eGovernment 2015

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

ISSS LOCAL AND REGIONAL INFORMATION SOCIETY

Realizace zákona o kybernetické bezpečnosti na MV

Ing. Miroslav Tůma, Ph.D.

Ministerstvo vnitra ČR

ředitel odboru kybernetické bezpečnosti a koordinace ICT

14. dubna 2015 (ISSS 2015)

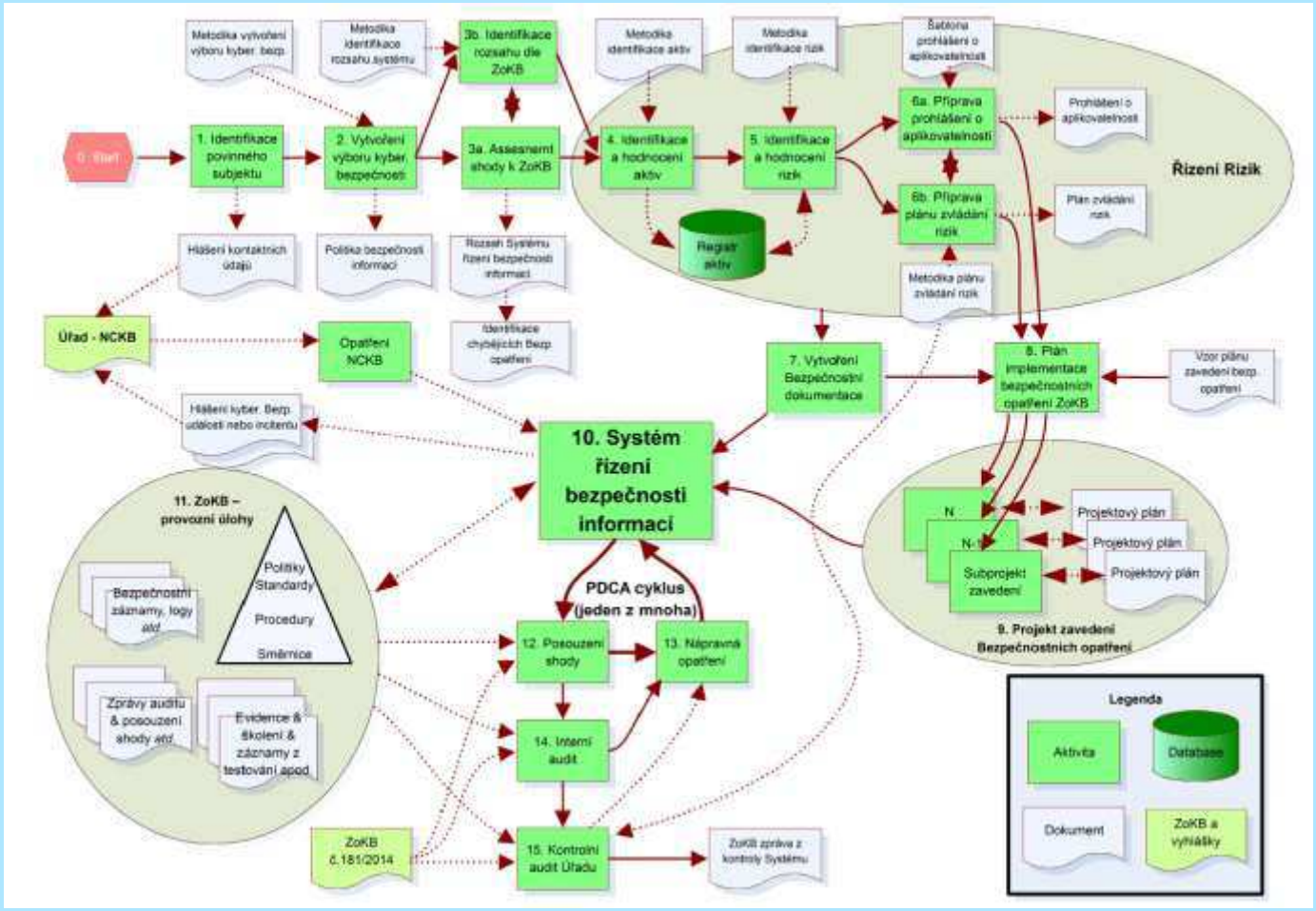
Obsah prezentace

- Implementace požadavků ZoKB – Systém řízení bezpečnosti informací MV
- SOCCR – Security Operation Center for Cyber Reliability
- DCeGOV – Dohledové centrum eGOV

Implementace požadavků ZoKB (Systém řízení bezpečnosti informací MV)

0. **STUDIE DOPADŮ ZoKB NA IS RESORTU MV – JEDNOTNÝ systém řízení bezpeč. informací v rámci resortu MV**
1. **ŘÍZENÍ DOKUMENTACE SYSTÉMU**
2. **IDENTIFIKACE POVINNÉHO SUBJEKTU**
3. **URČENÍ VÝBORU A POVINNÝCH BEZPEČNOSTNÍCH ROLÍ**
4. **POLITIKA BEZPEČNOSTI INFORMACÍ**
5. **IDENTIFIKACE ROZSAHU ŘÍZENÍ SYSTÉMU BEZPEČNOSTI INFORMACÍ**
6. **ASSESMENT – VSTUPNÍ ANALÝZA ZoKB**
7. **REVIZE METODICKÉ ZÁKLADNY**
8. **ŘÍZENÍ RIZIK**
9. **ŘÍZENÍ KONTINUITY ČINNOSTI – DISASTER RECOVERY PLAN**
10. **PRACOVNÍ POSTUPY, ŘÍDICÍ DOKUMENTACE**
    - *10.1. ŘÍZENÍ DOKUMENTACE*
    - *10.2. ŘÍZENÍ KOMUNIKACE*
    - *10.3. ŘÍZENÍ DODAVATELŮ*
    - *10.4. ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ A UDÁLOSTÍ*
    - *10.5. PŘEZKOUMÁNÍ SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ*
    - *10.6. PROVÁDĚNÍ INTERNÍCH AUDITŮ*
11. **PROHLÁŠENÍ O APLIKOVATELNOSTI**

Implementace požadavků ZoKB (Systém řízení bezpečnosti informací MV dle ZoKB)



SOCCR
(Security Operation Center for Cyber Reliability)

DOHLEDUJE BEZPEČNOST ICT SYSTÉMŮ RESORTU MV

PODPORUJE ŘÍZENÍ RIZIK A KONTINUITY

IDENTIFIKUJE, VYHODNOCUJE A HLÁSÍ INCIDENTY DO NCKB (NBÚ)

ŘÍDÍ BEZPEČNOST

24x7

TÝM SOCCR

POSKYTUJE PROVOZNÍ A BEZPEČNOSTNÍ REPORTING

JE V SOULADU
ISO 27001
ISO 22301
ISO 20000

JE MODULÁRNÍ A PŘIPRAVEN NA DALŠÍ ROZVOJ

SKENUJE ZRANITELNOSTI

PROVOZUJE ČPOZ

SOCCR
(Security Operation Center for Cyber Reliability)

- Sbírá a vyhodnocuje provozní a bezpečnostní události v režimu 24x7
- Identifikuje a řeší bezpečnostní incidenty, hlásí incidenty do NCKB
- Naplňuje technické požadavky kybernetického zákona
- Řídí bezpečnost systémů v aktivním a pasivním módu
- Automatizovaně skenuje technické zranitelnosti systémů
- Zajišťuje DDoS ochranu (prostřednictvím CMS)
- Poskytuje bezpečnostní reporting (administrátorský, manažerský…)
- Podporuje procesy řízení rizik a kontinuity
- Tým SOCCR
- Zajišťuje informační fórum pro bezpečnostní správce a manažery

SOCCR
(Security Operation Center for Cyber Reliability)

2015

- ✓ Definovat rozhraní pro připojené systémy
- ✓ Připravit typové projekty pro konektory na SOCCR
- ✓ Implementovat technologie a procesy
- ✓ Zahájit provoz dohledového centra SOCCR

2016

- ✓ Rozšířit pro korelaci interních událostí v systémech MV s podezřelými událostmi v externím prostředí
- ✓ Získávat informace o všech hrozbách z různých zdrojů a koncentrovat úsilí na relevantní nebezpečné případy
- ✓ Vytvořit SOCCR Intelligence Database – shromažďuje a koreluje všechny události v systémech MV
- ✓ Automatizovat procesy řízení rizik a kontinuity systémů MV
- ✓ Rozšířit bezpečnostní reporting o stavu systémů

eGovernment 2015

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

isss LOCAL AND REGIONAL INFORMATION SOCIETY

DCeGOV – Dohledové centrum eGOV

Dohledové centrum eGovernmentu

DCeGOV – NOC (Network Operation Centre)

Technické nástroje projektu NOC zajišťují navýšení stability provozu IS.

Vytváří efektivní procesy pomocí portálu Service Desk.

Provozní dohledy umožňují monitorovat systémy v režimech 24x7 a zajistit poskytování SLA na servisní úkony.

Přehled služeb NOC:

- Vybavení technologického vybavení dohledového centra
- Monitoring prvků – zajišťuje přehled o výpadcích systému
- Service Desk – umožňuje přijímat a dále řídit procesy Incidentů
- Sběr logů – součást rozhraní v rámci resortu MV
- Provisioning, Billing, CMDB, Knowledge base, CA Service Katalog, Process Automation a další

DCeGOV – Dohledové centrum eGOV

Rozšíří monitoring všech přípojných uzlů na krajích a připraví konektor pro napojení dalších prvků perimetrů ostatních systémů

- ✓ Bezpečnostní monitoring
- ✓ Provozní monitoring
- ✓ Potenciál monitorovat prvky celého resortu MV
- ✓ Více než 20 000 prvků v jednotlivých perimetrech
- ✓ Rozšiřuje monitoring do 14 krajů v resortu MV

eGovernment 2015

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

ISSS LOCAL AND REGIONAL INFORMATION SOCIETY

Realizace zákona o kybernetické bezpečnosti na MV

… děkuji za pozornost

a přeji hezký den

Ing. Miroslav Tůma, Ph.D.

Ministerstvo vnitra ČR

ředitel odboru kybernetické bezpečnosti a koordinace ICT

14. dubna 2015 (ISSS 2015)