Zkušenosti s implementací ZoKB a problémy, které nás pálí

Ing. Miroslav Tůma, Ph.D.

Ředitel odboru kybernetické bezpečnosti a koordinace ICT

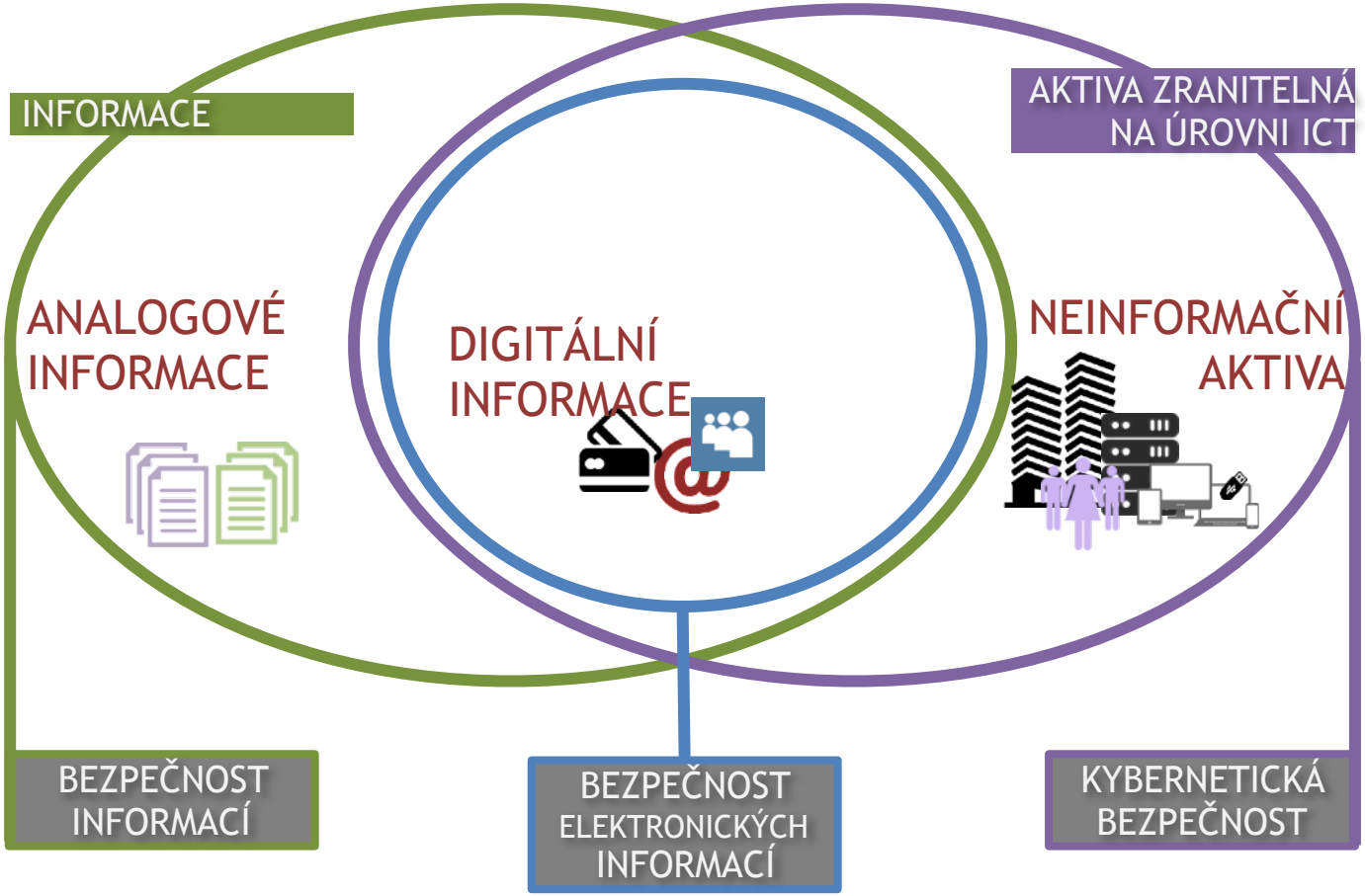
Program

- Působnost Ministerstva vnitra.
- Definiční rámec kybernetické bezpečnosti.
- Kybernetická bezpečnost resortu MV.
  - Systém řízení bezpečnosti informací resortu MV.
  - Kontinuální rozvoj ISMS – projekty v oblasti KB na rok 2018.
  - Úskalí zajišťování kybernetické bezpečnosti v resortu MV.
- Řízení kybernetických bezpečnostních událostí a incidentů – Dohledové centrum eGovernmentu.

Strategická role MV v oblasti ICT

- Ministerstvo vnitra si je vědomo své klíčové řídící a strategické role v oblasti ICT státu, a proto usiluje o jednotnost, centralizaci a bezpečnost základních služeb eGovernmentu, zejména prostřednictvím budování komplexních a vzájemně propojených infomačních a komunikačních systémů včetně dohledových systémů pro zajištění jejich plynulého provozu a bezpečnosti.
- Celkem **58** organizací včetně krajských ředitelství PČR a HZS.

Definiční rámec KB

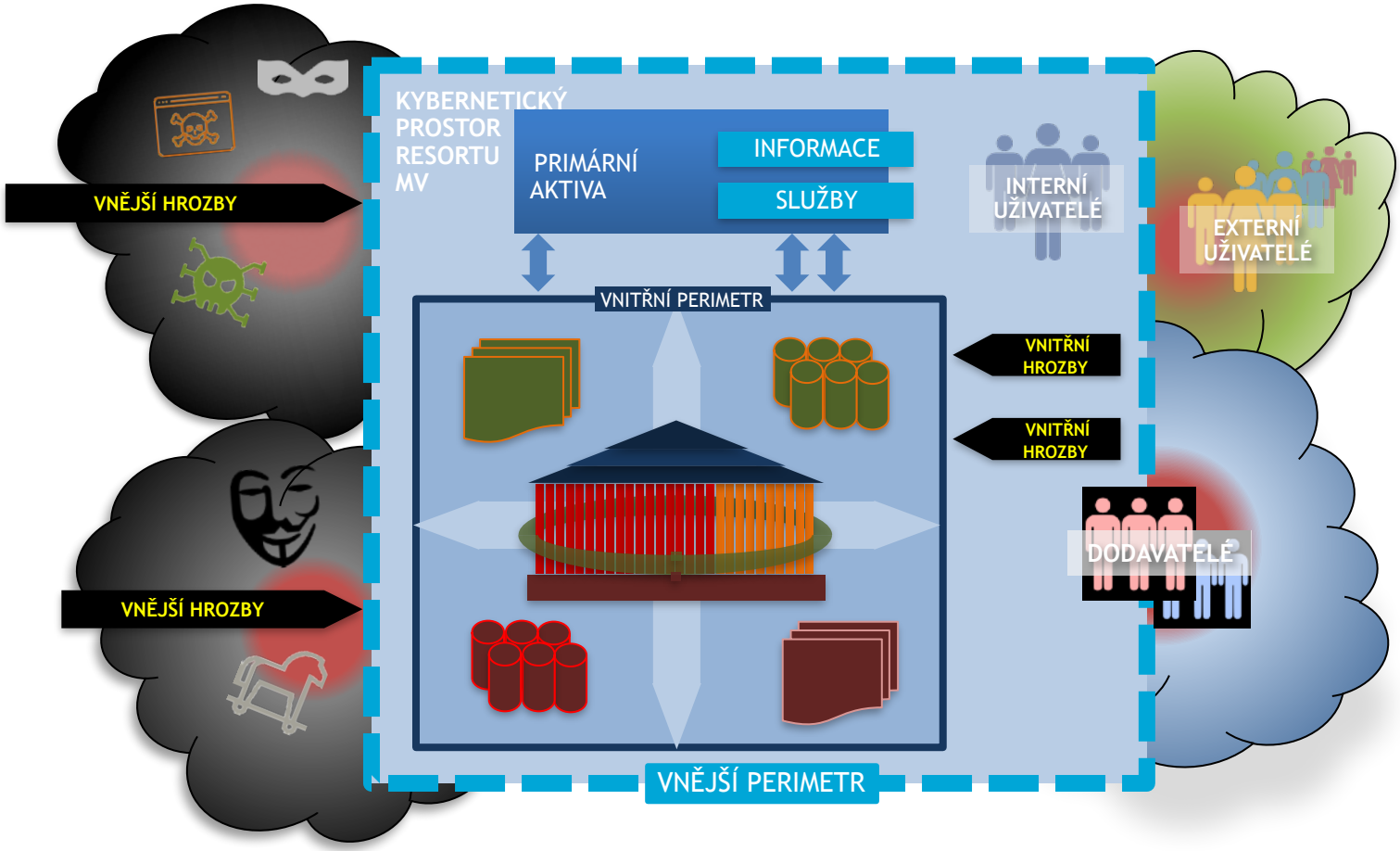


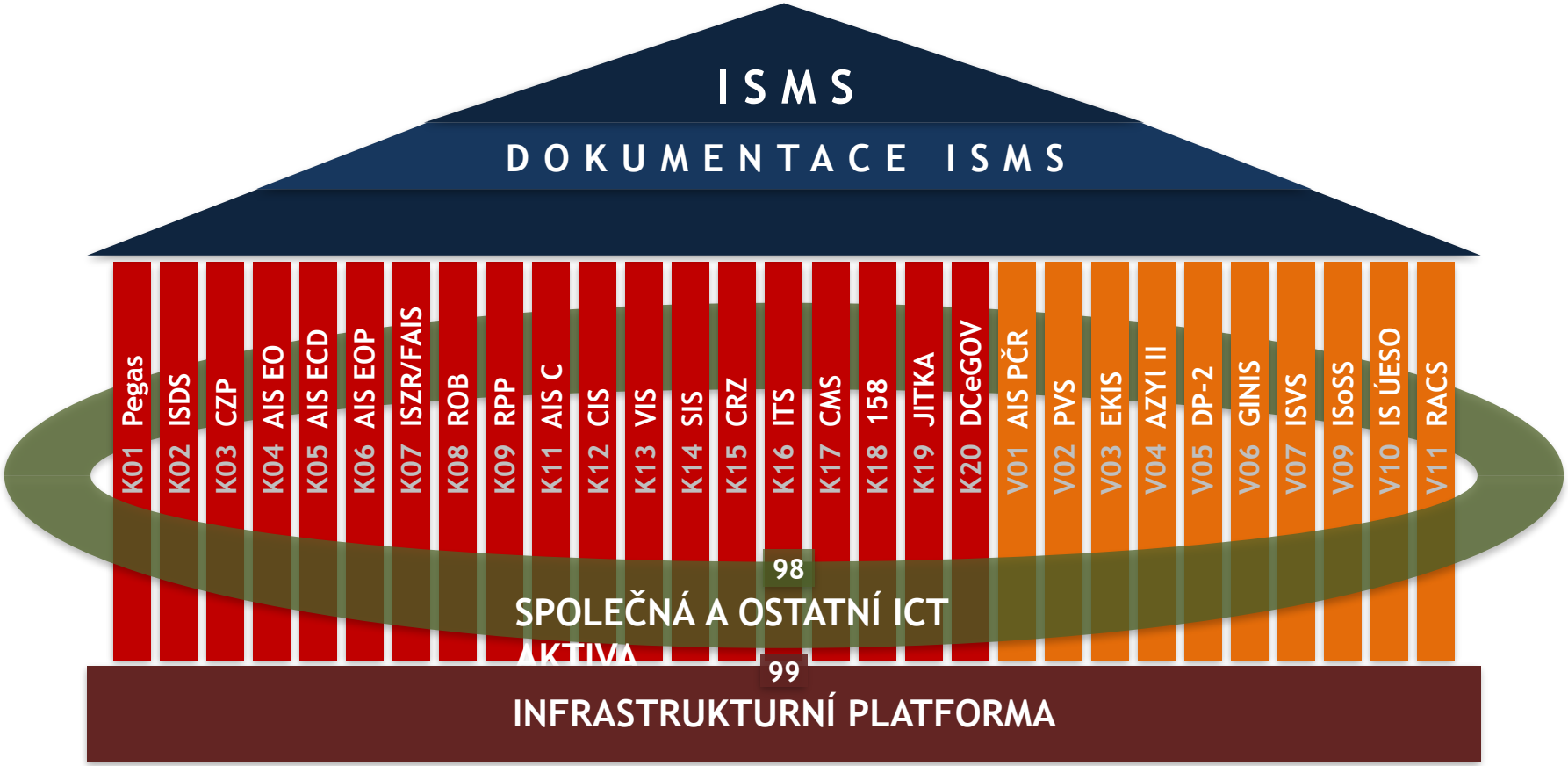
Kybernetická bezpečnosti resortu MV

Kybernetická bezpečnost resortu MV

- Cílem a úlohou kybernetické bezpečnosti resortu MV je zabezpečení kybernetického prostoru proti vnějším a vnitřním kybernetickým hrozbám prostřednictvím organizačních a technických opatření a minimalizace možných důsledků případných kybernetických událostí nebo incidentů.
- Bezpečnost kybernetického prostoru resortu MV je řízena průběžně zdokonalovaným Systémem řízení bezpečnosti informací (ISMS) a primárně zaměřena dle zákona o kybernetické bezpečnosti na kritickou informační infrastrukturu a významné informační systémy.

Kybernetická bezpečnost resortu MV





Rozsah ISMS resortu MV

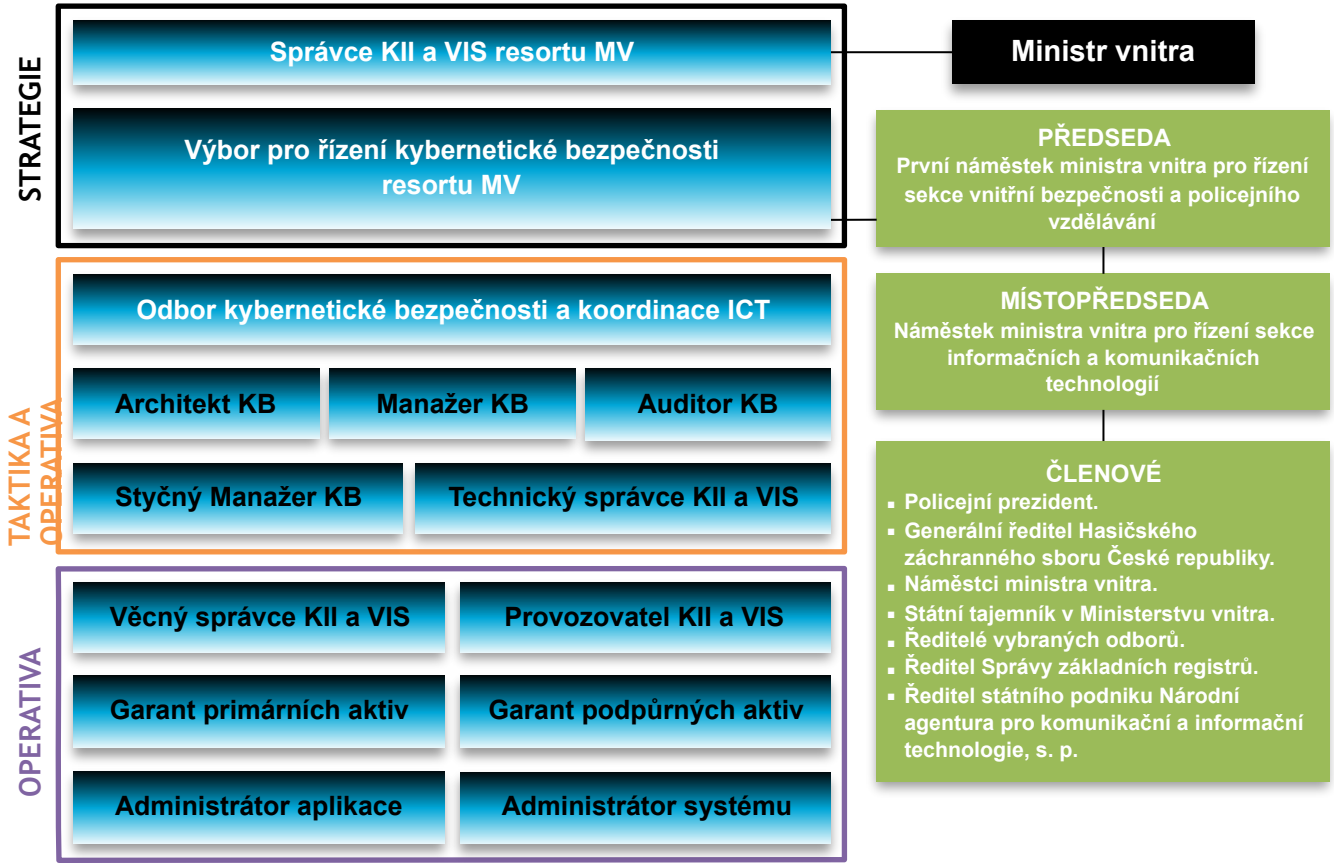
Vývoj počtu KII a VIS ve VS

Kritická informační infrastruktura	Roky			
	2015	2016	2017	2018
Veřejný sektor*	48	48	50	x
• Resort MV	18	17	18	19

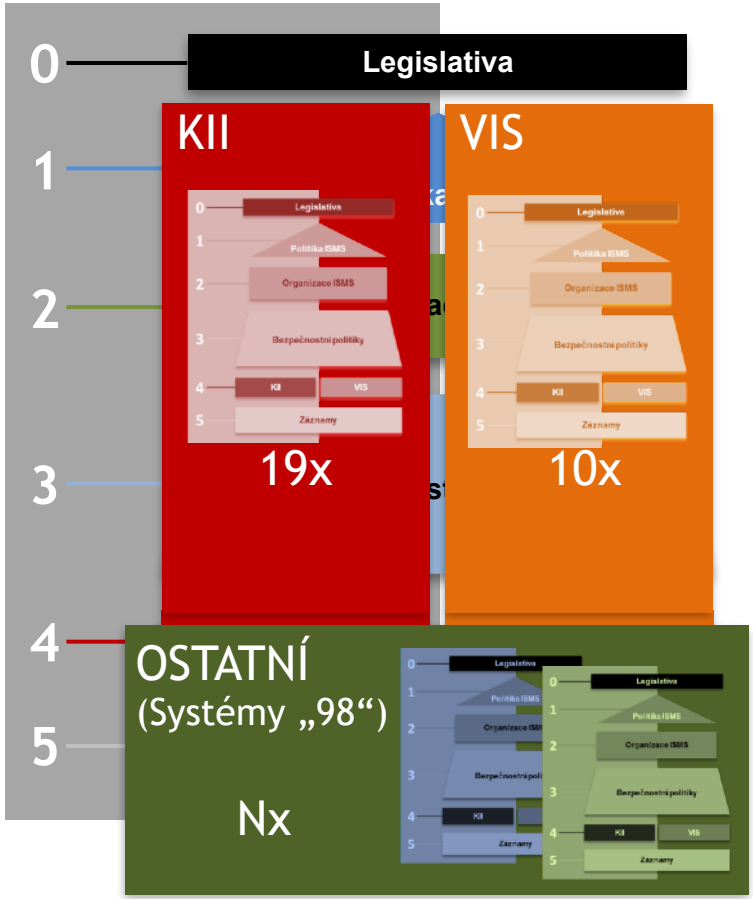
Významné informační systémy	Roky			
	2015	2016	2017	2018
Veřejný sektor*	105	158	169	x
• Resort MV	9	10	10	10

*Statistiky převzaty ze zpráv o stavu kybernetické bezpečnosti České republiky 2015-2016 a dalších podkladů Národního úřadu pro kybernetickou a informační bezpečnost

Organizace KB v resortu MV



ISMS certifikace I


0
1
2
3
4
5
Legislativa
KII
19x
VIS
10x
OSTATNÍ
(Systémy „98“)
Nx

Zásady kybernetické bezpečnosti pro uživatele ICT resortu MV

4. vydání

Zásada I. Podmínkou přístupu do kybernetického prostoru MV, tj. k prostředkům ICT resortu MV je seznámení se *„Základními materiály o dopadech zákona č. 181/2014 Sb. o kybernetické bezpečnosti na resort MV – implementace systému řízení bezpečnosti informací v kybernetickém prostoru resortu MV"* stanovené uvedeným zákonem a následně upravené ISMS 01.01 Politikou ISMS a schválenou Ministrem vnitra dne 07. 06. 2017.

Zásada II. Každý pracovník resortu MV má nárok na přidělení pouze takových prostředků ICT resortu MV (HW, SW, komunikační služby a přístupová oprávnění k datům a službám), které potřebuje pro zajištění výkonu činnosti zastávaného systemizovaného pracovního místa a funkce.

Zásada III. Jedinou osobou oprávněnou instalovat na stolní PC, notebook, tablet, chytrý telefon (dále jen „pracovní stanici") jakýkoliv SW (včetně antivirového), nastavovat uživatelské účty a připojovat tyto pracovní stanice do vnitřní sítě resortu MV, tj. intranetu MV je správce počítačových programů.

Zásada IV. Pro pracovní účely využívat primárně prostředky ICT resortu MV přidělené / určené zaměstnavatelem. Vlastní (soukromé) pracovní stanice využívat pouze s písemným souhlasem zaměstnavatele a v souladu s licenčními podmínkami SW.

Zásada V. Přidělené ICT prostředky resortu MV využívat pouze pro pracovní účely a mobilní pracovní stanice (notebook, tablet, chytrý telefon) chránit proti zcizení, neoprávněnému použití a poškození.

Zásada VI. Problémy s prostředky ICT resortu MV, podezření na kybernetickou bezpečnostní událost, neoprávněný přístup k pracovním datům, nebo dokumentům resortu, nedodržení bezpečnostních pravidel, selhání a poruchy, které by mohly způsobit ohrožení a dostupnost pracovních dat a informačních nebo komunikačních služeb, obdržení spamu na pracovní e-adresu elektronické pošty, apod. bezodkladně nahlásit na organizačně příslušný odborný útvar ICT nebo na pracoviště dohledového centra DCeGOV:

- ✓ telefonicky na linku číslo: 974 801 131,
- ✓ e-mailem na adresu: dohled@mvcr.cz.

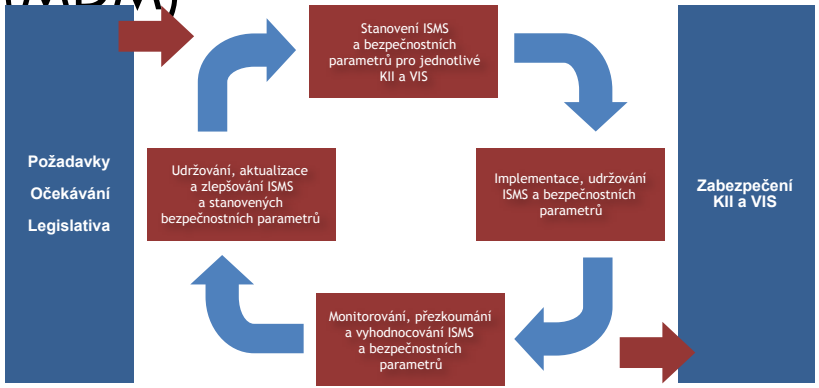
Zásada VII. Ztrátu nebo odcizení mobilní pracovní stanice nebo přiděleného paměťového nosiče bez zbytečného prodlení ohlásit odbornému útvaru ICT.

Zásada VIII. Přístup k přiděleným prostředkům ICT resortu MV vždy zabezpečovat osobním heslem. Základní doporučená pravidla pro osobní hesla:

- ✓ udržovat unikátní hesla, tj. různé (pro každého uživatele) pro jednotlivá zařízení i jednotlivé SW aplikace a systémy.

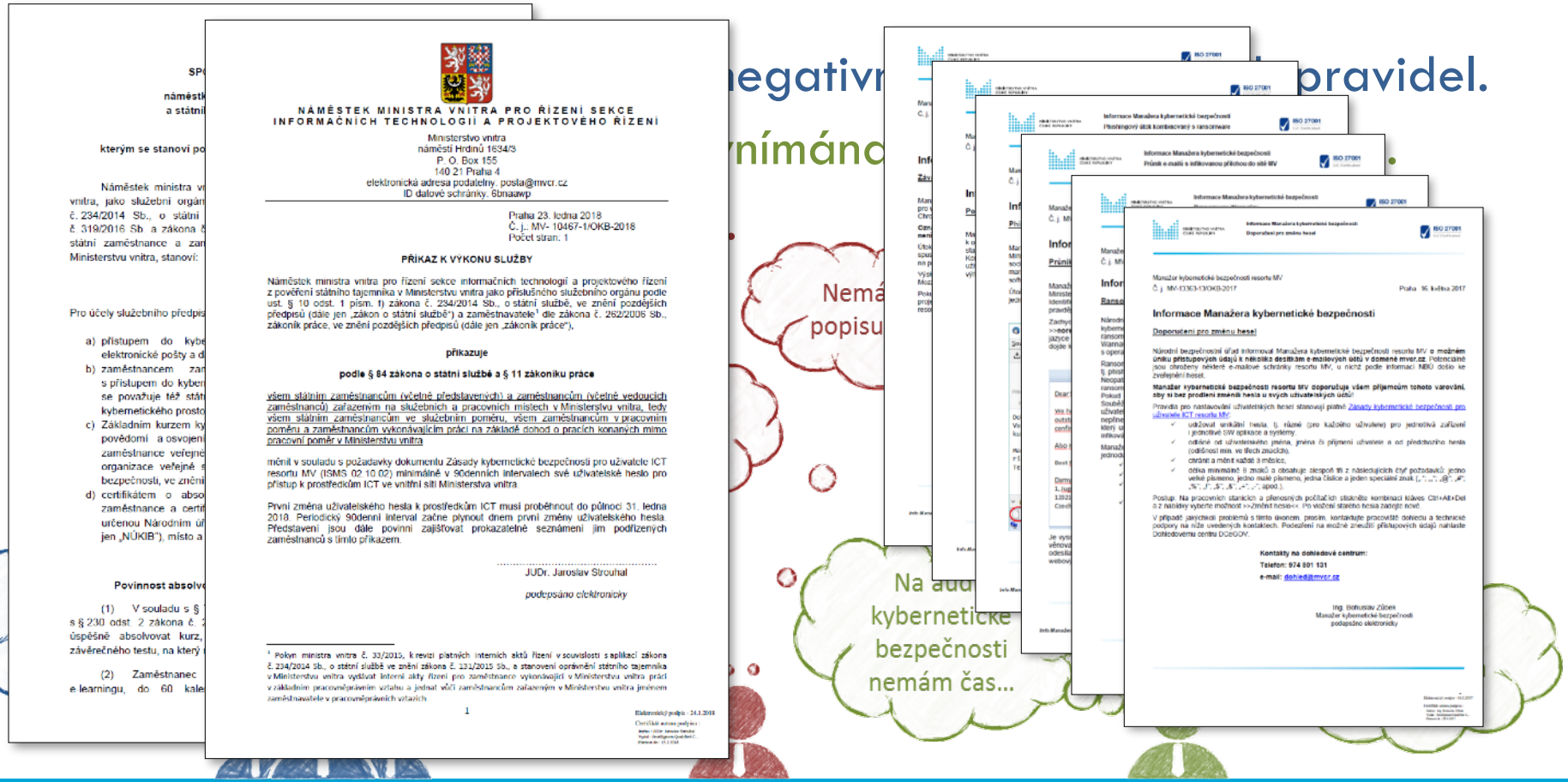
Stránky KB na portálu SIP

- Kontinuální rozvoj Dohledového centra eGovernmentu (DCeGOV)
- Mobile Device Management (MDM)
- Data Loss Prevention (DLP)
- OSC RED Team
- Identity Management (IdM)



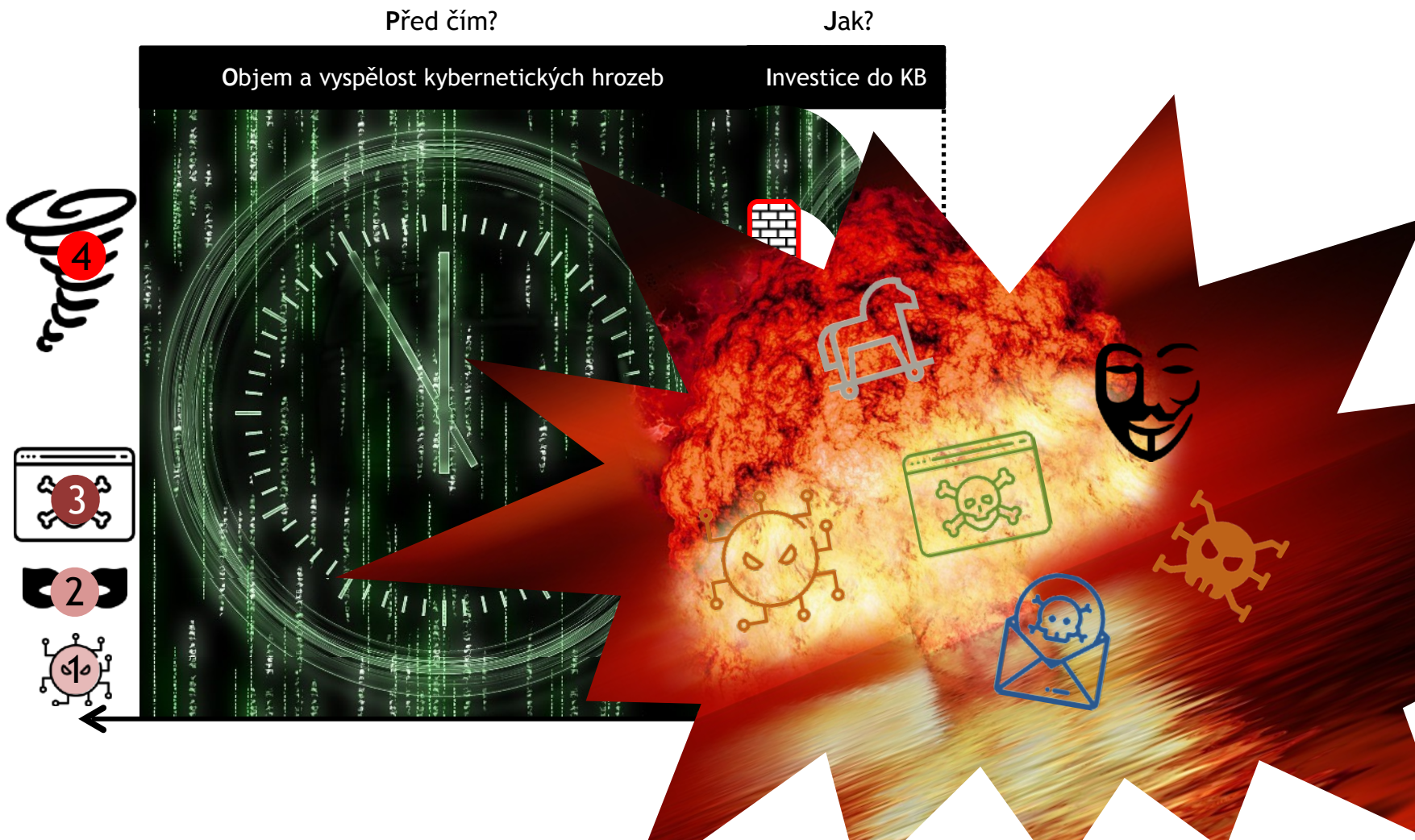
- E-learningové kurzy pro organizace veřejné správy vychází z:

  - **Modul A: Základní kurz kybernetické bezpečnosti**
  - **Modul B: Kurz kybernetické bezpečnosti dle ZKB**



Úskalí zajišťování KB v resortu MV

Hrozby a investice do zabezpečení



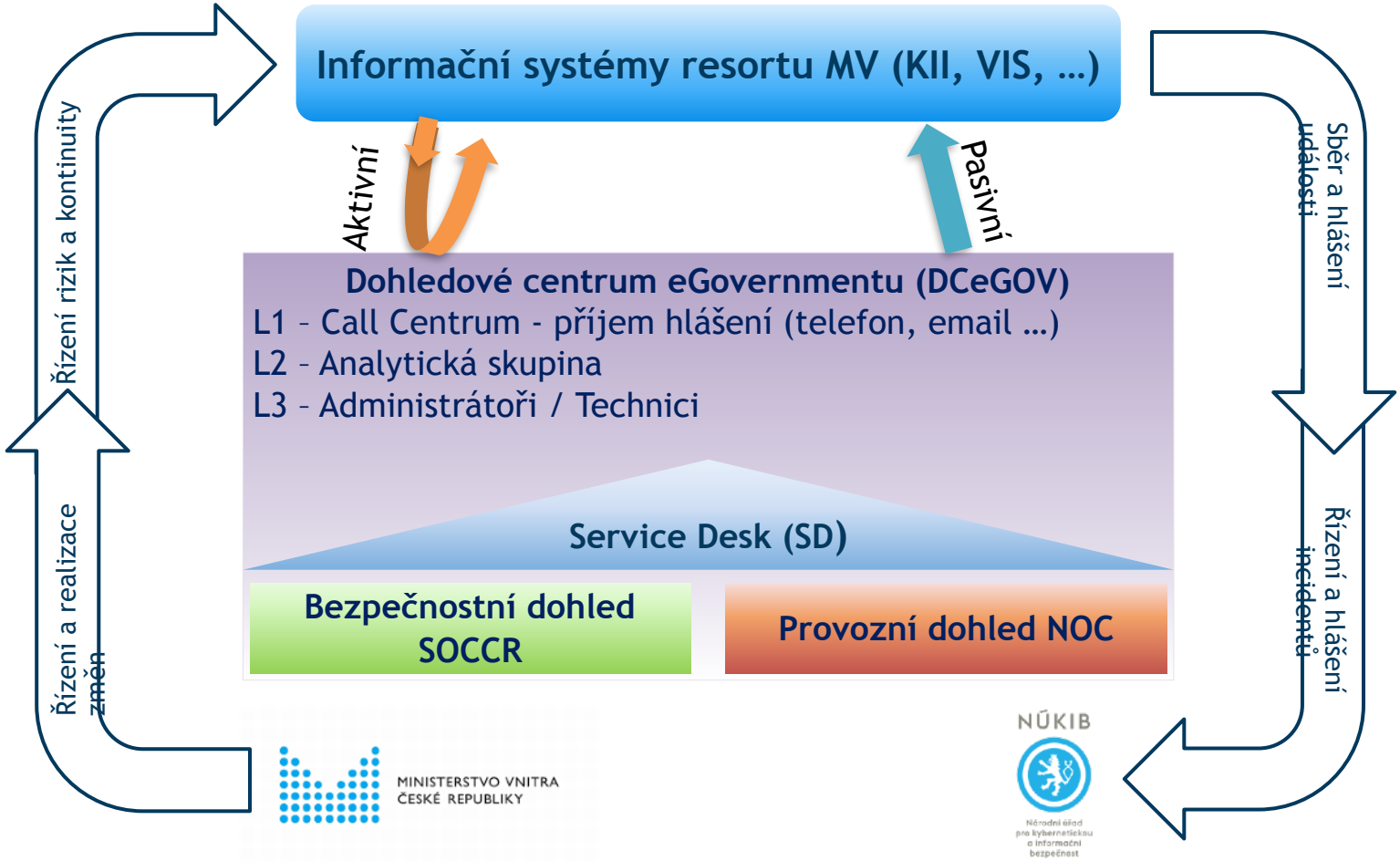
Úskalí zajišťování KB v resortu MV

Co s tím?

- 10 kroků ke „zlomení odporu“
  1. Nechci
  2. Nemohu
  3. Nevím
  4. Kdybych mohl
  5. Myslím, že bych mohl
  6. Mohl bych to zkusit
  7. Myslím, že mohu
  8. Mohu
  9. Udělám to
  10. Udělal jsem to!

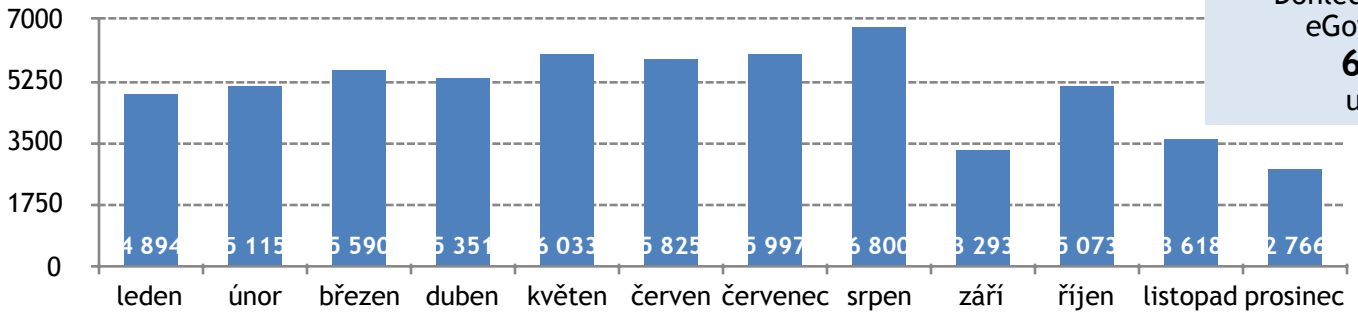
Dohledové centrum eGovernmentu

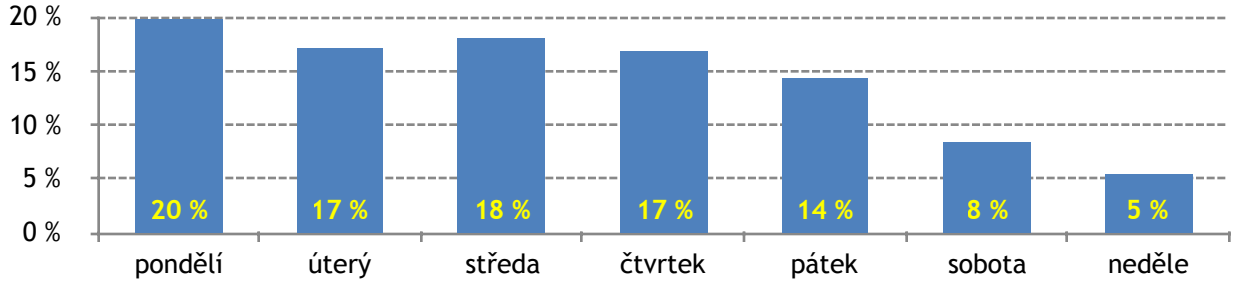
Funkční schéma DCeGOV



Dohledové centrum eGovernmentu

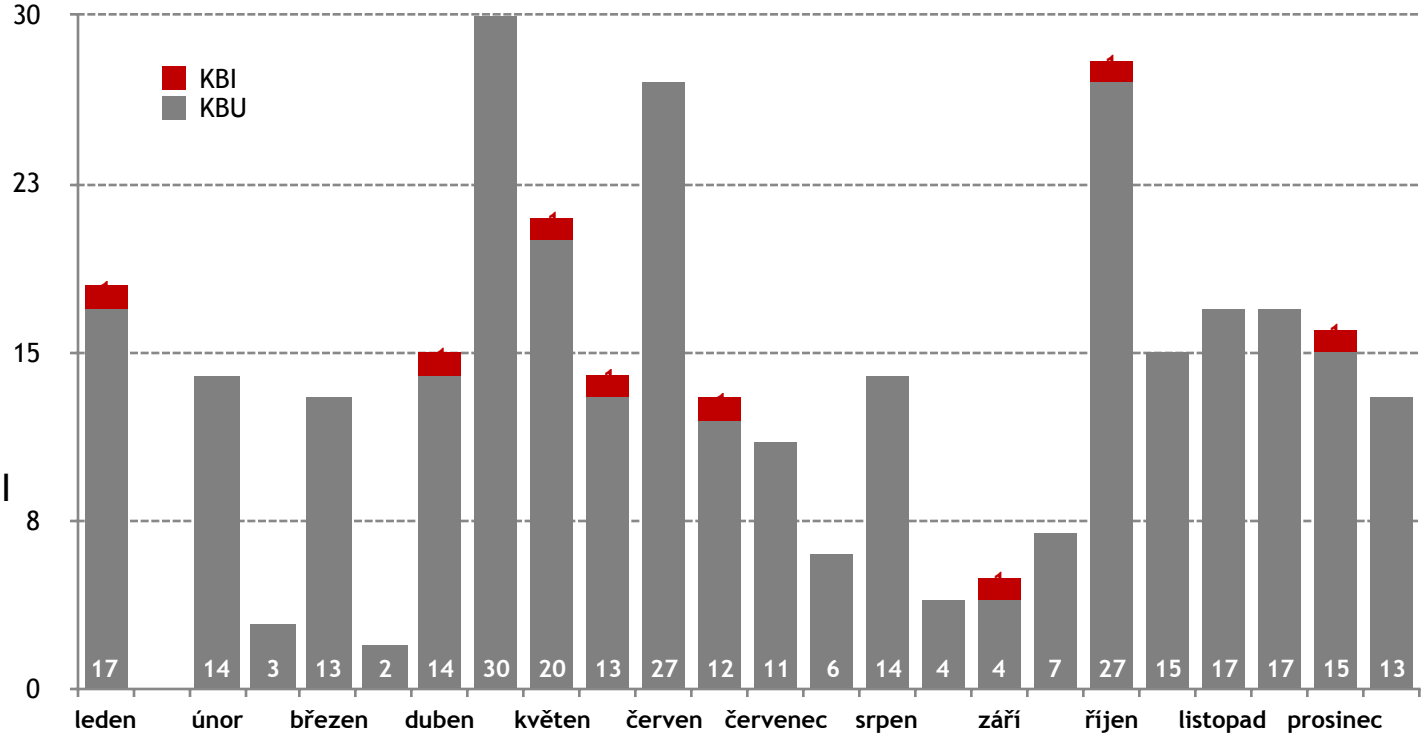
V roce 2017 řešilo Dohledové centrum eGovernmentu **60 355** událostí.

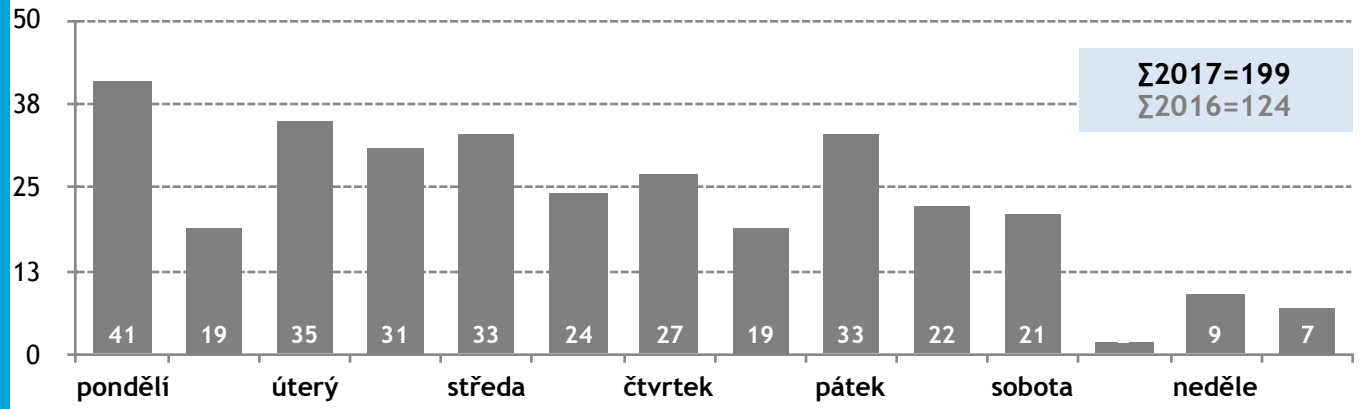


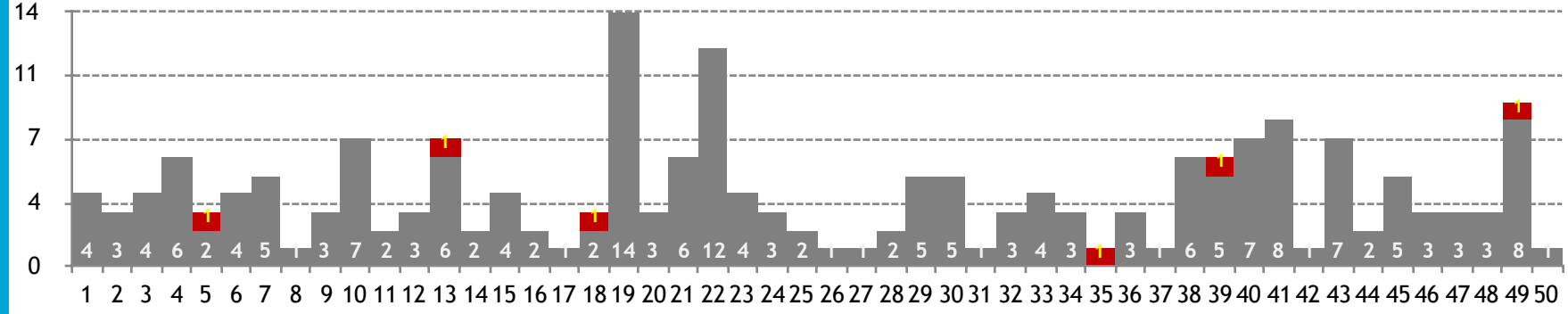


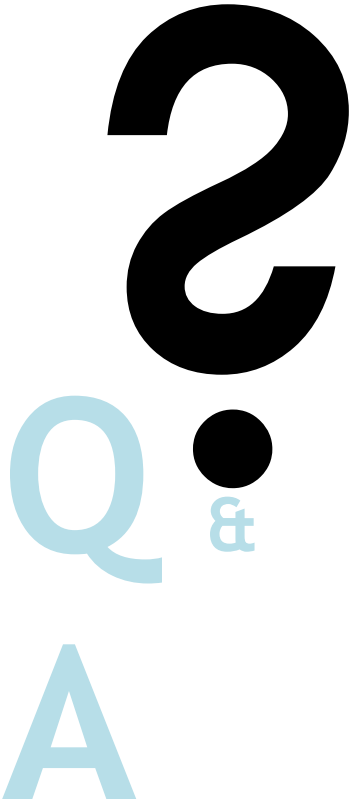
KBU a KBI v resortu MV

- Počet **kybernetických bezpečnostních událostí** vzrostl v roce 2017 o 58 % na **193.**
- Počet **kybernetických bezpečnostních incidentů** se vloni zvýšil na trojnásobek, konkrétně na **6.**




50
38
25
13
0
41
19
35
31
33
24
27
19
33
22
21
9
7
pondělí
úterý
středa
čtvrtek
pátek
sobota
neděle
Σ2017=199
Σ2016=124


14
11
7
4
0
4 3 4 6 2 4 5 1 3 7 2 3 6 2 4 2 1 2 14 3 6 12 4 3 2 1 1 2 5 5 1 3 4 3 1 3 1 6 5 7 8 1 7 2 5 3 3 3 8 1
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50


Q
&
A

Děkuji za pozornost a Váš čas.

Ing. Miroslav Tůma, Ph.D.

Ředitel odboru kybernetické bezpečnosti a koordinace ICT