MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Kybernetická bezpečnost MV

Ing. Miroslav Tůma Ph. D.

odbor kybernetické bezpečnosti a koordinace ICT

miroslav.tuma@mvcr.cz

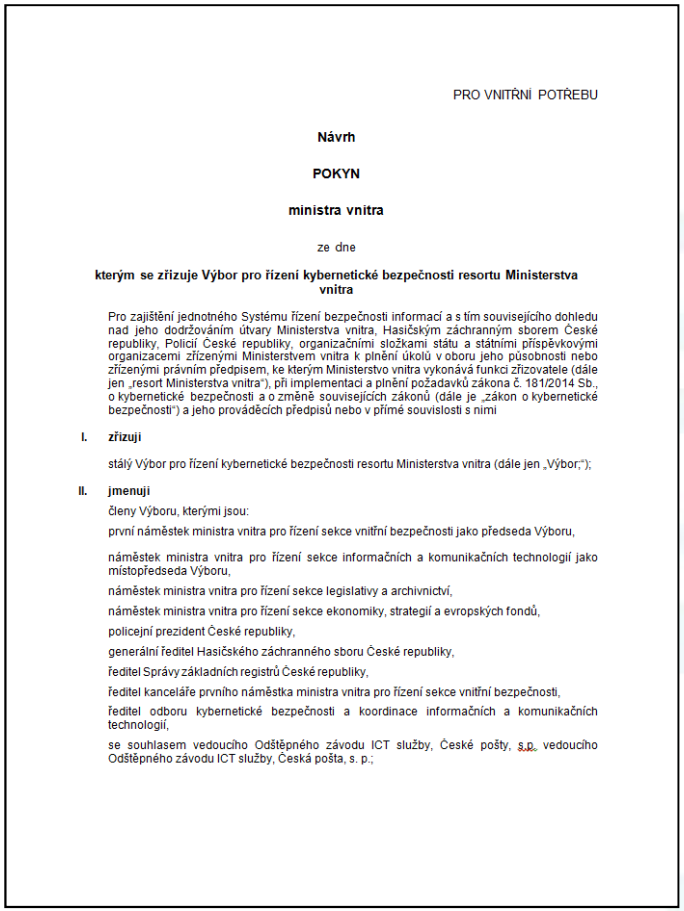
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Agenda

1. Pokyn MV - ustanovení Výboru pro řízení kybernetické bezpečnosti
2. Politika ISMS
3. Dokumentace ISMS
4. Analýza rizik VIS – AIS PČR a PVS
5. Plán bezpečnostního povědomí - vzdělávání

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Pokyn MV - ustanovení Výboru pro řízení KB



PRO VNITŘNÍ POTŘEBU

Návrh

POKYN

ministra vnitra

ze dne

kterým se zřizuje Výbor pro řízení kybernetické bezpečnosti resortu Ministerstva vnitra

Pro zajištění jednotného Systému řízení bezpečnosti informací a s tím souvisejícího dohledu nad jeho dodržováním útvary Ministerstva vnitra, Hasičským záchranným sborem České republiky, Policií České republiky, organizačními složkami státu a státními příspěvkovými organizacemi zřízenými Ministerstvem vnitra k plnění úkolů v oboru jeho působnosti nebo zřízenými právním předpisem, ke kterým Ministerstvo vnitra vykonává funkci zřizovatele (dále jen „resort Ministerstva vnitra"), při implementaci a plnění požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále je „zákon o kybernetické bezpečnosti") a jeho prováděcích předpisů nebo v přímé souvislosti s nimi

I. **zřizuji**

stálý Výbor pro řízení kybernetické bezpečnosti resortu Ministerstva vnitra (dále jen „Výbor,");

II. **jmenuji**

členy Výboru, kterými jsou:

první náměstek ministra vnitra pro řízení sekce vnitřní bezpečnosti jako předseda Výboru,

náměstek ministra vnitra pro řízení sekce informačních a komunikačních technologií jako místopředseda Výboru,

náměstek ministra vnitra pro řízení sekce legislativy a archivnictví,

náměstek ministra vnitra pro řízení sekce ekonomiky, strategií a evropských fondů,

policejní prezident České republiky,

generální ředitel Hasičského záchranného sboru České republiky,

ředitel Správy základních registrů České republiky,

ředitel kanceláře prvního náměstka ministra vnitra pro řízení sekce vnitřní bezpečnosti,

ředitel odboru kybernetické bezpečnosti a koordinace informačních a komunikačních technologií,

se souhlasem vedoucího Odštěpného závodu ICT služby, České pošty, s.p. vedoucího Odštěpného závodu ICT služby, Česká pošta, s. p.;

Zřízení Výboru pro řízení kybernetické bezpečnosti resortu Ministerstva vnitra

Příloha č.1 – Statut Výboru pro řízení kybernetické bezpečnosti resortu Ministerstva vnitra

- *Kompetence a odpovědnost Výboru*
- *Složení Výboru KB*
- *Předseda, místopředseda a tajemník Výboru*
- *Členové Výboru*
- *Administrativní zajištění činnosti Výboru*
- *Pracovní skupiny*

Příloha č.2 – Jednací řád Výboru pro řízení kybernetické bezpečnosti resortu MV

- *Zajištění činnosti Výboru*

Návrh na pověření Manažera kybernetické bezpečnosti

Návrh na pověření Architekta kybernetické bezpečnosti

Návrh na pověření Auditora kybernetické bezpečnosti

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Agenda

1. Pokyn MV - ustanovení Výboru pro řízení kybernetické bezpečnosti
2. Politika ISMS
3. Dokumentace ISMS
4. Analýza rizik VIS – AIS PČR a PVS
5. Plán bezpečnostního povědomí - vzdělávání

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Politika ISMS

1. Centrální řízení KB prostřednictvím ISMS včetně řízení kybernetických bezpečnostních incidentů a komunikace s NBÚ a NCKB

2. Komplexní audit minimálně jednou ročně

3. Důsledné využívání standardizace a ověřených technologií

4. měr rozvoje KB

-respektuje platnou republikovou a interní legislativu

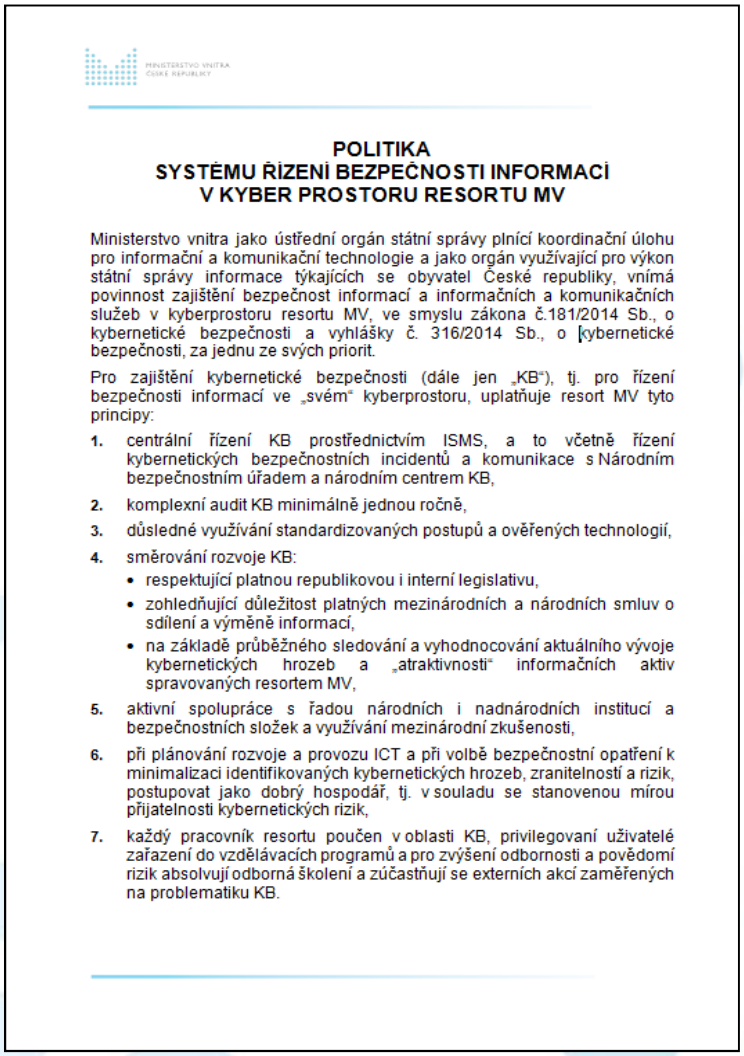
- zohlednění platných mezinárodních a národních smluv ohledně výměny informací

- realizován na základě sledování a vyhodnocování kybernetických hrozeb

5. Aktivní spolupráce při řešení KB s národními i nadnárodními institucemi včetně bezpečnostních složek

6. Plánovitý rozvoj a provoz ICT při volbě bezpečnostních opatření k minimalizaci kybernetických hrozeb

7. Bezpečnostní povědomí a plánovité vzdělávání v odborných kursech se zaměřením na problematiku KB



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

POLITIKA
SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ
V KYBER PROSTORU RESORTU MV

Ministerstvo vnitra jako ústřední orgán státní správy plnící koordinační úlohu pro informační a komunikační technologie a jako orgán využívající pro výkon státní správy informace týkajících se obyvatel České republiky, vnímá povinnost zajištění bezpečnost informací a informačních a komunikačních služeb v kyberprostoru resortu MV, ve smyslu zákona č.181/2014 Sb., o kybernetické bezpečnosti a vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti, za jednu ze svých priorit.

Pro zajištění kybernetické bezpečnosti (dále jen „KB“), tj. pro řízení bezpečnosti informací ve „svém“ kyberprostoru, uplatňuje resort MV tyto principy:

1. centrální řízení KB prostřednictvím ISMS, a to včetně řízení kybernetických bezpečnostních incidentů a komunikace s Národním bezpečnostním úřadem a národním centrem KB,
2. komplexní audit KB minimálně jednou ročně,
3. důsledné využívání standardizovaných postupů a ověřených technologií,
4. směrování rozvoje KB:
   - respektující platnou republikovou i interní legislativu,
   - zohledňující důležitost platných mezinárodních a národních smluv o sdílení a výměně informací,
   - na základě průběžného sledování a vyhodnocování aktuálního vývoje kybernetických hrozeb a „atraktivnosti“ informačních aktiv spravovaných resortem MV,
5. aktivní spolupráce s řadou národních i nadnárodních institucí a bezpečnostních složek a využívání mezinárodní zkušenosti,
6. při plánování rozvoje a provozu ICT a při volbě bezpečnostní opatření k minimalizaci identifikovaných kybernetických hrozeb, zranitelností a rizik, postupovat jako dobrý hospodář, tj. v souladu se stanovenou mírou přijatelnosti kybernetických rizik,
7. každý pracovník resortu poučen v oblasti KB, privilegovaní uživatelé zařazení do vzdělávacích programů a pro zvýšení odbornosti a povědomí rizik absolvují odborná školení a zúčastňují se externích akcí zaměřených na problematiku KB.

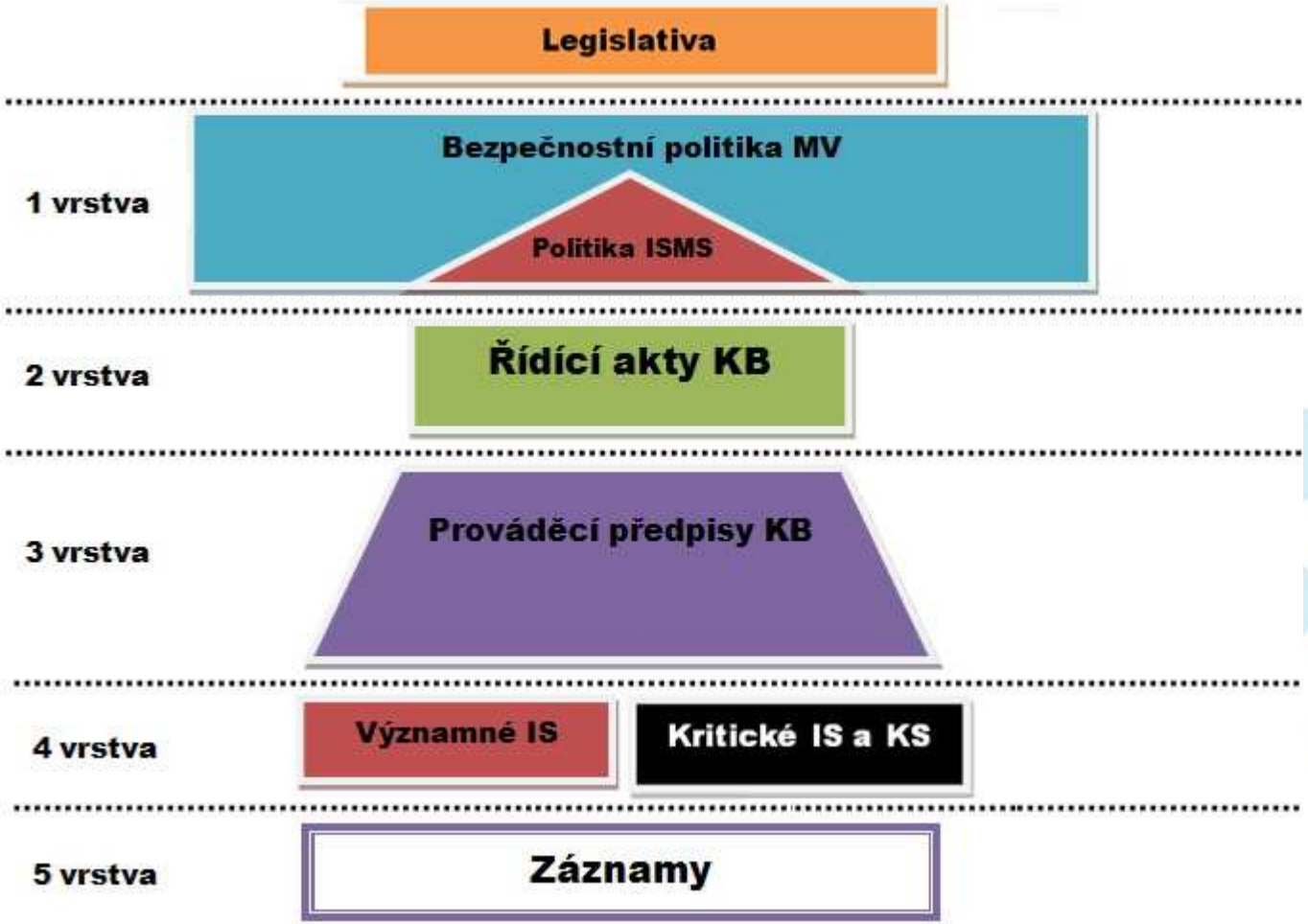
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Agenda

1. Pokyn MV - ustanovení Výboru pro řízení kybernetické bezpečnosti
2. Politika ISMS
3. Dokumentace ISMS
4. Analýza rizik VIS – AIS PČR a PVS
5. Plán bezpečnostního povědomí - vzdělávání

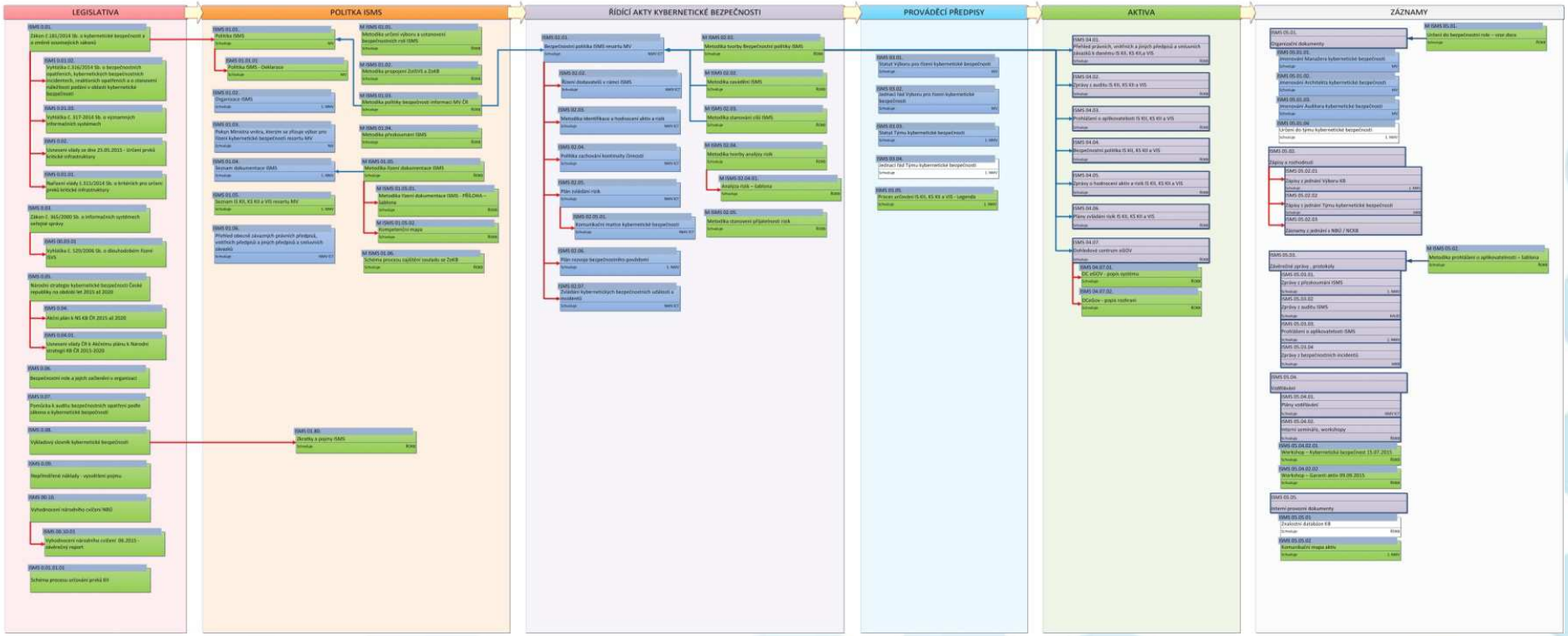
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dokumentace ISMS



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dokumentace ISMS



LEGENDA:

ZKRATKY:
1. NMV – 1. NÁMĚSTEK MV
KAUD – AUDITOR PRO KYBERNETICKOU BEZPEČNOST
MKB - MANAŽER KYBERNETICKÉ BEZPEČNOSTI
MV – MINISTR VNITRA
NMV ICT – NMV PRO INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE
ŘOKB - ŘEDITEL ODBORU PRO KYBERNETICKOU BEZPEČNOST
ZoKB - ZÁKON Č.181/2014 SB., O KYBERNETICKÉ BEZPEČNOSTI

STAV DOKUMENTU:
SCHVÁLENO
HOTOVO
ROZPRACOVÁNO
NEZAHÁJENO

VAZBY:
PODŘÍZENOST
METODIKA

SYMBOLY:
SLOŽKA
DOKUMENT

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dokumentace ISMS – vrstva legislativy

Legislativa

mezinárodní standardy, předpisy, zákony ČR, prováděcí předpisy a pomůcky

- *Zákon č.181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů*
- *Vyhláška č.316/2014 Sb. o kybernetické bezpečnosti*
- *Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích*
- *Usnesení vlády ze dne 25.05.2015 – Určení prvků kritické infrastruktury*
- *Nařízení vlády č.315/2014 Sb. o kritériích pro určení prvků kritické infrastruktury*
- *Zákon č.365/2000 Sb. o informačních systémech veřejné správy*
- *Vyhláška č.529/2006 Sb., o dlouhodobém řízení ISVS*
- *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020*
- *Akční plán k NS KB ČR 2015 až 2020*
- *Usnesení vlády ČR k Akčnímu plánu Národní strategie KB ČR na období let 2015 až 2020*
- *Bezpečnostní role a jejich začlenění v organizaci*
- *Pomůcka k auditu bezpečnostních opatření podle zákona o kybernetické bezpečnosti*
- *Výkladový slovník kybernetické bezpečnosti (3. vydání 2015)*
- *Nepřiměřené náklady – vysvětlení pojmu*
- *Vyhodnocení národního cvičení NBÚ*
- *Schéma procesu určování prvků KII*

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dokumentace ISMS – 1. vrstva

- *Politika ISMS*
- *Organizace ISMS*
- *Pokyn MV, kterým se zřizuje Výbor pro řízení kybernetické bezpečnosti resortu MV*
- *Seznam dokumentace ISMS*
- *Seznam IS KII, KS KII a VIS*
- *Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků*
- *Zkratky a pojmy ISMS*

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dokumentace ISMS – 2. vrstva

Řídící akty KB

- *Bezpečnostní politika ISMS resortu MV*
- *Řízení dodavatelů v rámci ISMS*
- *Metodika identifikace a hodnocení aktiv a rizik*
- *Politika zachování kontinuity činností*
- *Plán zvládání rizik*
- *Plán rozvoje bezpečnostního povědomí*
- *Zvládání kybernetických bezpečnostních událostí a incidentů*

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

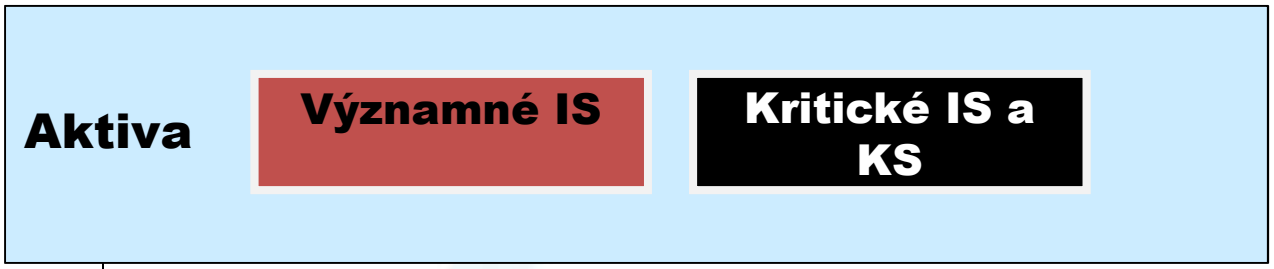
Dokumentace ISMS – 3. vrstva

Prováděcí předpisy KB

- *Statut Výboru pro řízení kybernetické bezpečnosti*
- *Jednací řád Výboru pro řízení kybernetické bezpečnosti*
- *Statut Týmu kybernetické bezpečnosti*
- *Jednací řád Týmu kybernetické bezpečnosti*
- *Proces určování IS KII, KS KII a VIS - Legenda*

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dokumentace ISMS – 4. vrstva



- *Přehled právních, vnitřních a jiných předpisů a smluvních závazků k danému IS KII, KS KII a VIS*
- *Zprávy z auditu IS KII, KS KII a VIS*
- *Prohlášení o aplikovatelnosti IS KII, KS KII a VIS*
- *Bezpečnostní politika IS KII, KS KII a VIS*
- *Zpráva o hodnocení aktiv a rizik IS KII, KS KII a VIS*
- *Plán zvládání rizik IS KII, KS KII a VIS*
- *Dohledové centrum eGOV*

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dokumentace ISMS – 5. vrstva

Záznamy

- ***Organizační dokumenty*** *(Jmenování Manažera KB, Architekta KB, Auditora KB, určení týmu KB)*
- ***Zápisy a rozhodnutí*** *(jednání Výboru KB, týmu KB, NBÚ)*
- ***Závěrečné zprávy, protokoly*** *(zprávy z přezkoumání ISMS, auditu ISMS, prohlášení o aplikovatelnosti, zprávy z bezpečnostních incidentů)*
- ***Vzdělávání*** *(plán vzdělávání, interní semináře, workshopy, prezentace,)*
- ***Interní provozní dokumenty*** *(znalostní databáze KB, komunikační mapa aktiv)*

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Agenda

1. Pokyn MV -ustanovení Výboru pro řízení kybernetické bezpečnosti
2. Politika ISMS
3. Dokumentace ISMS
4. Analýza rizik VIS – AIS PČR a PVS
5. Plán bezpečnostního povědomí - vzdělávání

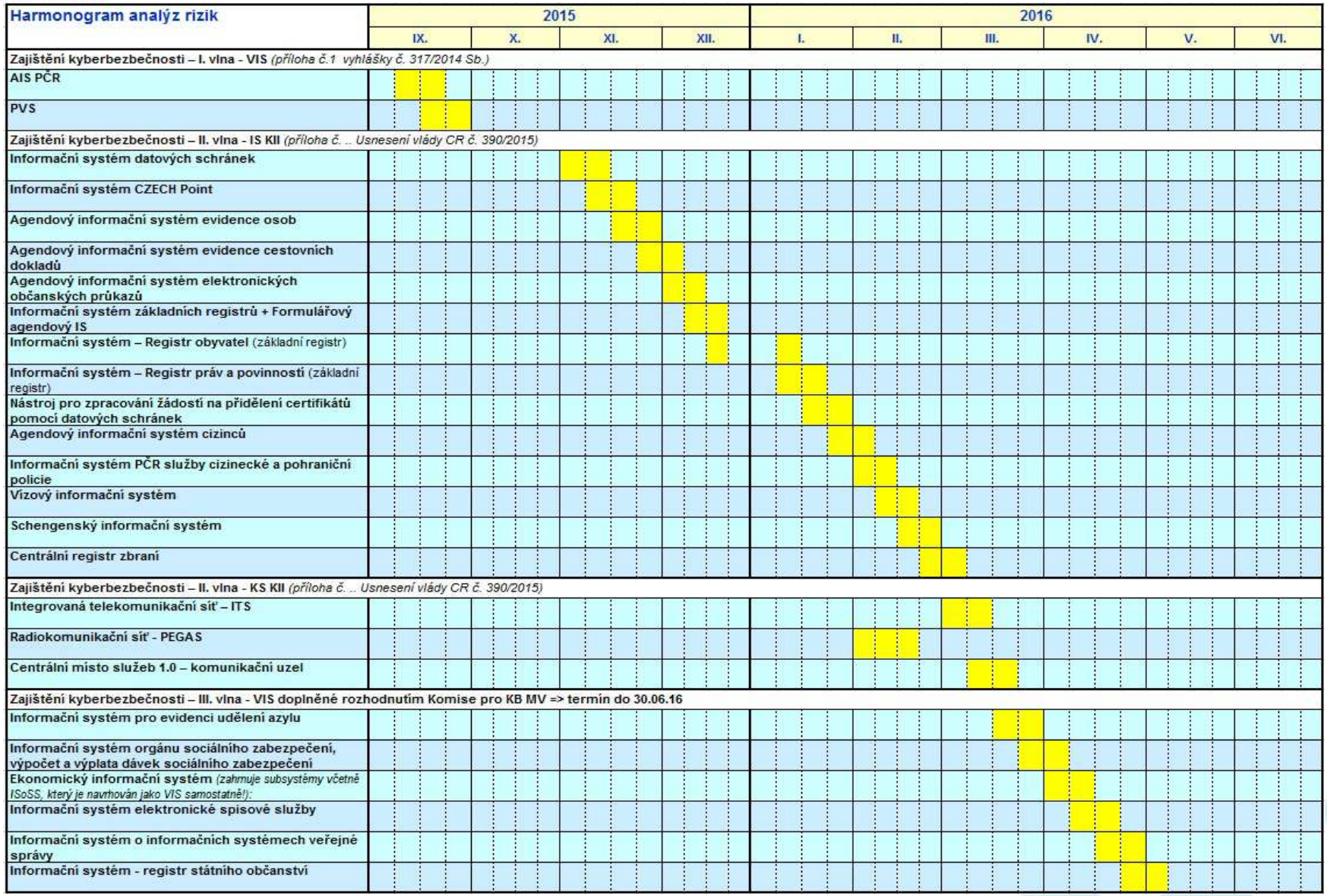
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Analýza rizik – VIS – AIS PČR a PVS

- Příprava proběhla ve dvou fázích:
  - 15.07.2015 – Workshop – Kybernetická bezpečnost
  - 09.09.2015 – Workshop – Garanti aktiv (příprava analýz rizik)
- Analýzy proběhly formou řízeného rozhovoru, při kterém pracovníci OKBK vyplňovali dotazníky na základě sdělení Garantů aktiv a vyhodnocení předloží ke korektuře Garantům aktiv
- Dotazník obsahuje jednotné otázky, na které bylo třeba získat pro všechna identifikovaná aktiva resortu MV, konkrétní odpovědi
- Rozhovory se uskutečnily ve 2 kolech: s Garanty primárních a podpůrných aktiv

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Harmonogram Analýz rizik



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Agenda

1. Pokyn MV - ustanovení Výboru pro řízení kybernetické bezpečnosti
2. Politika ISMS
3. Dokumentace ISMS
4. Analýza rizik VIS – AIS PČR a PVS
5. **Plán bezpečnostního povědomí - vzdělávání**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Plán bezpečnostního povědomí - vzdělávání

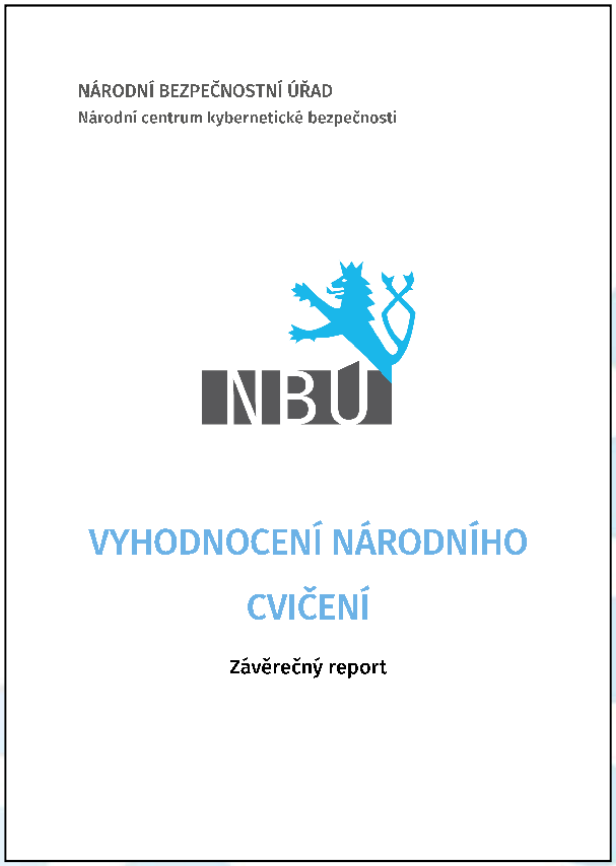
Vyhodnocení národního cvičení NBÚ – 10/2015

Příprava e-learningu – 11/2015

Cvičení na Cyber-polygonu v Brně – 10/2015

Školení a nácvik – T-Soft Praha – 12/2015

Školení DCeGOV – 10-11/2015



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Plán bezpečnostního povědomí – e-learning MV

modul	uživatel					
	každý	s přístupem do sítě MV	operátoři VIS nebo KII	mobilní uživatelé	Garanti primárních aktiv	privilego-vaní uživatelé
Základní modul	X	X	X	X	X	X
Sdílené informační prostředí a ICT služby		X	X	X	X	X
VIS a KII			X		X	
Mobilní zařízení				X	X	X
Správa uživatelů					X	(x)
Bezpečná správa ICT						X

- **Základní modul – od 1.12.2015**
- Sdílené informační prostředí – od 1.5.2016
- VIS a KII – od 1.7.2016
- Mobilní zařízení – od 1.8.2016
- Správa uživatelů – od 1.9.2016
- Bezpečná správa ICT – od 1.9.2016

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dotazy a odpovědi

Děkuji za pozornost a Váš čas

Ing. Miroslav Tůma Ph. D.
odbor kybernetické bezpečnosti a koordinace ICT
miroslav.tuma@mvcr.cz

GSM: +420 734 267 036