MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL
INFORMATION SOCIETY

Kybernetická bezpečnost resortu

Ing. Miroslav Tůma, Ph. D.
Odbor kybernetické bezpečnosti a koordinace
informačních a komunikačních technologií MVČR

Agenda

- **Kybernetické nebezpečí a bezpečnostní povědomí**
  - *Čelíme reálné hrozbě nebo pouze dobrému obchodnímu tahu?*
- **Dohledové centrum MV**
  - *centralizovaný dohled systémů*
- **Kybernetické hrozby**
  - *realita a jejich podceňování - katalog hrozeb*

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISSS
LOCAL AND REGIONAL INFORMATION SOCIETY

Co je to kybernetické nebezpečí

- Vše co dokáže narušit

  dostupnost – integritu – důvěrnost

  informací v kyberprostoru

- Pokus o

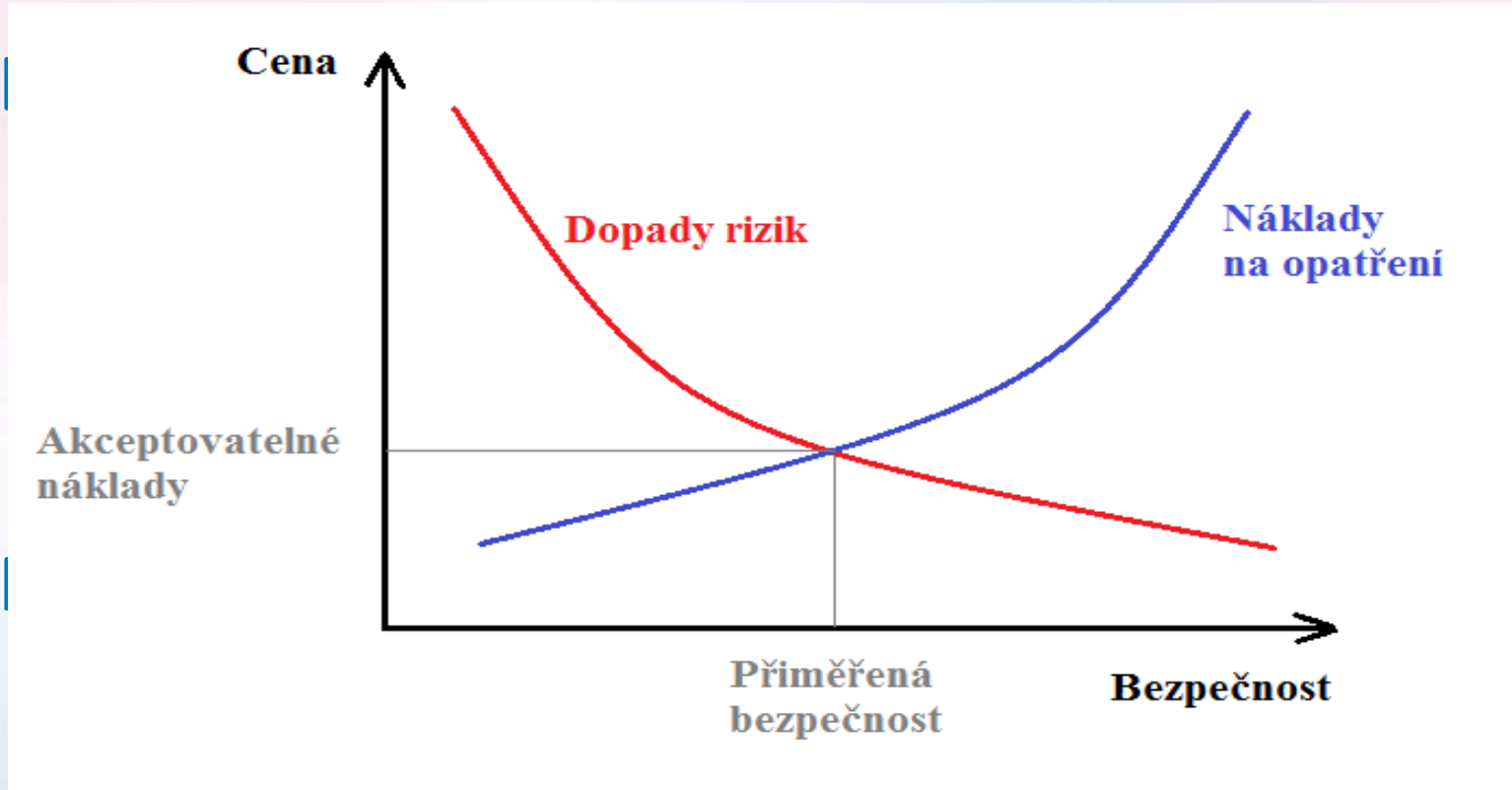
  odcizení – pozmění – ovlivňování

  „uživatele“ v kyberprostoru

  - **Kybernetický útok**
  - **Kybernetická špionáž**
  - **Kybernetická válka**

Dopady kybernetických útoků

-
-



Jak se bránit a chránit před kybernetickým nebezpečím

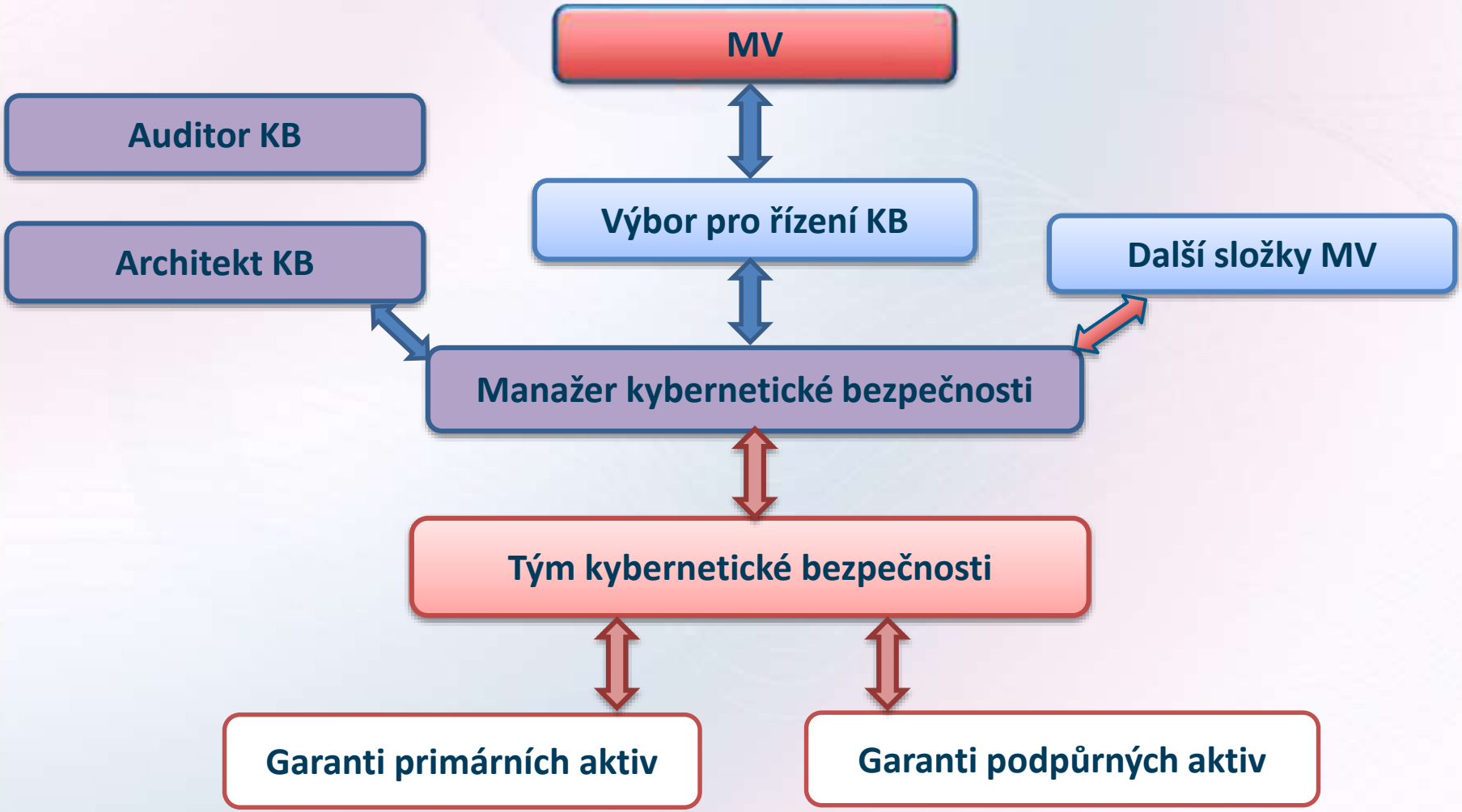
- Tvorba a implementace systému řízení bezpečnosti informací (ISMS)
- Implementace organizačních a technických opatření
  - Metodiky zpracované MV ve spolupráci s ostatními resorty a NBÚ

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISSS
LOCAL AND REGIONAL INFORMATION SOCIETY

Bezpečnostní role a jejich odpovědnosti

- Bezpečnostní role resortu MV:
  - Výbor pro řízení kybernetické bezpečnosti
  - Manažer kybernetické bezpečnosti
  - Auditor kybernetické bezpečnosti
  - Architekt kybernetické bezpečnosti
  - Tým kybernetické bezpečnosti
  - Garanti aktiv
- Vzájemná spolupráce při implementaci ISMS, dohled nad jejím dodržováním a návrhy implementace bezpečnostních opatření v čase


MV
Auditor KB
Výbor pro řízení KB
Architekt KB
Další složky MV
Manažer kybernetické bezpečnosti
Tým kybernetické bezpečnosti
Garanti primárních aktiv
Garanti podpůrných aktiv

MINISTERSTV
ČESKÉ REPUB

Systé

rmací

CERTIFIKÁT

č. 42009742

LL-C Certification

Osvědčujeme a prohlašujeme, že systém managementu bezpečnosti informací ve společnosti

Ministerstvo vnitra
Nad Štolou 936/3
170 34 Praha 7, Holešovice

Odbor kybernetické bezpečnosti a koordinace ICT
Nám. Hrdinů 1634/3
140 21 Praha 4

byl prověřen a shledán splňující požadavky normy

ISO/IEC 27001:2013

pro předmět činnosti

Systém řízení bezpečnosti informací podle zákona 181/2014 Sb., a jeho prováděcích předpisů s rozsahem na informační a komunikační systémy kritické informační infrastruktury a významné informační systémy resortu Ministerstva vnitra České republiky.

Prohlášení o aplikovatelnosti ISMS poslední verze ze dne 10. 12. 2015

Tento certifikát byl vydán pod číslem **42009742** a je platný od 11. ledna 2016 do 10. ledna 2019.

Schválil

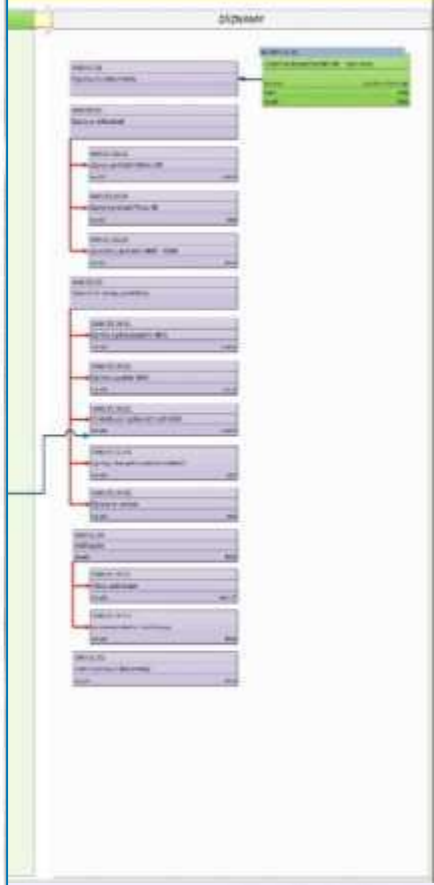
Vytiskl

S 3137

ověřovací kód: **87AC30B3-685**
Platnost certifikátu ověřte tímto kódem na www.ll-c.info

www.ll-c.net

LL-C (Certification) Czech Republic s.r.o. | Pobřežní 620/3, 186 00 Praha 8



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISSS
LOCAL AND REGIONAL INFORMATION SOCIETY

Jak se bránit a chránit před kybernetickým nebezpečím

- Zajištění celého kybernetického prostoru resortu MV
- Zabezpečení KII a VIS resortu MV
- Resort MV – aktuálně 27 KII (18) a VIS (9) a dalších cca 120 IS
- Bezpečnostní dokumentace KII a VIS
- Napojení na Dohledové centrum MV - DCeGOV
- Hlášení kybernetických bezpečnostních incidentů na NCKB a komunikace s NBÚ (NCKB)

POVINNÁ BEZPEČNOSTNÍ DOKUMENTACE (vyhláška č. 316/2014 Sb.)	KII	VIS
RESORTNĚ PLATNÁ BEZPEČNOSTNÍ DOKUMENTACE		
Plán rozvoje bezpečnostního povědomí (OBECNÉ BEZPEČNOSTNÍ POVĚDOMÍ)	X	X
Bezpečnostní politika (RESORTU)	X	X
Přehled právních, vnitřních a jiných předpisů a smluvních závazků (RESORT)	X	X
Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hod. rizik	X	X
Zvládání kybernetických bezpečnostních incidentů	X	X
Zpráva z přezkoumání systému řízení bezpečnosti informací	X	
BEZPEČNOSTNÍ DOKUMENTACE PRO KONKRÉTNÍ SYSTÉM		
Přehled právních, vnitřních a jiných předpisů a smluvních závazků	X	X
Bezpečnostní politika (VIS/KII)	X	X
Zpráva o hodnocení aktiv a rizik	X	X
Prohlášení o aplikovatelnosti	X	X
Plán zvládání rizik	X	X
Strategie řízení kontinuity činností	X	X
Plán rozvoje bezpečnostního povědomí (povědomí k danému VIS / KII)	X	X
Zpráva z auditu kybernetické bezpečnosti (porovnání souladu se ZoKB)	X	
PROVOZNÍ DOKUMENTACE PRO KONKRÉTNÍ SYSTÉM		
Uživatelská příručka	X	X
Příručka systému	X	X
Bezpečnostní směrnice pro činnost bezpečnostního správce systému	X	X

Bezpečnostní povědomí

- Nastavení zásadních pravidel kybernetické bezpečnosti:
  - Nejdůležitějším, ale také nejslabším článkem v organizaci bezpečnosti jsou **LIDÉ**

» Základem je **zvyšování bezpečnostního povědomí**.

» Za **dodržování pravidel jsou zodpovědní všichni jednotliví pracovníci**, **vedoucí pracovníci** jsou zodpovědní **za kontrolu** dodržování.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISSS
LOCAL AND REGIONAL INFORMATION SOCIETY

Dohledové centrum MV - DCeGOV

- Jeden z úkolů Akčního plánu k Národní strategii KB 2015-2020
  - C.2.03 Vybudovat resortní CERT/CSIRT pracoviště MV k ochraně základních registrů a nejdůležitějších systémů pro fungování eGovernmentu
- Centrální dohledový systém pro zajištění bezpeč. dohledů nejen pro KII a VIS resortu MV
- Funkční rozhraní pro hlášení KBI na NCKB
- Sbírá a vyhodnocuje provozní a bezpečnostní události v režimu 24x7

Dohledové centrum MV - DCeGOV

- Geograficky redundantní řešení
- Řídí bezpečnost systémů v aktivním a pasivním módu
- 14 konektorů na úrovni krajů pro napojení krajských prvků a rozšíří monitoring do všech přípojných uzlů síti MV
- Vytváří efektivní procesy pomocí portálu Service Desk

Dohledové centrum MV - DCeGOV

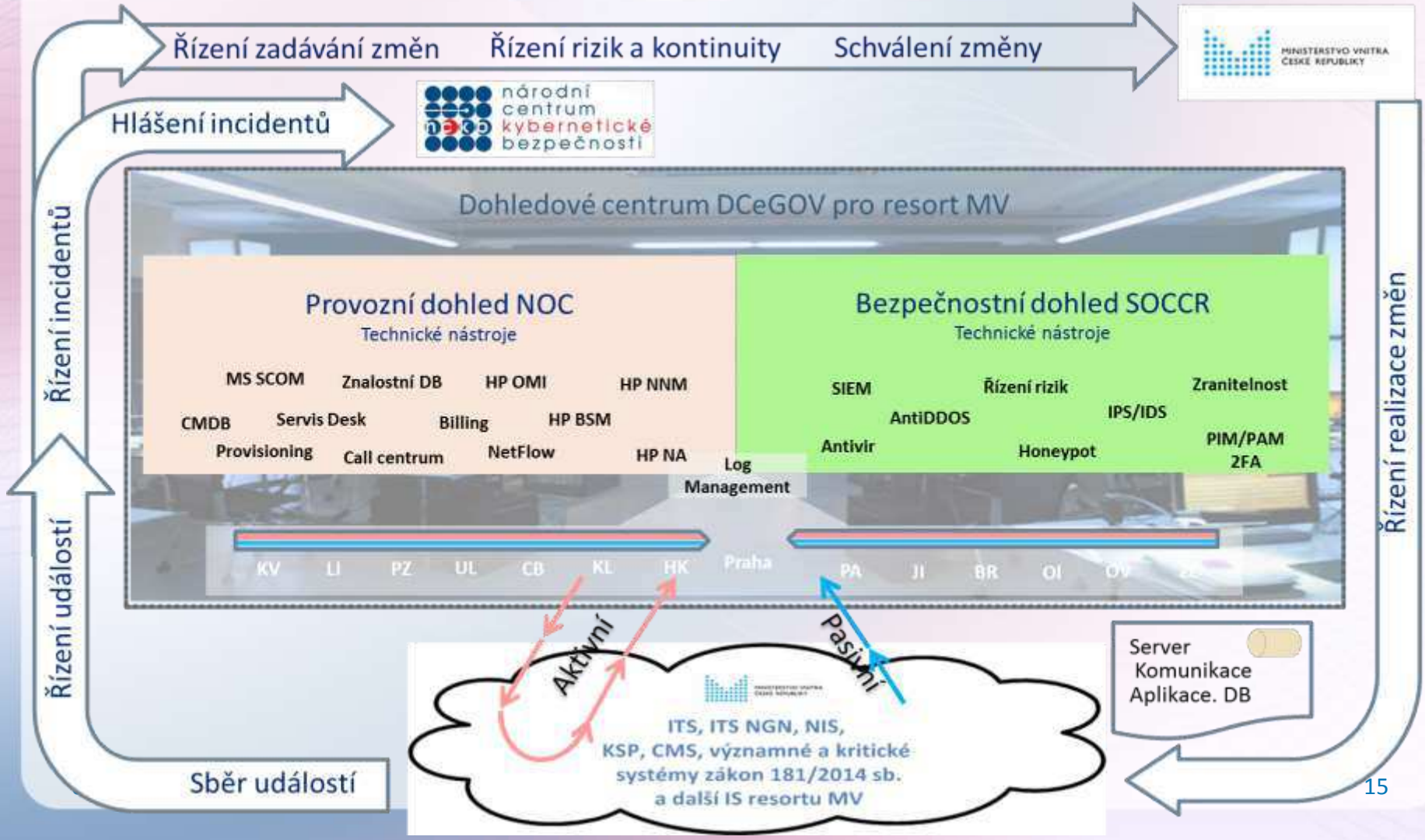
- Přehled služeb:

  Vybavení dohledového centra
  - **HoneyPot** - doplňkový systém pro identifikaci kybernetických útoků
  - **Antivirus** – detekce virových nákaz
  - **2 FA** – dvoufaktorová autentizace – klíčenka, která umožní autentizovat administrátora
  - Systémy pro **řízení rizik a BCP** (analýza zranitelnosti a řízení kontinuity)

  Technologie, které DCeGOV rozšiřuje do krajů:
  - **SIEM** – vyhodnocování, alertování a řešení bezpečnostních událostí + reporting
  - **Vulnerability scanner** – kontrola aktualizací a bezpečnostní konfigurace systému
  - **Netflow analyzer, IPS/IDS, AntiDDoS** a další …

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Dohledové centrum MV - DCeGOV



Kybernetické hrozby realita a jejich podceňování

Zdroje:

- Internet – otevřené zdroje
- Interní a zpravodajské zdroje
- Sdílené informace NBÚ
- Znalostní databáze DCeGOV

Analýza:

- Tým kybernetické bezpečnosti
- Analytická skupina

Sdílení:

- *kyberinfo@mvcr.cz*

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISSS
LOCAL AND REGIONAL
INFORMATION SOCIETY

Děkuji Vám za pozornost,

Miroslav Tůma

ředitel
Odbor kybernetické bezpečnosti a koordinace ICT
MV ČR