Dopady novely ZoKB - aplikace v ISMS resortu MV

Ing. Miroslav Tůma, Ph.D.

ředitel odboru Kybernetické bezpečnosti a koordinace ICT

Ministerstvo vnitra ČR

Program

- Změnový zákon č. 104/2017 Sb.
- Novela zákona o kybernetické bezpečnosti č. 205/2017 Sb.
- Zabezpečení systémů KII a VIS - Povinnosti věcných správců a provozovatelů.
- Kurz kybernetické bezpečnosti pro zaměstnance státní správy.

Změnový zákon č. 104/2017 Sb.

- Účinnost od 1. 7. 2017.
- Zavádí změny především do:
  - Zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.
  - Zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.

Změny v zákoně č. 181/2014 Sb.

§ 104

- Nově přidaná definice bezpečnostní role provozovatele systému.
- Provozovatel systému nový povinným subjektem, kterému se stejně jako správci ukládají povinnosti („správce a provozovatel“).
- Povinným subjektem se provozovatel stává ze zákona v případě naplnění definičních znaků.
- Ukotvení vztahu mezi správcem a provozovatelem systému.
- Zavedení bezpečnostních opatření provozovatelem k 1. lednu 2018.

Zákonné povinnosti provozovatele

- Provozovatel předává správci data a informace, které má k dispozici v souvislosti s provozováním tohoto systému:
  - na vyžádání a bezodkladně (v případě hrozícího kybernetického bezpečnostního incidentu toto předání může nařídit Národní úřad pro kybernetickou a informační bezpečnost (dále NÚKIB),
  - po ukončení provozování systému, kdy kopie těchto dat a informací bezpečně zklikviduje.
- Provozovatel má nárok na úhradu účelně vynaložených nákladů souvisejících s předáním.
- Povinnost hlásit kybernetické bezpečnostního incidenty NÚKIB se vztahuje na správce a nově i na provozovatele.
- Zostřené sankce za nedodržování požadavků zákona, které mohou dosáhnout až 1 000 000 Kč.

Shodné povinnosti správců a provozovatelů

- zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti systému a vést o nich bezpečnostní dokumentaci,
- zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatelů pro systém,
- detekovat kybernetické bezpečnostní události v systému,
- hlásit kybernetické bezpečnostní incidenty NÚKIB.

Novela ZoKB č. 205/2017 Sb.

§ 205

- Účinnost od 1. 8. 2017.
- Zavádí změny do zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění zákona č. 104/2017 Sb.
- Implementuje směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společenské úrovně bezpečnosti sítí a informačních systémů v Evropské unii (směrnici NIS)

- Vznik samostatného Národního úřadu pro kybernetickou a informační bezpečnost se sídlem v Brně (NÚKIB).
- Působnost zákona o kybernetické bezpečnosti rozšířena o nové povinné subjekty a typy služeb.
  - Nové povinné subjekty:
    - Poskytovatel digitální služby.
    - Provozovatel základní služby.
    - Správce a provozovatel informačního systému základní služby.
  - Nově definované typy služeb:
    - Základní služba.
    - Digitální služba.

Základní služba:

- služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení činností v některém z těchto odvětví:
  - Energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, dodávky a rozvody pitné vody, digitální infrastruktura, chemický průmysl.
- Provozovatel základní služby:
  - subjekt, který základní službu poskytuje a je určen NÚKIB.
- Informační systém základní služby:
  - informační systém, na jehož fungování je závislé poskytování základní služby.

§ 205

Digitální služby

Digitální služba:

- Služba informační společnosti, tedy jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu. Spočívá v provozování on-line tržiště, internetového vyhledávače nebo cloud computingu.
- Poskytovatel digitální služby
  - Zákon se vztahuje pouze na poskytovatele digitálních služeb, kteří nejsou malým podnikem, či mikropodnikem.
  - V případě poskytovatele digitální služby v ČR, který nemá sídlo v ČR ani v EU, je povinen si svého zástupce v ČR, resp. EU ustanovit.

- Zavedení nové vzájemné informační povinnosti (neprodleně a prokazatelně):
  - Správce KII nebo VIS musí informovat provozovatele KII nebo VIS, že se stává provozovatelem KII nebo VIS, a že se na něj vztahuje ZoKB.
  - Správce a provozovatel KII musí informovat subjekt zajišťující síť elektronických komunikací, ke které je systém připojen, že se stává subjektem zajišťující významnou síť.
  - Provozovatel základní služby musí informovat, pokud se nejedná o stejný subjekt, správce a provozovatele systému základní služby o jejich určení.

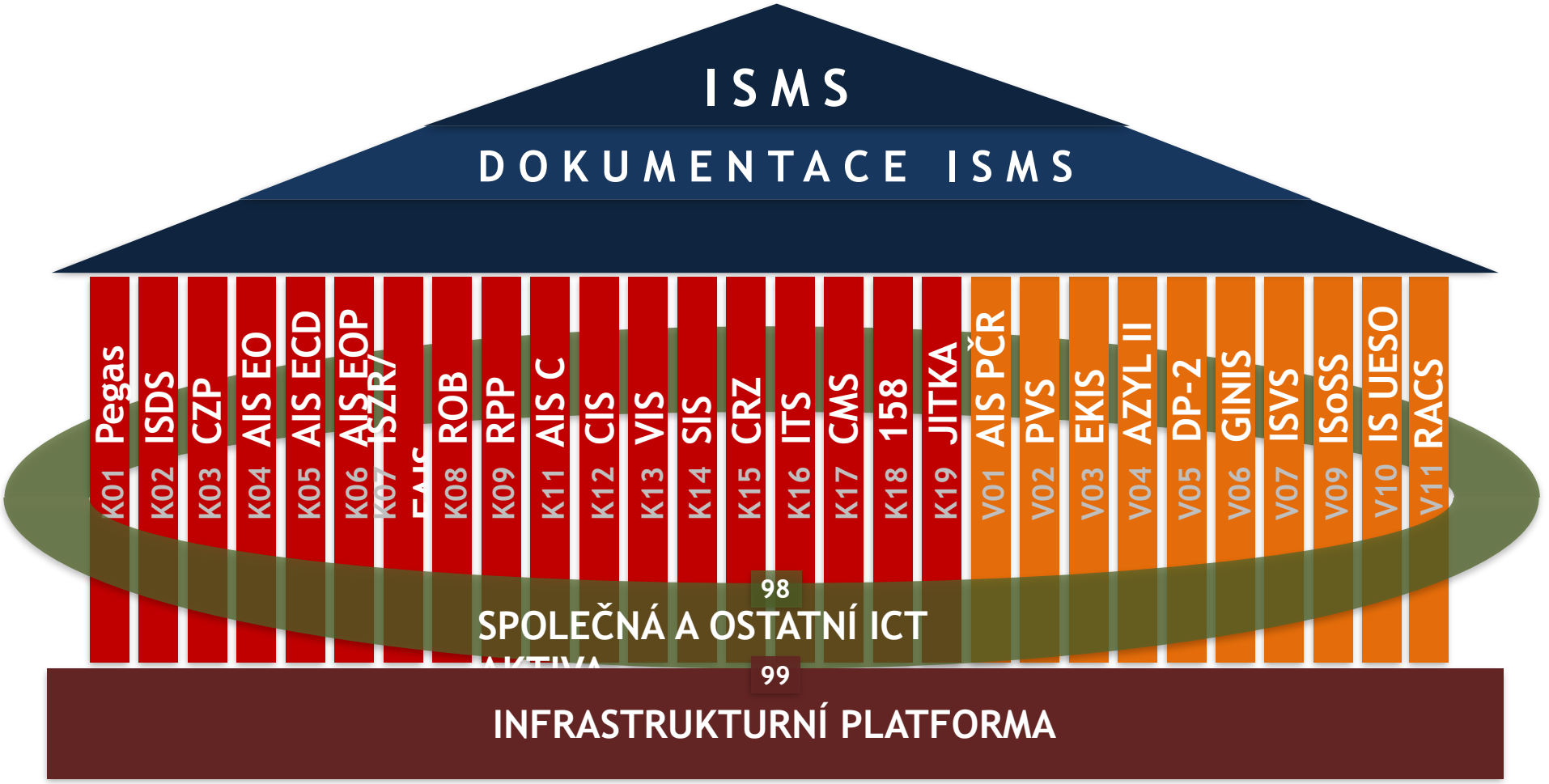
Smluvní vztahy

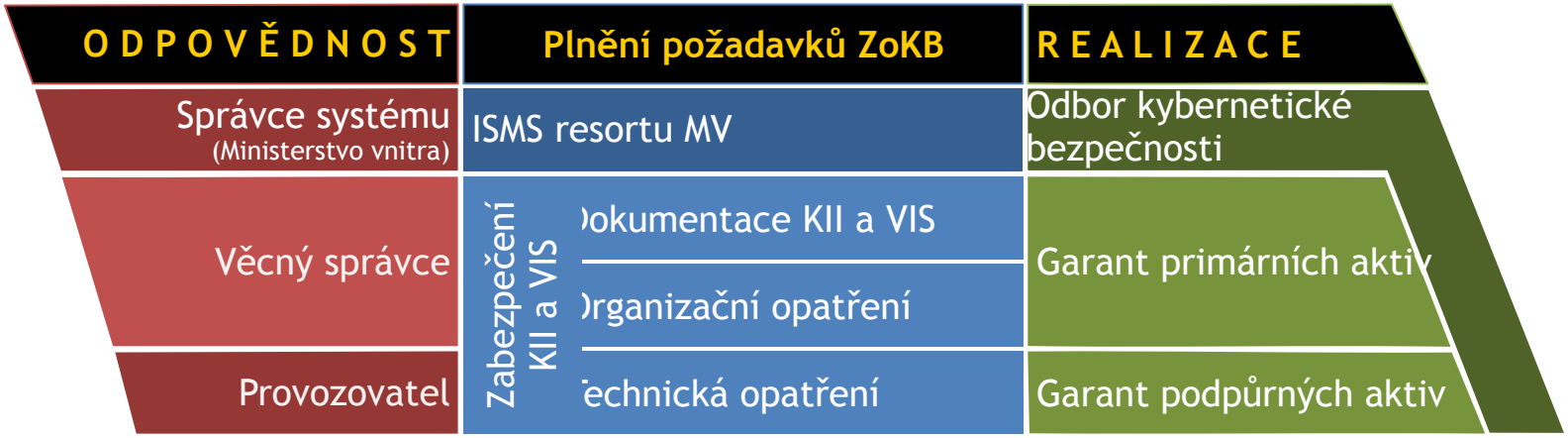
- Nové náležitosti při uzavírání smluv s poskytovatelem cloud computingu v případě orgánů veřejné moci, které jsou povinnými subjekty. Smlouvy musí nově obsahovat:
  - zakotvení povinnosti poskytovatele služeb respektovat bezpečnostní politiku odběratele služeb,
  - stanovení úrovně poskytovaných služeb,
  - systém schvalování subdodavatelů služby cloud computingu,
  - podmínky ukončení smluvního vztahu z pohledu bezpečnosti,
  - řízení kontinuity činností v souvislosti s poskytovanou službou cloud computingu,
  - určení vlastníka uchovávaných dat,
  - dohoda o důvěrnosti smluvního vztahu,
  - stanovení úrovně ochrany dat z pohledu důvěrnosti, dostupnosti a integrity,
  - pravidla zákaznického auditu.

Zabezpečení KII a VIS v resortu MV
Úprava povinností správců a provozovatelů

- Organizace kybernetické bezpečnosti v resortu MV.
- Bezpečnostní role a jejich kompetence - zabezpečení systémů KII a VIS:
  - Bezpečnostní dokumentace.
  - Organizační opatření.
  - Technická opatření.
- Dohledové centru eGOV (DCeGOV).

Rozsah ISMS resortu MV





- ZoKB definuje správce systému, provozovatele a garanty aktiv.
- Role věcného správce je vymezena organizačním řádem MV.

Nadřízená role	Osoba	Činnost	Podřízená role	Osoba
Správce systému	Ministr vnitra	Jmenuje	Manažer kybernetické bezpečnosti	Fyzická osoba
Věcný správce	Ředitel odboru	Určuje	Garant primárních aktiv	Fyzická osoba
			Technický správce	Útvar MV
			Administrátor aplikace	Fyzická osoba
Provozovatel	Ředitel odboru nebo externí poskytovatel	Určuje	Garant podpůrných aktiv	Fyzická osoba
			Administrátor systému	Fyzická osoba

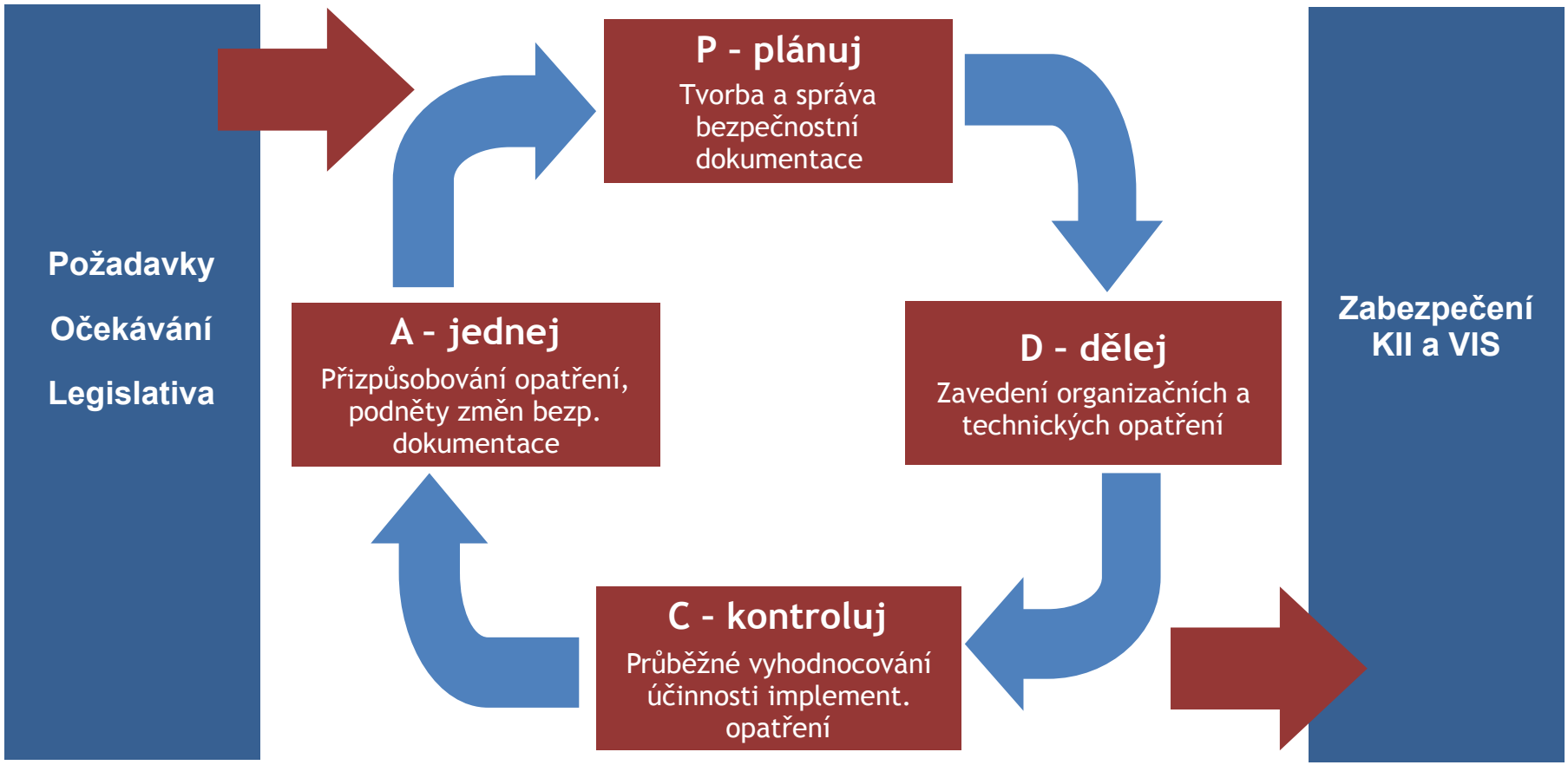
- Osoby určené do role garantů ustanovuje náměstek pro řízení sekce ICT, který současně zastává funkci místopředsedy výboru pro řízení kybernetické bezpečnosti v resortu MV.

Personální kompetence bezpečnostních rolí

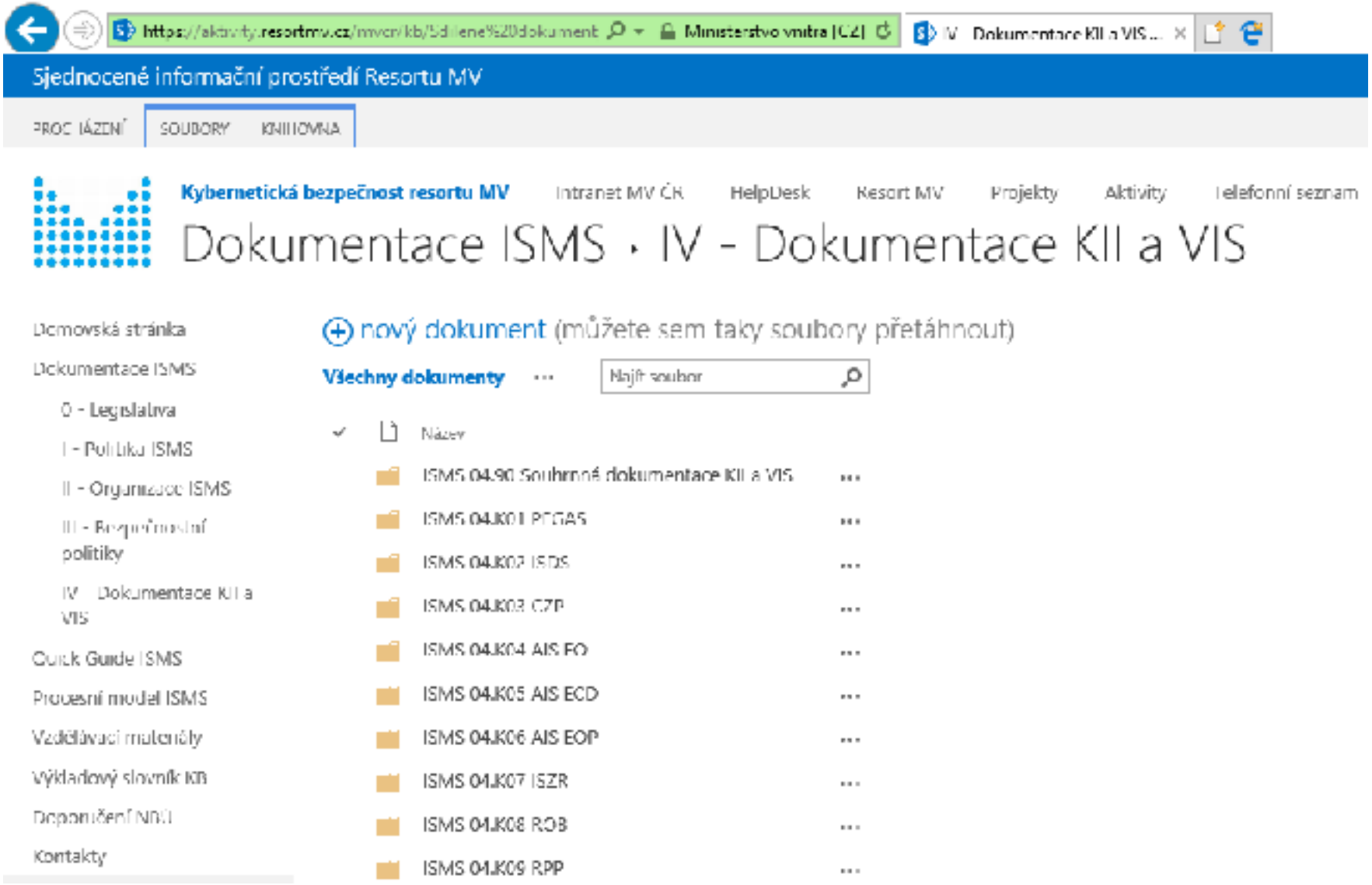
Věcné kompetence bezpečnostních rolí

Role	Činnost	Kontakt pro
Správce systému	Odpovídá za plnění požadavků ZoKB na systémy KII a VIS resortu MV.	--
Manažer KB	Odpovídá za systém řízení bezpečnosti informací a zastává tuto roli za všechny KII a VIS resortu MV.	--
Věcný správce	Určuje garanty podpůrných aktiv, odpovídá za plnění požadavků ISMS pro příslušný systém KII nebo VIS.	OKB, NÚKIB
Provozovatel	Určuje garanty podpůrných aktiv, odpovídá za plnění požadavků ISMS pro příslušný systém KII nebo VIS.	OKB, NÚKIB
Garant primárních aktiv	Plní požadavky ISMS pro příslušný systém KII nebo VIS, zejména v oblasti organizačních opatření	OKB
Garant podpůrných aktiv	Plní požadavky ISMS pro příslušný systém KII nebo VIS, zejména v oblasti technických opatření	OKB
Technický správce	Realizuje rozvoj a vývoj příslušného KII nebo VIS, a to i v oblasti KB. Současně stanovuje technické parametry provozu systémů, jež naplňuje provozovatel.	OKB
Administrátor aplikace	Zajišťuje bezpečnostní aspekty správy systému KII nebo VIS na funkční, resp. uživatelské úrovni.	--
Administrátor systému	Na technické úrovni zajišťuje bezpečnostní aspekty správy systému KII nebo VIS.	OKB, NÚKIB

Čtyři kroky zabezpečení systémů KII a VIS



- Bezpečnostní dokumentaci každého ze systémů KII a VIS resortu MV spravuje osoba určená věcným správcem, tzv. správce bezpečnostní dokumentace ISMS. Samotnou tvorbu lze ale rozdělit a přidělit dle příslušných věcných kompetencí:
  - Garant primárních aktiv - organizační témata.
  - Garant podůrných aktiv - technická témata.
- Individuální bezpečnostní dokumentace systémů KII a VIS nesmí být v rozporu se schválenou podobou resortní dokumentace ISMS.
- Zpracovatelé se musí řídit principy řízení bezpečnostní dokumentace ISMS v resortu MV ISMS 02.03 Řízená dokumentace, které mimo jiné vyžadují:
  - Použití schválených šablon pro programy Microsoft Word a Microsoft Excel.
  - Publikaci dokumentů v sekci KB Sdíleného informačního prostředí resortu MV.



Kybernetická bezpečnost v prostředí SIP

Principy tvorby bezpečnostní dokumentace

- Struktura bezpečnostní dokumentace se v souladu s VyKB dělí na
  - Bezpečnostní politiky.
  - Ostatní bezpečnostní dokumentaci.
- Zpracovatelé mohou ve spolupráci s OKB při tvorbě bezpečnostních politik postupovat následujícími způsoby:
  - převzít plné znění centrálního dokumentu z resortní dokumentace ISMS, na který se v rámci připravených šablon odvolají,
  - převzít znění centrálního dokumentu formou odkazu a současně popsat modifikace, tj. zpřesnění a specifika konkrétního systému,
  - v odůvodněných případech vytvořit nový vlastní dokument.
- Zpracování většiny dokumentů z části ostatní bezpečnostní dokumentace centrálně zajišťuje OKB. Určení garanti primárních a podpůrných aktiv aktivně spolupracují na jejich přípravě a aktualizaci.

BD - Bezpečnostní politiky

Č.	Oblast	KII	VIS	DISMS	Změny	Gesce	Spolupráce	Šablona
1	Systém řízení bezpečnosti informací	✓	✓	ISMS 01.01	NE	OKB	-	
2	Řízení vztahů s dodavateli / řízení dodavatelů	✓	✓	ISMS 03.01.01	ANO	GPrA	OKB, GPoA	
3	Bezpečnost lidských zdrojů	✓	✓	ISMS 03.01.03	NE	OKB	--	
4	Řízení přístupu	✓	✓	ISMS 03.01.05	ANO	GPrA	OKB, GPoA	
5	Zálohování a obnova	✓	✓	ISMS 03.01.07	ANO	GPoA	OKB, GPrA	
6	Řízení technických zranitelností	✓	✗	ISMS 03.01.09	ANO	GPoA	OKB, GPrA	
7	Poskytování a nabývání licencí programového vybavení a informací	✓	✓	ISMS 03.01.11	NE	OKB	--	
8	Ochrana osobních údajů	✓	✓	ISMS 03.01.13	NE	OKB		
9	Bezpečnost komunikační sítě	✓	✗	ISMS 03.01.15	ANO	GPoA	OKB, GPrA	
10	Nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí	✓	✓	ISMS 03.01.17	NE	OKB		
11	Používání kryptografické ochrany	✓	✓	ISMS 03.01.19	ANO	GPoA	OKB, GPrA	
12	Organizační bezpečnost	✓	✓	ISMS 02.01.01	NE	OKB	--	
13	Klasifikace aktiv	✓	✓	ISMS 03.01.02	NE	OKB	--	
14	Řízení provozu a komunikací	✓	✓	ISMS 03.01.04	ANO	GPoA	OKB, GPrA	
15	Bezpečné chování uživatelů	✓	✓	ISMS 03.01.06	ANO	GPrA	OKB, GPoA	
16	Bezpečné předávání a výměna informací	✓	✗	ISMS 03.01.08	ANO	GPrA	OKB, GPoA	
17	Bezpečné používání mobilních zařízení	✓	✗	ISMS 03.01.10	ANO	GPoA	OKB, GPrA	
18	Dlouhodobé ukládání a archivace informací	✓	✗	ISMS 03.01.12	ANO	GPrA	OKB, GPoA	
19	Fyzická bezpečnost	✓	✗	ISMS 03.01.14	ANO	GPoA	OKB, GPrA	
20	Ochrana před škodlivým kódem	✓	✓	ISMS 03.01.16	NE	OKB	--	
21	Využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí	✓	✗	ISMS 03.01.18	ANO	OKB	--	

ISMS 02.01.01.T03

Č.	Název	KII	VIS	DISMS	Metodika	Změny	Gesce	Spolupráce	Šablona
1	Zpráva z auditu kybernetické bezpečnosti	✓	✗	ISMS 05.15	ISMS 03.02.01	NE	AUD	PR, OKB	ISMS 02.03.01.P05
2	Zpráva z přezkoumání systému řízení bezpečnosti informací	✓	✓	ISMS 05.03	ISMS 02.04.05	NE	OKB	CPrA, GPoA	--
3	Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik	✓	✓	ISMS 03.01.02.P01	ISMS	NE	OKB		--
4	Zpráva o hodnocení aktiv a rizik	✓	✓	ISMS 04.50	ISMS 03.01.02.P01	NE	OKB	GPrA, GPoA	
5	Prohlášení o aplikovatelnosti	✓	✓	ISMS 01.50	ISMS ?	NE	OKB	CPrA, GPoA	--
6	Plán zvládání rizik	✓	✓	ISMS 05.15	ISMS ?	NE	OKB	GPrA, GPoA	--
7	Plán rozvoje bezpečnostního povědomí	✓	✓	ISMS 05.05.10	ISMS ?	ANO	OKB	GPrA, GPoA	ISMS 02.03.01.P07
8	Zvládání kybernetických bezpečnostních incidentů	✓	✓	ISMS 03.03.01	ISMS --	NE	OKB	GPrA, GPoA	
9	Strategie řízení kontinuity činností	✓	✓	ISMS 03.04.01	ISMS ?	ANO	CPrA, GPoA,	VS, PR, OKB	ISMS 02.03.01.P08
10	Přehled právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků	✓	✓	ISMS 00.50	ISMS	ANO	VS, PR	GPrA, GPoA,	ISMS 02.03.01.P09

BD – Ostatní bezpečnostní dokumentace

- Stanovování a zavádění bezpečnostních opatření primárně vychází z provedeného hodnocení aktiv a rizik. Jeho realizaci centrálně řídí a zajišťuje OKB u všech systémů KII a VIS resortu MV.
- Transformované výstupy hodnocení aktiv a rizik obsahuje plán zvládání rizik resortu MV, který schvaluje výbor pro řízení kybernetické bezpečnosti:
  - **ISMS 05.45.01-2017.01 Plán zvládání rizik KB resortu MV pro rok 2017.**
- Věcní správci a provozovatelé se v oblasti implementace opatření řídí pokyny OKB a spolupracují s ním na zavádění všech typů opatření.
- Garanti aktiv konzultují s OKB veškerá další identifikovaná rizika a relevantní opatření, která nevyplynula z hodnocení aktiv a rizik.

Organizační bezpečnostní opatření

Č.	Oblast	VyKB	PZR	Realizace opatření	Gesce	Spolupráce
1	Systém řízení bezpečnosti informací	§ 3	14	resortní opatření	OKB	
2	Řízení rizik	§ 4	14.1	resortní opatření	OKB	
3	Bezpečnostní politika	§ 5	13.1	resortní opatření + individuální úprava	OKB	VS, PR
4	Organizační bezpečnost	§ 6	14.6	resortní opatření	OKB	
5	Stanovení bezpečnostních požadavků na dodavatele	§ 7	14.3	resortní opatření + individuální úprava	OKB	VS, PR
6	Řízení aktiv	§ 8	4.1	resortní opatření	OKB	
7	Bezpečnost lidských zdrojů	§ 9	14.7	resortní opatření + individuální úprava	OKB	VS, PR
8	Řízení provozu a komunikací KII nebo VIS	§ 10	2	resortní opatření + individuální úprava	OKB	VS, PR
9	Řízení přístupu osob ke KII nebo VIS	§ 11	1	resortní opatření + individuální úprava	OKB	VS, PR
10	Akvizice, vývoj a údržba KII a VIS	§ 12	14.5	resortní opatření + individuální úprava	OKB	VS, PR
11	Zvládání KBU a KBI	§ 13	2	resortní opatření	OKB	
12	Řízení kontinuity činností	§ 14	13.2	resortní opatření + individuální úprava	OKB	VS, PR
13	Kontrola a audit KII a VIS	§ 15	13.4	resortní opatření	AUD	

Č.	Oblast	VyKB	PZR	Realizace opatření	Gesce	Spolupráce
14	Fyzická bezpečnost	§ 16	12	PZR: Zabezpečení budov		
15	Nástroj pro ochranu integrity komunikačních sítí	§ 17	5.1	PZR: Správa bezpečnosti sítí	OKB	PR
17	Nástroj pro ověřování identity uživatelů	§ 18	1	PZR: Identity Management	OKB	PR
18	Nástroj pro řízení přístupových oprávnění	§ 19	1	PZR: Identity Management	OKB	PR
19	Nástroj pro ochranu před škodlivým kódem	§ 20	2.4	PZR: Ochrana před malwarem	OKB	PR
20	Nástroj pro zaznamenávání činnosti uživatelů a administrátorů KII a VIS	§ 21	14.2	PZR: Pravidlo čtyř očí u operací prováděných administrátory	OKB	PR
21	Nástroj pro detekci KBU	§ 22	2	PZR: Kontinuální rozvoj Dohledového centra eGovernmentu	OKB	PR
22	Nástroj pro sběr a vyhodnocení KBU	§ 23	2	PZR: Kontinuální rozvoj Dohledového centra eGovernmentu	OKB	PR
23	Aplikační bezpečnost	§ 24	5	PZR: OSC RED Team	OKB	PR
24	Kryptografické prostředky	§ 25	10	PZR: Šifrování dat	OKB	PR
25	Nástroj pro zajišťování úrovně dostupnosti informací	§ 26	5.1	PZR: Správa bezpečnosti sítí	OKB	PR
26	Bezpečnost průmyslových a řídicích systémů	§ 27	-	v resortu MV neaplikovatelné	--	--

Technická bezpečnostní opatření

Povinnosti vůči Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB):

- oznamovat prostřednictvím OKB povinně uváděné kontaktní osoby, konkrétně provozovatele a správce systému, pro jednotlivé KII a VIS,
- ohlašovat prostřednictvím Dohledového centra eGovernmentu (DCeGOV) kybernetické bezpečnostní incidenty.

Povinnosti vůči OKB, resp. vůči manažerovi kybernetické bezpečnosti resortu MV :

- respektovat parametry a požadavky ISMS resortu MV,
- ohlašovat na DCeGOV kybernetické bezpečnostní události,
- předkládat ke schválení bezpečnostní dokumentace systémů KII a VIS,
- řídit se pokyny OKB v oblasti implementace bezpečnostních opatření,
- hlásit změny kontaktních osob ve všech bezpečnostních rolích.

Kurz kybernetické bezpečnosti pro zaměstnance státní správy

E-learningový kurz kybernetické bezpečnosti

- Vychází z:
  - Akčního plánu pro rozvoj digitálního trhu.
  - Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 - 2020 (bod F.3.01).
- Spolupráce:
  - Národní úřad pro kybernetickou a informační bezpečnost.
  - Ministerstvo vnitra.
  - Úřad vlády ČR.
  - Institut pro veřejnou správu.
- Realizaci kurzu zajišťuje Institut pro veřejnou správu Praha.
- Pilotní test kurzu bude na Ministerstvu vnitra zahájen v říjnu 2017.

E-learningový kurz kybernetické bezpečnosti

Modul A: Úvod do kybernetické bezpečnosti

- Cílem kurzu je získání povědomí a osvojení základních návyků digitální hygieny zaměstnanců státní správy.
- Dvouměsíční kurz.
- 14 kapitol s praktickými ukázkami a průběžnými testy.
- Úspěšný absolvent musí dosáhnout hranice 75 % správných odpovědí na 28 otázek závěrečného testu.
- Získání certifikátu, který je zařazen do osobního spisu státního zaměstnance.

Modul B: „Pro pokročilé uživatele“

- Kurz je určen konkrétním bezpečnostním rolím dle ZoKB a vybraným pokročilým uživatelům, např. vedoucím zaměstnancům.
- Předpokládá základní znalost zásad bezpečného používání ICT a internetu a povinností ukládaných ZoKB.

E-learningový kurz kybernetické bezpečnosti

… děkuji za pozornost a Váš čas, přeji hezký den

Ing. Miroslav Tůma, Ph.D.

ředitel odboru Kybernetické bezpečnosti a koordinace ICT

Ministerstvo vnitra ČR