Ceny Ministerstva vnitra za kvalitu a inovaci ve veřejné správě

ročník 2012

ZÁVĚREČNÁ ZPRÁVA Z ŘEŠENÍ

☒ bronzového stupně ceny

☐ stříbrného stupně ceny

☐ inovace

(zatrhněte cenu, o jakou soutěžíte)

1. Název řešení:

Implementace Systému řízení bezpečnosti informací dle normy ISO/IEC 27001 v prostředí Krajského úřadu Jihomoravského kraje

2. Autor zprávy:

Jméno: Ing. Martin Havel, MBA
Funkce: manažer bezpečnosti informací
Organizace: Krajský úřad JMK
Telefon: 541 651 139
E-mail: havel.martin@kr-jihomoravsky.cz

Jméno: Ing. Jarmila Beránková, Ph.D.
Funkce: manažerka kvality
Organizace: Krajský úřad JMK
Telefon: 541 651 223
E-mail: berankova.jarmila@kr-jihomoravsky.cz

3. Organizace, kde bylo řešení aplikováno:

Jihomoravský kraj
Krajský úřad Jihomoravského kraje
Žerotínovo nám. 3/5, 601 82 Brno

4. Popis řešení

4.1 Podstata řešení:

Podstatou řešení je vytvoření jednotného systému Bezpečnosti informací dle požadavků normy ISO/IEC 27001 včetně certifikace procesů bezpečnosti informací dle téže normy na dvou odborech Krajského úřadu Jihomoravského kraje (dále jen „KrÚ JMK"), které jsou zásadní z hlediska technického a organizačního zajištění chodu úřadu.

Jedná se o komplexní zajištění bezpečnosti informací, které jsou spravovány při výkonu samostatné působnosti nebo přenesené působnosti ve smyslu příslušných zákonů.

Celé řešení přináší globální přístup k celé problematice Bezpečnosti informací. Pomáhá prověřit současný stav, naplánovat a realizovat nejvhodnějšího řešení s nastavením účinných kontrolních mechanismů.

4.2 Důvod a cíle řešení (včetně doložení jejich měřitelnosti)**:**

Pro KrÚ JMK je charakteristická vysoká úroveň informatizace činnosti a organizace činností. Proto jsou zpracovávaná data, resp. informace pro KrÚ JMK tím nejcennějším aktivem. Přiměřená ochrana těchto aktiv musí zajistit jejich důvěrnost, integritu a dostupnost. Vedení KrÚ JMK si je

vědomo povinnosti a odpovědnosti zajistit bezpečnost dat a ochranu komunikačního prostředí (Informační a Komunikační Technologie, dále jen ICT) před neustále se vyvíjejícími hrozbami, kompromitací či modifikací.

Bezpečnost utajovaných informací a informací souvisejících s krizovým řízením jsou regulovány zákonem číslo 412/2005 Sb. *o ochraně utajovaných informací a o bezpečnostní způsobilosti*, ve znění pozdějších předpisů a zákonem číslo 24/2000 Sb. *o krizovém řízení a o změně některých zákonů*, ve znění pozdějších předpisů, prováděcími vyhláškami a jasně definovanými standardy.

Složitější situace nastává při řešení bezpečnosti informací v rámci provozovaných informačních systémů veřejné správy ve smyslu zákona číslo 365/2000 Sb., *o informačních systémech veřejné správy*, ve znění pozdějších předpisů. Oblast bezpečnosti informací je zde definována v mnohem obecnější podobě, což dává poměrně značný prostor pro různou interpretaci aplikovaných organizačních a technických opatření.

Největší komplikace však představuje oblast zajištění bezpečnosti informací, která není regulována žádným z výše uvedených zákonů. Přesto je každý subjekt, který nakládá s těmito informacemi v rámci provozovaných informačních systémů, povinen zajistit jejich ochranu. Týká se to především informací charakteru osobních a citlivých údajů, obchodního tajemství apod.

Z výše uvedených důvodů se vedení KrÚ JMK rozhodlo zajistit bezpečnosti informací (aktiv) v rámci KrÚ JMK zavedením Systému řízení bezpečnosti informací - Information Security Management System (dále jen „ISMS") v souladu s pravidly stanovenými skupinou norem ČSN ISO/IEC 270xx (Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací).

Hlavním cílem bylo vytvoření systému ISMS tak, aby se bezpečnost stala součástí všech procesů KrÚ, aby ochrana aktiv probíhala jako nepřetržitý proces zajišťování důvěrnosti, integrity a dostupnosti chráněných informací.

Dílčím cílem pak bylo certifikovat systém ISMS a tedy transparentně prokázat shodu systému s normou ISO/IEC 27001:2005 pro oblast Činnosti veřejné správy – Odbor kanceláře ředitelky, Odbor informatiky.

4.3 Implementace řešení:

Implementace požadavků normy ISO/IEC 27001, neboli vytvoření ISMS probíhala v postupných krocích:

1. Zpracování analýzy (audit), která obsahovala zejména:
    a) Identifikaci aktiv (co je předmětem ochrany)
    b) Analýzu ochrany aktiv (ověření, jak jsou aktiva chráněna)
    c) Popis zjištěných nedostatků a identifikaci klíčových rizik

2. Podrobné posouzení aktuálního stavu bezpečnosti:
    a) Zhodnocení nastavení systému bezpečnosti ICT
    b) Zhodnocení na základě „kontroly shody" u ICT
    c) Zhodnocení řízení oblasti bezpečnosti informací ve vztahu ICT

3. Zpracování detailního plánu implementace, který zahrnuje zejména:
    a) Identifikaci opatření
    b) Vztah k identifikovaným rizikům
    c) Harmonogram, Cestovní mapa
    d) Očekávaný efekt, Priority řešení

4. Vlastní implementace:
    a) Stanovení implementačního týmu
    b) Realistický harmonogram, kontrolní dny
    c) Školení uživatelů

d) Tvorba interních informačních týmových webů

Při implementaci byly využity:

1. zkušenosti KrÚ JMK z oblasti řízení kvality dle ISO/IEC 9001:2009.
2. rozšíření existující bezpečnostní infrastruktury v následující posloupnosti: Bezpečností ředitel, Manažer bezpečnosti informací, Bezpečnostní správce odboru.

   Důležitá je linie podřízenosti Manažera bezpečnosti informací. Jeho úkolem je vytvářet a aktualizovat směrnice, dohlížet na jejich dodržování, zajišťovat jejich implementaci, kontrolovat a informovat vedení o průběžné situaci. Praxe ukazuje, že je rizikové ponechat „vládu nad bezpečností informací" jen v rukou Odboru informací, který spravuje ICT. Obecně platí, že pohled správce ICT na bezpečnost je zpravidla odlišný od pohledu příslušného bezpečnostního pracovníka.
3. projektové řízení – metodika MDIS – se zaměřením zejména na následující úkony:

Nejdůležitějšími faktory implementace řešení byly:

1. Podpora vedení organizace.
2. Efektivní a konstruktivní projektový tým.
3. Vytvoření a nastavení správné bezpečnostní infrastruktury.
4. Využití synergie s jinými ISO normami.
5. Kvalitní analýza počátečního stavu jako základní kámen úspěšné implementace.

- ***zainteresované strany***

  interní účastníci - zaměstnanci a vedení KrÚ Jihomoravského kraje

  externí zákazníci – občané, dodavatelé, spolupracující strany

- ***odpovědnost za řešení***

  Manažer bezpečnosti informací, jehož nadřízeným je Bezpečností ředitel KrÚ JMK.

- ***podpora řešení ze strany vedení***

  Podpora ze strany vedení probíhala v několika úrovních:

  1. vedení Jihomoravského kraje, pan hejtman, osobní angažovaností a podporou aktivit v oblasti Bezpečnosti informací, podpora ředitelky KrÚ JMK v prosazování principů Bezpečnosti informací, prosazení schválení vytvoření ISMS radou JMK
  2. vedení KrÚ JMK, paní ředitelka, osobní angažovaností, zřízením funkce Manažer bezpečnosti informací, jehož nadřízeným je Bezpečností ředitel KrÚ JMK. Jmenováním členů Bezpečnostního fóra Úřadu, vytvořením prostoru této problematice na poradách, zařazením problematiky Bezpečnosti informací mezi priority KrÚ JMK. Dále pak motivací vedoucích odborů a získáním jejich podpory při prosazování principů Bezpečnosti informací formou vytvoření pracovních týmů ISMS, realizací diskusních kulatých stolů.

- ***podpora řešení ze strany zaměstnanců***

  Zkušenosti vycházející z úspěšné implementace řízení kvality dle ISO/IEC 9001:2009, vstřícný přístup v součinnosti při identifikaci aktiv a zpracování analýzy rizik. Poskytnutí detailních informací pro zpracování nové ISMS dokumentace nebo aktualizaci stávajících dokumentů.

- ***překážky***

Na začátku to byly obavy z něčeho nového. Proto bylo důležité tyto obavy rozptýlit, získat důvěru a podporu zaměstnanců, vedoucích odborů jako hlavních nositelů principů Bezpečnosti informací a vykonavatelů jednotlivých bezpečnostních politik.

Dále také nalezení časového prostoru jednotlivých zaměstnanců a vedoucích odborů pro zpracování jednotlivých analýz a školení daného tématu.

- ***úspěchy***

  Získání certifikátu dle shody ISMS s normou ISO/IEC 27001:2005 pro oblast Činnosti veřejné správy – Odbor kanceláře ředitelky, Odbor informatiky.

5. Výsledky řešení

- *Jaké byly hlavní výsledky (uvést pokud možno kvalitativní i kvantitativní ukazatele)?*

  V oblasti zavedení ISMS v podmínkách KrÚ JMK lze identifikovat následující kvantitativní ukazatele:

  - Vytvoření nebo aktualizace 14 dokumentů v rámci zavedeného ISMS
  - Implementace ISMS do 9 interních norem (včetně 1 nově vytvořené).
  - Počet neshod z certifikačního auditu= 0
  - Počet odchylek z certifikačního auditu = 0
  - Počet doporučení z certifikačního auditu = 14
  - Počet proškolených vedoucích odborů, útvarů = 18
  - Počet proškolených zaměstnanců = více jak 600
  - Vytvoření dvou interních portálů k tématu Bezpečnost informací

  Jako hlavní kvalitativní ukazatel lze uvést:

  - Získání certifikátu dle shody ISMS s normou ISO/IEC 27001:2005 pro oblast Činnosti veřejné správy – Odbor kanceláře ředitelky, Odbor informatiky.

- ***Jaké nástroje pro jejich měření jste použili a jak hodnověrné jsou důkazy?***

  Pro měření kvalitativních a kvantitativních ukazatelů jsme využili následující nástroje:

  - zprávy z interních auditů
  - zpráva z certifikačního auditu
  - prezenční listiny z jednotlivých školení
  - zpětná vazba ze školení prostřednictvím portálu Bezpečnost informací

  Hodnověrnost je zajištěna přezkoumáním nezávislého certifikačního orgánu formou certifikačního auditu.

- ***Vyskytly se nějaké specifické faktory, které mohly ovlivnit úspěch tohoto řešení?***

  Ne

- ***Projevil se nějaký vedlejší negativní či pozitivní účinek?***

  Projevilo se několik pozitivních účinků:

  1. synergie v návaznosti na řízení kvality dle ISO/IEC 9001:2009;

2. vytvoření bezpečnostní infrastruktury KrÚ JMK, včetně nového meziodborového Bezpečnostního fóra Úřadu;
3. zvýšení znalostí v oblasti bezpečnosti informací u zaměstnanců, ustanovení a vyškolení bezpečnostních správců na každém odboru KrÚ;
4. zavedení ISMS do podmínek KrÚ JMK lze jmenovat připravenost na projekty související s elektronizací státní a veřejné správy (eGovernement). Díky zavedenému systém ISMS lze pak velmi jednoduše aplikovat stejné bezpečnostní požadavky na jakýkoliv nový prvek Informačních nebo komunikačních technologií KrÚ JMK.

Jako negativní účinek lze zmínit: počáteční nedůvěra k zavedení novinek v přístupu k bezpečnosti informací, vycházející z tradičních rezistentních přístupů účastníků ke změně.

6. Inovativnost a přenositelnost dobré praxe[1]

- *V čem spočívá inovativnost tohoto řešení? Jak se liší od jiných čpodobných aplikací/přístupů?*
- *Může být/bylo již toto řešení přeneseno/aplikováno v jiné organizaci či sektoru? Pokud ano, které jeho základní prvky? Nebo jste v tomto případě sami využili dobrou praxi od jiných organizací?*
- *Jaké nejdůležitější poznatky/zkušenosti jste při realizaci řešení získali?*
- *Jaké je Vaše doporučení pro ty, kteří sezajímají o implementaci tohotořešení ve své organizaci?*
- *Souhlasíte s prezentací Vašeho řešení na nadcházející Národní konferenci kvality ve veřejné správě a v časopise Veřejná správa jakožto s prezentací dobré praxe?*

7. Přílohy

Kopie certifikátu ISO/IEC 27001:2005

Prohlášení o politice ISMS

Datum: 8.10.2012

Vyhotovil/a: Ing. Martin Havel, MBA; Ing. Jarmila Beránková, Ph.D.

Podpis: JUDr. Věra Vojáčková, ředitelka Krajského úřadu Jihomoravského kraje

Pozn.: V případě ceny udílené za implementaci modelu CAF musí být přílohou Závěrečné zprávy Sebehodnotící zpráva CAF a na ni navazující Akční plán zlepšování, případně vyhodnocení plnění předchozího Akčního plánu zlepšování. Sebehodnotící zpráva musí obsahovat popis naplnění minimálních kritérií pro udělení daného stupně Ceny MV za model CAF.

Pokud jsou výše uvedené informace součástí Sebehodnotící zprávy, lze na ně pouze odkázat.

[1] *Vyplní pouze uchazeč o cenu MV za inovaci ve veřejné správě*