



MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Kybernetická bezpečnost resortních IS

Ing. Fares Shima
ředitel odboru INF MZČR

Seminář „Zákon o kybernetické bezpečnosti a řízení bezpečnosti IS ve veřejné správě a ve zdravotnictví“

4.11.2014, Poslanecká sněmovna Parlamentu ČR

- Zajištění informačních a komunikačních technologií a kybernetické bezpečnosti v resortu zdravotnictví
- Řízení bezpečnosti informací Ministerstva zdravotnictví ČR
- Projekt „Zajištění kybernetické bezpečnosti resortních IS a komunikační infrastruktury“
- Informační systémy MZČR zahrnuté do kybernetické bezpečnosti

Zajištění informačních a komunikačních technologií a kybernetické bezpečnosti v resortu zdravotnictví

Kompetenční centrum ICT bylo zřízeno v roce 2012 rozhodnutím Ministerstva zdravotnictví ČR v rámci Koordinačního střediska pro resortní zdravotnické informační systémy (KSRZIS) jako reakce na aktivity NBÚ v oblasti přípravy nové legislativy a výstavby Národního centra kybernetické bezpečnosti (NCKB).

Cílem Kompetenčního centra ICT je komplexně a centralizovaně poskytovat služby ICT v rámci resortu zdravotnictví, včetně služeb tvorby koncepční, strategické a provozní bezpečnosti informací, systému řízení a výkonu kontroly bezpečnosti informací.

Poskytování služeb ICT v resortu zdravotnictví:

- Informační systémy elektronického zdravotnictví
- Provozní informační a komunikační systémy v resortní působnosti
- Resortní agendové a kompetenční informační systémy

- Tvorba a rozvoj ICT strategie MZČR
- Implementace platné legislativy, údržbu standardů a norem ČNS ISO/EN, včetně bezpečnostních a provozních směrnic a pravidel
- Bezpečná správa a údržba výpočetní techniky
- Uživatelská podpora prostřednictvím HelpDesku, správa účtů, školení uživatelů

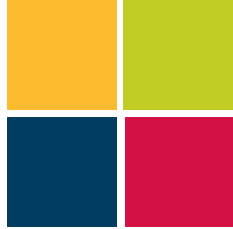
Řízení bezpečnosti informačních systémů Ministerstva zdravotnictví ČR

Ministerstvo zdravotnictví ČR zavedlo v roce 2012 v rámci realizace projektu „**Zavedení systému kvality a systému řízení ochrany informací na MZČR**“, registrační číslo CZ.1.04/4.1.00/48.00053 systém řízení bezpečnosti informací v souladu s normou ČSN EN ISO 27001.

Projekt byl spolufinancován z Operačního programu Lidské zdroje a zaměstnanost (OOPL) a státního rozpočtu.

Systém řízení bezpečnosti informací (ISMS) byl v roce 2012 zaveden na těchto organizacích:

- **Ministerstvo zdravotnictví ČR**
- **Koordinační středisko pro resortní zdravotnické informační systémy (KSRZIS)**
- **Ústav zdravotnických informací a statistiky ČR (ÚZIS ČR)**



Zavedením systému řízení bezpečnosti informací MZČR dosáhlo:

- optimalizace procesů v souladu s normou ISO 27001,
- identifikace procesů pro transformaci a identifikaci šedých zón,
- popisu nových procesů a jejich parametrů,
- pravidelného ověřování funkčnosti systému a nastavení kontrolních mechanismů v rámci interních a externích (recertifikačních) auditů.



Dohledový audit 2013 (Závěrečná zpráva)

- Dokumentace integrovaného systému řízení je velmi pečlivě zpracována,
- Prohlášení o aplikovatelnosti je podrobně zpracováno a plně odpovídá požadavkům normy ISO 27001,
- Metodika analýzy rizik, vlastní analýza rizik, seznam aktiv, katalog hrozeb a zranitelností odpovídají požadavkům normy a jsou řádně spravovány a řízeny.

Oproti roku 2012 došlo k:

- výraznému usazení a doladění systému řízení,
- efektivnímu vypořádání všech neshod z minulého auditu (2012),
- zpracování podrobného popisu procesů a činností,
- provázání systémů QMS a ISMS na systém řízení ministerstva.

Dohledový audit 2013 (Závěrečná zpráva)

Pravidelné dozorové audity vnímá MZČR pozitivně, protože nutí organizaci kontinuálně se problematice bezpečnosti informací věnovat a doporučeními ke zlepšení efektivně pomáhají neustále zvyšovat ochranu a bezpečnost informací.

Příklady doporučení ke zlepšování

- Rozvoj Helpdesku – využití HelpDesku pro hlášení bezpečnostních událostí a incidentů, pro podporu dalších procesů, např. monitoring plnění servisních smluv, SLA dodavatelů aplikací. Rozvoj klasifikací typů požadavků v Helpdesku – **provoz HelpDesku je kontinuálně rozvíjen.**
- Doplnění současných postupů a pravidel MZ pro zálohování emailů a dat na odborových discích do Příkazu ministra (směrnice MZNet) – **bude aktualizována do konce roku 2014.**
- Prověření plánu obnovy informačního systému (popis obnovy, klíčový režim, režim hesel apod.)

Řízení bezpečnosti informací v roce 2014

Vedením schválená „Příručka ochrany informací“ je v současné době přepracována dle požadavků vyhlášky o kybernetické bezpečnosti a její přílohy:

1. Hodnocení a úrovně aktiv
2. Hodnocení rizik
3. Minimální požadavky na kryptografické algoritmy
4. Struktura bezpečnostní dokumentace (21 dílčích politik, 10 souvisejících dokumentů)
5. Formulář hlášení kybernetického bezpečnostního incidentu
6. Formulář oznámení o provedení reaktivního opatření a jeho výsledek
7. Formulář pro hlášení kontaktních údajů

Projekt „Zajištění kybernetické bezpečnosti resortních IS a komunikační infrastruktury“

V září 2014 byl Ministerstvem vnitra schválen projekt podporovaný a z části financovaný z Integrovaného operačního programu (IOP):

„Zajištění kybernetické bezpečnosti resortních IS a komunikační infrastruktury“

Předložený projekt je v souladu s Usnesením vlády ČR ze dne 14. května 2008 č. 536 o strategických projektových záměrech pro čerpání prostředků ze Strukturálních fondů EU v rámci Smart Administration.

Zajištění provozní bezpečnosti je jednou z klíčových priorit Kompetenčního centra ICT v souladu se strategickým řízením a naplňováním požadavků a cílů resortu zdravotnictví v podmínkách legislativy v oblasti kritické infrastruktury a kybernetické bezpečnosti státu.

Projekt „Zajištění kybernetické bezpečnosti resortních IS a komunikační infrastruktury“

Cíle projektu „Zajištění kybernetické bezpečnosti resortních IS a komunikační infrastruktury“:

- **Vypracování resortního strategického dokumentu jednotného systému řízení kybernetické bezpečnosti** v resortu zdravotnictví, v souladu s požadavky platné legislativy, bezpečnostních norem a doporučení a následná implementace jednotných postupů, politik a směrnic do všech organizací resortu,
- **Vytvoření bezpečné technologické platformy** pro komunikaci informačních systémů a zabezpečení požadované kvality, dostupnosti a spolehlivosti chodu resortních služeb,
- **Zajištění bezpečných přístupových bodů** pro komunikaci s informačními systémy resortu a registry.

Současný systém řízení bezpečnosti informací nesplňuje požadavky na centrální systém řízení bezpečnostního monitoringu a centrální bezpečnostní správy v rámci resortu zdravotnictví

Návrh vyhlášky o významných informačních systémech

Národní bezpečnostní úřad a Ministerstvo vnitra předložil **návrh vyhlášky o významných informačních systémech a jejich určujících kritériích**, kterou se stanoví významné informační systémy a jejich určující kritéria.

Mezi významné informační systémy zařadil Národní bezpečnostní úřad 2 informační systémy MZČR (Příloha č. 1 k vyhlášce):

67 Ochrana veřejného zdraví – v gesci sekce NH

68 Zdravotní služby – v gesci ÚZIS ČR

66	MZV	System na pořizování, přenos a zpracování žádostí o cestovní doklad s biometrickými prvky (ePasy)
67	MZ	Ochrana veřejného zdraví
68	MZ	Zdravotní služby
69	MZe	Informační systém VODA
70	MZe	Integrovaný zemědělský registr (IZR)

Návrh vyhlášky o významných informačních systémech

Ochrana veřejného zdraví – systém hygienických registrů

Registr hygieny výživy	SZD – HVY
Registr hygieny dětí a mladistvých	SZD – HDM
Registr předmětů běžného užívání	SZD – PBU
Registr chemických látek a prostředků	SZD – CHLAP
Registr oznamovatelé (předmětem CHLAP a ROP)	SZD – OZN
Registr Hygiena obecná a komunální	SZD – HOK
Informační systém Pandemie	PAN
Registr oznámených potravin (Registr rozhodnutí hlavního hygienika)	SZD-ROP (RHH)
Registr akutních respiračních infekcí	ARI
SZD v Epidemiologii	SZD - EPI
Registr pohlavních nemocí	RPN
Registr tuberkulózy	TBC

Návrh vyhlášky o významných informačních systémech

Zdravotní služby – systém zdravotnických registrů

Národní registr reprodukčního zdraví	NRRZ
Národní registr kardiovaskulárních operací a intervencí	NRKOI
Národní registr kloubních náhrad	NRKN
Národní registr léčby uživatelů drog	NRLUD
Národní registr hospitalizovaných	NRHOSP
Registr intenzivní péče	RIP
Národní registr úrazů	NRU
Národní systém pro hlášení nežádoucích událostí	NSHNU
Národní registr osob trvale vyloučených z dárkovství krve	NROVDK

Národní registr pitev a toxikologických vyšetření prováděných na oddělení soudního lékařství	NRPATV
IS List o prohlídce zemřelého	IS LPZ
IS Pracovní neschopnost (databáze z ČSSZ)	IS PN
IS Demografie	IS DEM
Transplantační registry	TRINIS
Tkáňový registr	TISSIS
Národní registr nemocí z povolání	NRNP
Centrální úložiště výkazů (portál výkazů)	CUV
Centrální úložiště dat (portál hlášení)	CUD

Návrh vyhlášky o významných informačních systémech

Výkonný výbor projektu „**Úprava resortních registrů a konsolidace resortních dat v návaznosti na základní registry VS**“ (eREG) vyjádřil souhlas se zařazením 2 agend MZČR

- **Ochrana veřejného zdraví**
- **Zdravotní služby**

do významných informačních systémů dle návrhu vyhlášky o významných informačních systémech a jejich určujících kritériích.



DĚKUJI ZA POZORNOST

Ing. Fares Shima
ředitel odboru informatiky