návrh a implementace politiky Bezpečnost lidských zdrojů	100%	80%	Vypracování modulů vzdělávání - průběžné, odborné
4	Návrh a implementace politiky Řízení aktiv	100%	90%	Evidence garantů na intranetu
5	Návrh a implementace politiky Řízení přístupů	100%	80%	Nastavení heslových politik, nastavení systému HelpDesk
6	Návrh a implementace politiky Kryptografie	90%	90%	definování procesu revokace, nastavení systému HelpDesk
7	Návrh a implementace politiky Fyzické bezpečnosti	100%	75%	Sepsání seznamu osob oprávněných ke vstupu, nastavení systému HelpDesk
8	Návrh a implementace politiky Bezpečnost provozu	100%	60%	dokumentace (z části hotovo), nastavení systému HelpDesk, oddělení prostředí, řízení technických zranitelností, provádění testů informační bezpečnosti
9	Návrh a implementace politiky Bezpečnost komunikací	100%	100%	x
10	Návrh a implementace politiky akvizice, vývoj a údržba IS	100%	x	x
11	Návrh a implementace politiky Dodavatelské vztahy	100%	100%	x
12	Návrh a implementace politiky Řízení bezpečnostních incidentů	100%	80%	nastavení systému HelpDesk, vyřešení reklamace GPC
13	Návrh a implementace politiky Řízení kontinuity	100%	90%	korektura dokumentu
14	Soulad s požadavky	x	0%	provedení precertifikačního auditu

Harmonogram:

Termín	Úkol
1.10.	zveřejnění Směrnice, kterou se stanoví bezpečnostní politika Kraje Vysočina
říjen	zveřejnění veřejné zakázky na certifikační agenturu
2. polovina října 2016	interní precertifikační audit
1. polovina listopadu 2016	školení zaměstnanců - obecná problematika směrnice, povinnosti vyplývající ze směrnice pro běžné zaměstnance
2. polovina listopadu 2016	školení bezpečnostních rolí
prosinec 2016	zahájení certifikace
1.1. 2017	účinnost směrnice
leden 2017	obdržení certifikátu

Zjednodušení pro běžné uživatele

ČSN ISO/IEC 27001:2013 → **ZKB 181/2014 Sb.**

Směrnice, kterou se stanoví bezpečnostní politika Kraje Vysočina

Metodické příručky pro uživatele + rozkreslené procesy

Školení dle jednotlivých rolí

Přínos ISMS (výběr):

- 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
  - pravidla pro používání mobilních zařízení, paměťových médií, zaměstnaneckých a čipových karet
  - pravidla na manipulaci s informacemi
- bezpečnost lidských zdrojů
  - systém vzdělávání zaměstnanců v oblasti bezpečnosti
- fyzická bezpečnost
  - zabezpečení důležitých místnosti – serverovny, spisovny, kanceláře

Přínos ISMS (výběr):

- řízení přístupů
  - schvalování a evidence přístupů
  - přidělování přístupů na základě principu „potřeba znát“ a „potřeba použít“
  - používáme bezpečná hesla a přístupy včas odebíráme
- kryptografie
  - používání bezpečných kryptografické prostředků a jejich ochrana
- bezpečnost provozu
  - evidence změn v IS
  - dokumentace provozních postupů
  - plánování kapacit
  - pravidelná a obnovitelná záloha dat
  - řešení technických zranitelností
  - zaznamenávání a vyhodnocování vzniklých událostí
  - provádění bezpečnostního auditu
- řízení incidentů
  - snažíme se efektivně řešit bezpečnostní incidenty, mít o nich přehled a stanovovat protiopatření

Děkuji za pozornost!

Dominik Marek

marek.dominik@kr-vysocina.cz

564 602 325