Kybernetická bezpečnost resortu MV ČR 2019

Varování NÚKIB 17.12.2019 - **JAK POSTUPOVALO MV ČR**

Ing. Miroslav Tůma, Ph.D.

Ředitel odboru kybernetické bezpečnosti a koordinace ICT

Ministerstvo vnitra

Program

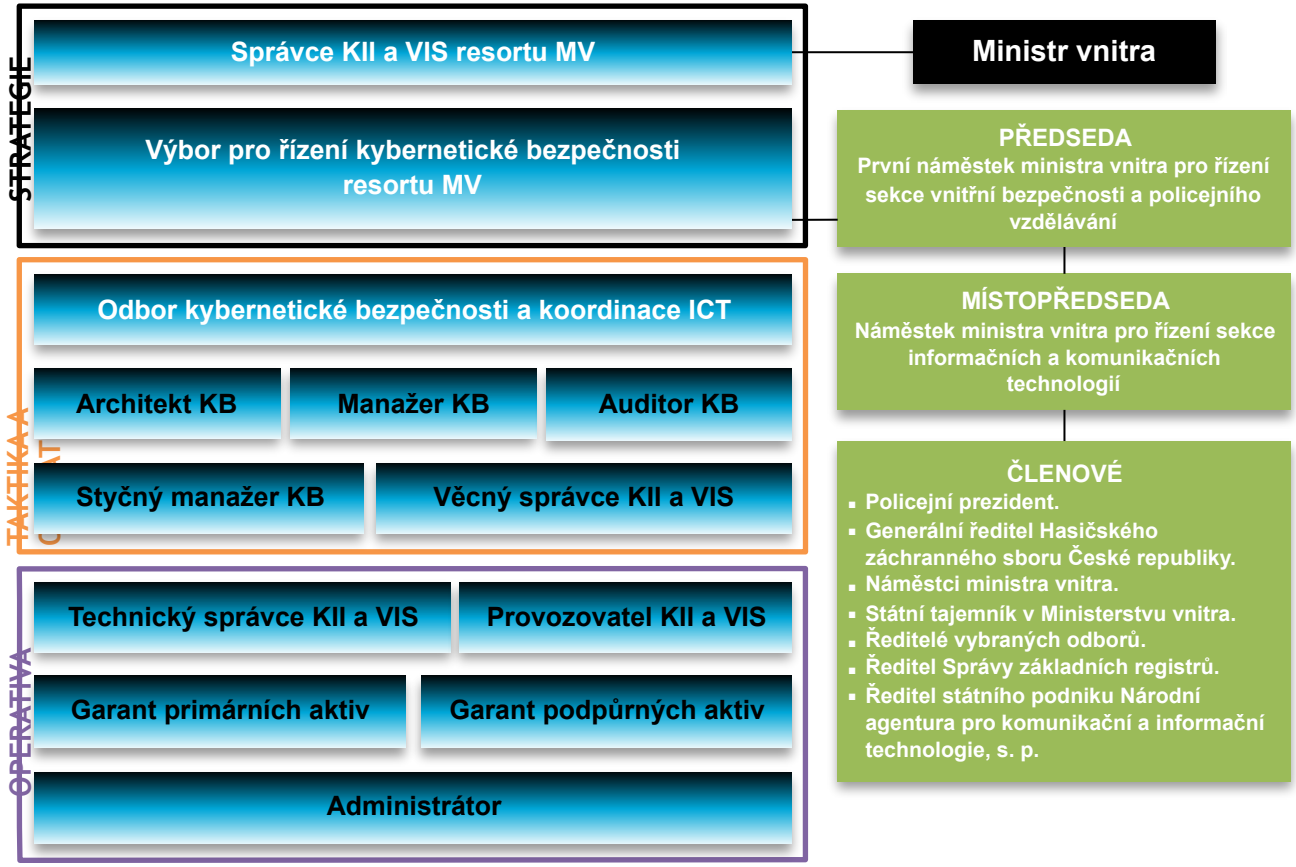
- Působnost Ministerstva vnitra.
  - Legislativní ukotvení.
  - Strategická role MV v oblasti ICT.
- Kybernetická bezpečnost resortu MV.
  - Odbor kybernetické bezpečnosti a koordinace ICT.
  - Organizace KB v resortu MV.
- Systém řízení bezpečnosti informací resortu MV.
  - Rozsah ISMS resortu MV.
  - Dokumentace ISMS resortu MV.
  - Sjednocené informační prostředí resortu MV.
- Aktualizace dokumentace ISMS resortu MV.
  - Metodika identifikace a hodnocení aktiv a rizik.
  - Poznatky při aktualizaci.
- Úskalí zajišťování kybernetické bezpečnosti.
- Vývoj kybernetických bezpečnostní událostí a incidentů v letech 2016-2018.

Kybernetická bezpečnost resortu MV

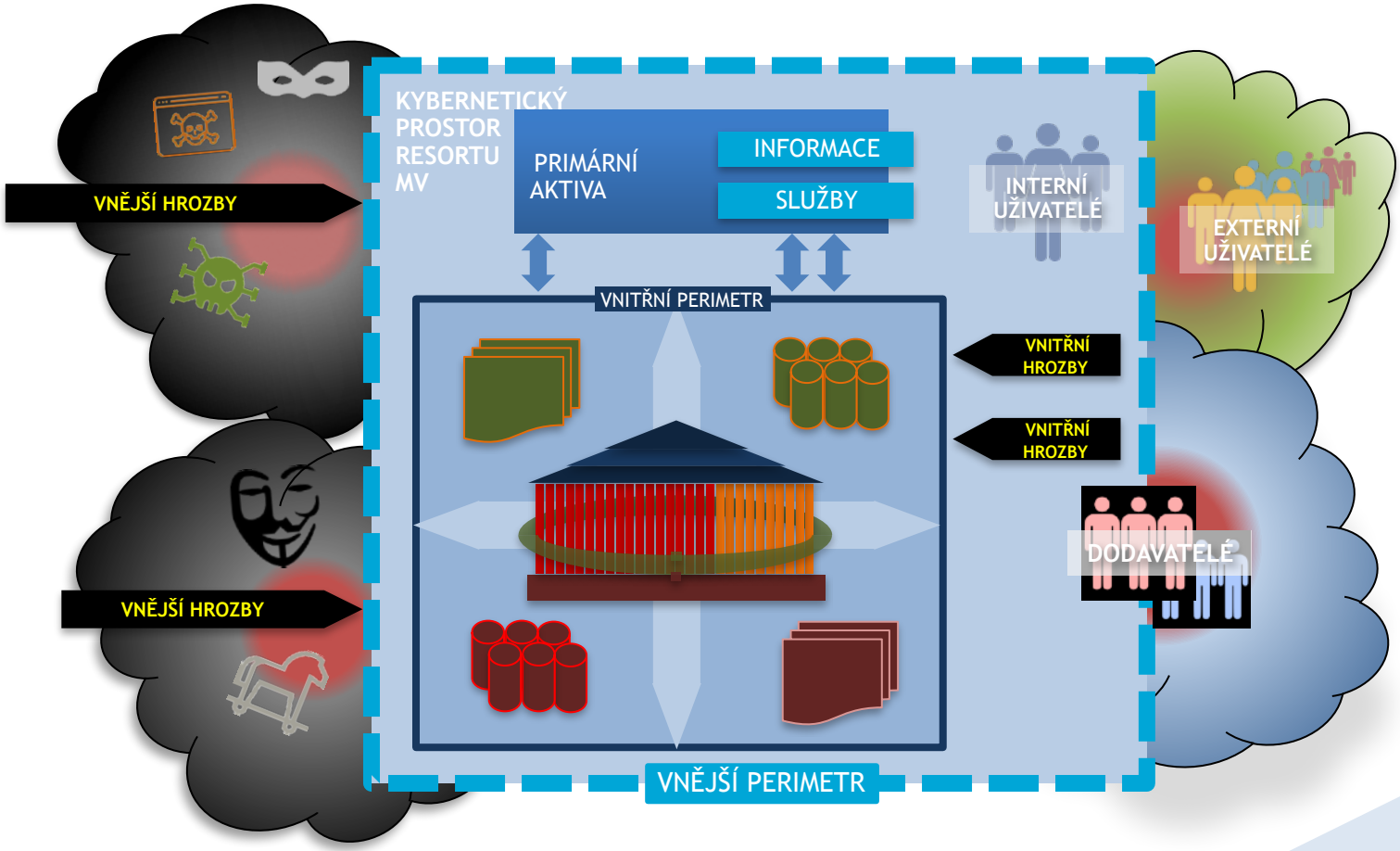
Kybernetická bezpečnost resortu MV

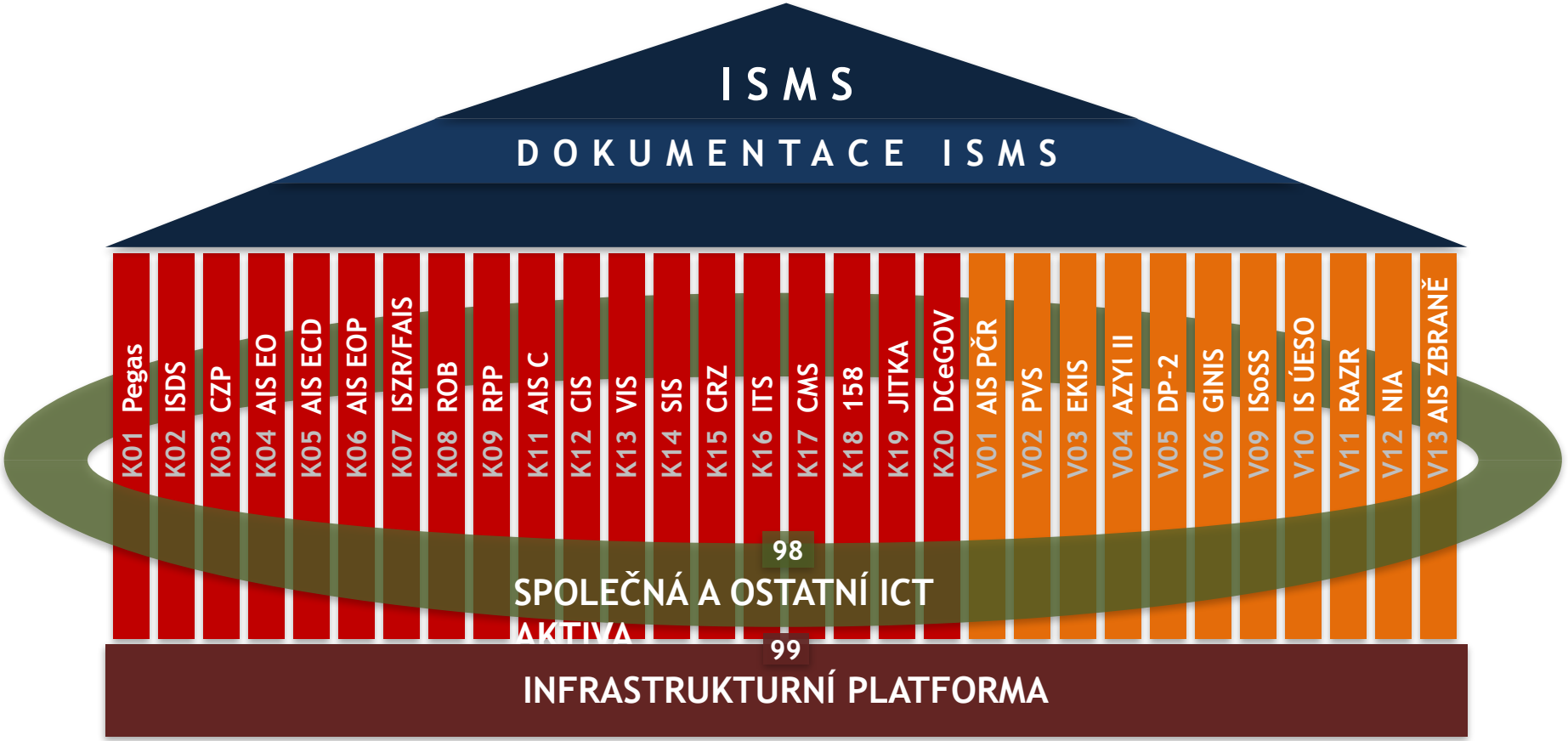
- Cílem a úlohou kybernetické bezpečnosti resortu MV je zabezpečení kybernetického prostoru proti vnějším a vnitřním kybernetickým hrozbám prostřednictvím organizačních a technických opatření a minimalizace možných důsledků případných kybernetických událostí nebo incidentů.
- Bezpečnost kybernetického 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.

Organizace KB v resortu MV

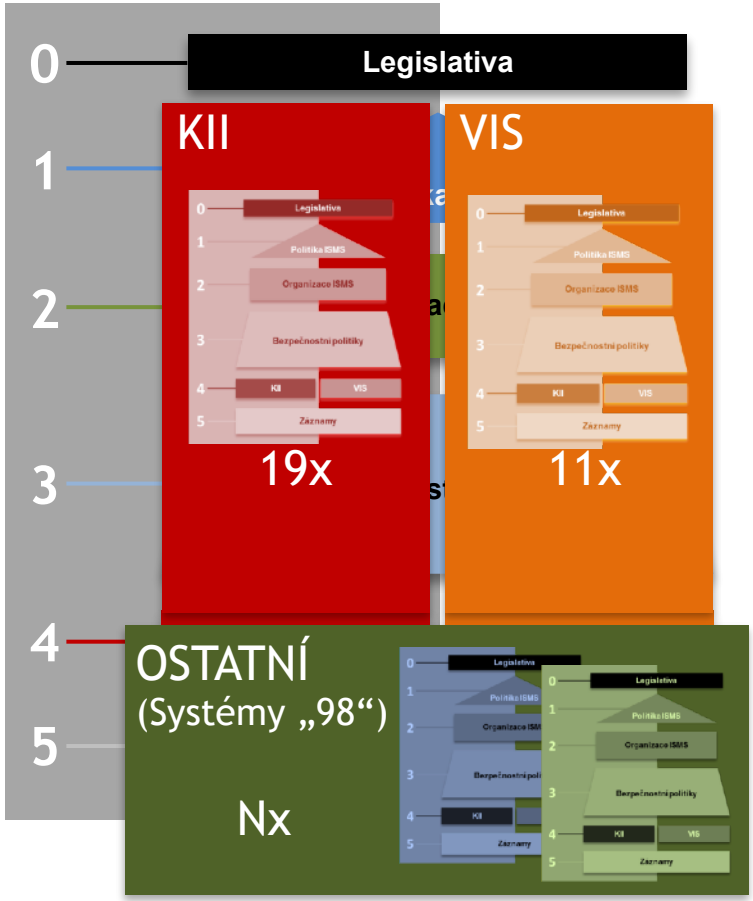


Systém řízení bezpečnosti informací resortu MV


KYBERNETICKÝ PROSTOR RESORTU MV
PRIMÁRNÍ AKTIVA
INFORMACE
SLUŽBY
VNĚJŠÍ HROZBY
VNĚJŠÍ HROZBY
VNITŘNÍ PERIMETR
VNITŘNÍ HROZBY
VNITŘNÍ HROZBY
INTERNÍ UŽIVATELÉ
EXTERNÍ UŽIVATELÉ
DODAVATELÉ
VNĚJŠÍ PERIMETR



Rozsah ISMS resortu MV


0
1
2
3
4
5
Legislativa
KII
Legislativa
Politika ISMS
Organizace ISMS
Bezpečnostní politiky
KII
VIS
Záznamy
19x
VIS
Legislativa
Politika ISMS
Organizace ISMS
Bezpečnostní politiky
KII
VIS
Záznamy
11x
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.

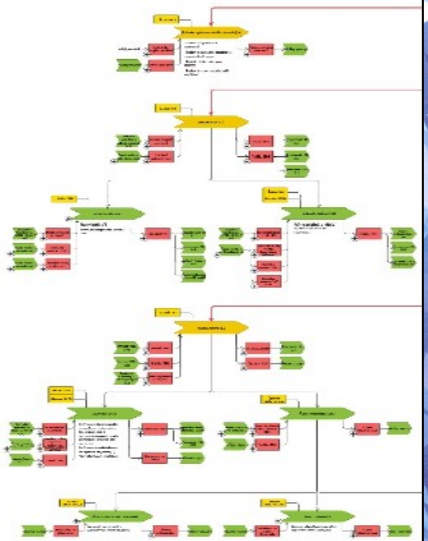
Zásada VII. Ztrátu nebo odcizení mobilní pracovní stanice nebo přiděleného paměťového nosiče bez zbytečného prodlení ohlásit odbornému útvaru ICT.

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

- ISMS certifikace



CERTIFIKÁT

č. 42012425

LL-C Certification

Osvědčujeme a prohlašujeme, že systém managementu bezpečnosti informací ve společnosti

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

Místo poskytování služeb:
Odbor kybernetické bezpečnosti a koordinace ICT, Nám. Hrdinů 1634/3, 14021 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 významné IS, IS a KS systémy kritické infrastruktury resortu MVCR.

PoA 2017 ISMS 05.50-2017

Tento certifikát byl vydán pod číslem **42012425** a je platný od 11. ledna 2019 do 10. ledna 2022. První certifikát byl vystaven dne 11. ledna 2016.

Schválil

Vytiskl

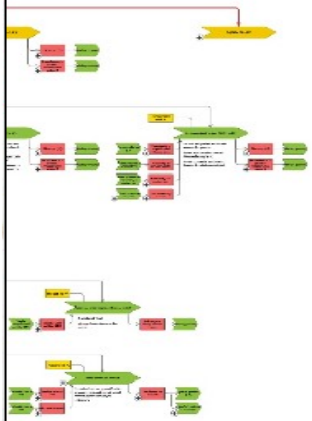
S 3137

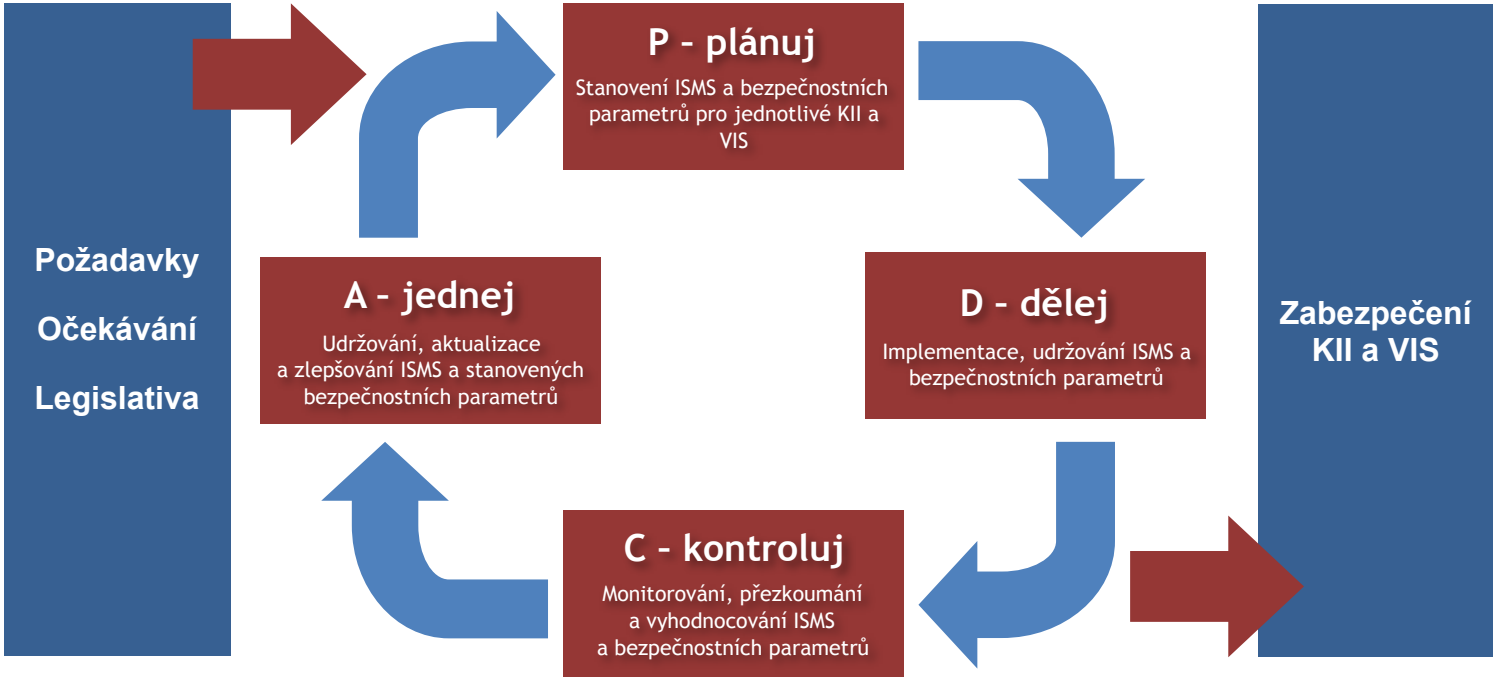
ověřovací kód: **97FCD6C1-4D6**

Platnost certifikátu ověřte tímto kódem na www.ll-c.info

www.ll-c.net

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




Požadavky
Očekávání
Legislativa
P - plánuj
Stanovení ISMS a bezpečnostních parametrů pro jednotlivé KII a VIS
D - dělej
Implementace, udržování ISMS a bezpečnostních parametrů
C - kontroluj
Monitorování, přezkoumání a vyhodnocování ISMS a bezpečnostních parametrů
A - jednej
Udržování, aktualizace a zlepšování ISMS a stanovených bezpečnostních parametrů
Zabezpečení KII a VIS

Aktualizace dokumentace ISMS

- Nástroj pro hodnocení aktiv a rizik.
- Hodnocení aktiv: **D= MAX(Du; In; Do)**
- Výpočet míry rizika: **MR= D × Z × H**
- Legenda:

Zkratka	Popis	Vysvětlení
D	Dopad (hodnota aktiva)	/
Du	Důvěrnost	Zhodnocení dopadu neautorizovaného vyzrazení dat.
In	Integrita	Zhodnocení dopadu neautorizované úpravy dat.
Do	Dostupnost	Zhodnocení dopadu ztráty přístupu k datům.
MR	Míra rizika	Možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu.
AR	Akceptovatelné riziko	Riziko, které je přijatelné a není nutné jej zvládat pomocí dalších bezpečnostních opatření.
Z	Zranitelnost	Slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.
H	Hrozba	Potenciální příčina KBU nebo KBI, která může způsobit škodu a která působí na jeden nebo více atributů informační bezpečnosti

Míra akceptovatelnosti rizik

Úroveň	Hranice míry rizika	Popis	Od	Do
Nízká	**20 %**	Riziko je považováno za přijatelné – akceptovatelné.	1	13
Střední	**48 %**	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné na základě schválení Výboru KB.	14	31
Vysoká	**73 %**	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.	32	47
Kritická	**–**	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.	48	64

		Hrozba × zranitelnost								
		1	**2**	**3**	**4**	**6**	**8**	**9**	**12**	**16**
Hodnota aktiva	**1**	1	2	3	4	6	8	9	12	16
	2	2	4	6	8	12	16	18	24	32
	3	3	6	9	12	18	24	27	36	48
	4	4	8	12	16	24	32	36	48	64

- Poznatky při aktualizaci dokumentace ISMS:
  - Slučování dokumentů a jejich provazba.
  - Jasně nastavené procesy a pravidla.
  - Jednotnost zkratek a pojmů.
  - Jednoduchá textace s ohledem na adresáty.
  - Procesní uchopení tvorby dokumentace.
- Základní pravidla při tvorbě dokumentace ISMS:
  1. Určení jasných rolí a odpovědností.
  2. Neopakovat nic, co už je někde napsáno (pouze tam, kde to má smysl).
  3. Nepsat do dokumentace obecné nic neříkající formulace.
  4. Psát jasná a jednoznačná pravidla a postupy.
  5. Zachovat logičnost dokumentů, tzv. červenou nit.
  6. Pokud je to možné a dává to smysl, vytvářet procesní modely.

Úskalí zajišťování kybernetické bezpečnosti

- Příprava nové vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.
  - Nevyjasněny personální ani finanční dopady.
  - V rámci resortu MV by došlo k rozšíření z 30 systémů KII a VIS na 200.
- Varování Národního úřadu pro kybernetickou a informační bezpečnost o hrozbě ze dne 17. prosince 2018.
  - Nejednoznačnost postupu.
  - Těžko uchopitelné:
    - V případě vyloučení společnostní zmíněných ve varování hrozí riziko soudních řízení ze strany Úřadu pro ochranu hospodářské soutěže a soudních řízení ze strany vyloučených společností.
    - V případě nezohlednění varování hrozí riziko sankcí ze strany Národního úřadu pro kybernetickou a informační bezpečnost a případné uskutečnění hrozeb technických a programových prostředků.

14

NAŘÍZENÍ

Ministerstva vnitra

a

SPOLEČNÝ SLUŽEBNÍ PŘEDPIS

náměstka ministra vnitra pro státní službu a státního tajemníka v Ministerstvu vnitra

ze dne 7. května 2018

o povinnosti absolvovat Základní kurz kybernetické bezpečnosti

K zajištění splnění povinnosti státních zaměstnanců a zaměstnanců v základním pracovněprávním vztahu na Ministerstvu vnitra absolvovat Základní kurz kybernetické bezpečnosti **se stanoví**:

Čl. 1
Pojmy

Pro účely tohoto nařízení a společného služebního předpisu se rozumí:

a) přístupem do kybernetického prostoru Ministerstva vnitra využívání elektronické pošty a dalších digitálních služeb Ministerstva vnitra;

b) zaměstnancem zaměstnanec v základním pracovněprávním vztahu s přístupem do kybernetického prostoru Ministerstva vnitra, za zaměstnance se považuje též státní zaměstnanec s přístupem do kybernetického prostoru Ministerstva vnitra;

c) Základním kurzem kybernetické bezpečnosti e-learningový kurz k získání povědomí a osvojení si základních pravidel bezpečného využívání kybernetického prostoru pro zaměstnance veřejné správy, kteří mají přístup do kybernetického prostoru[1] příslušné organizace veřejné správy, vytvořený a certifikovaný Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „Úřad");

d) evidenčním číslem zaměstnance osobní evidenční číslo zaměstnance v základním pracovněprávním vztahu a evidenční číslo státního zaměstnance.

Čl. 2
Povinnost absolvovat kurz a přihlašování do kurzu

(1) Zaměstnanec je povinen absolvovat Základní kurz kybernetické bezpečnosti (dále jen „kurz"), a to do 6 měsíců ode dne zahájení výkonu práce nebo státní služby na pracovním místě nebo služebním místě zařazeném v Ministerstvu vnitra. Tato povinnost neplatí v případě zařazení zaměstnance na systemizované místo v Ministerstvu vnitra z jiného služebního úřadu, pokud kurz absolvoval před méně než 2 roky.

[1] § 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

ní změn, negativn… pravidel.

čnost je vnímán… .

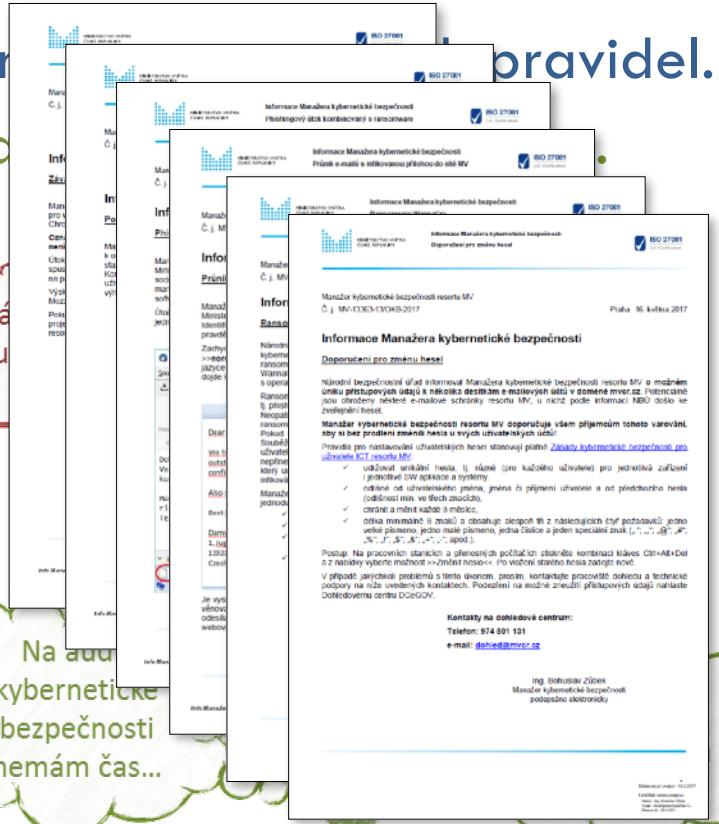
ovědnost.

Nemá … popisu…

Nechci být garantem!

má být to … slo tak … ožité?

Na aud… kybernetické bezpečnosti nemám čas…

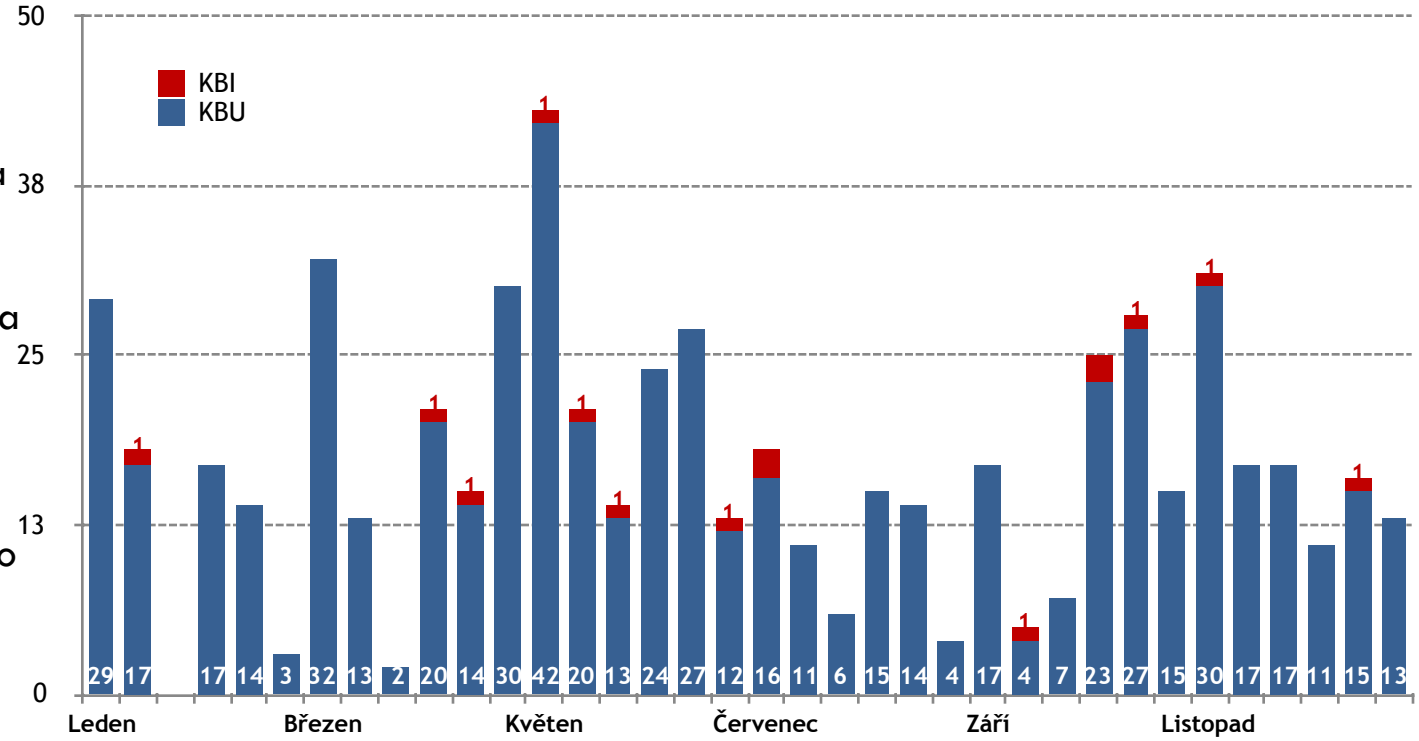


Vývoj KBU a KBI v letech 2016-2018

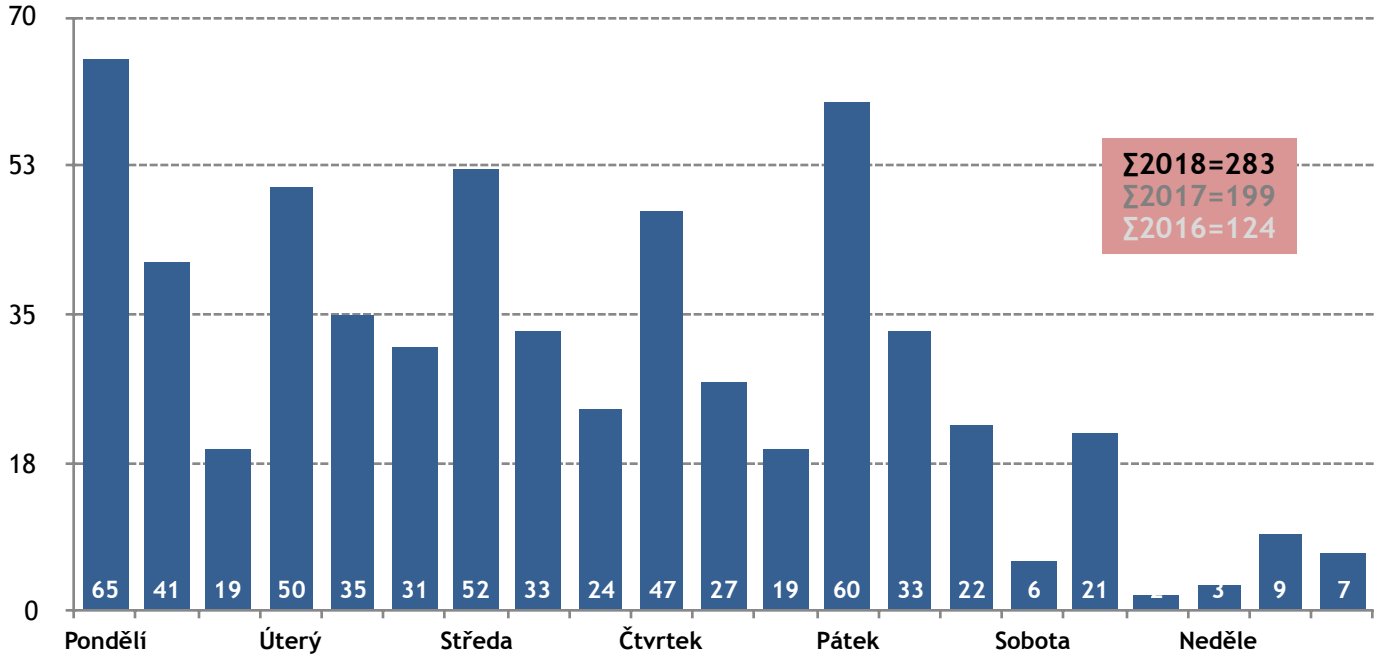
Vývoj KBU a KBI v letech 2016-2018

Σ2018=283
Σ2017=199
Σ2016=124

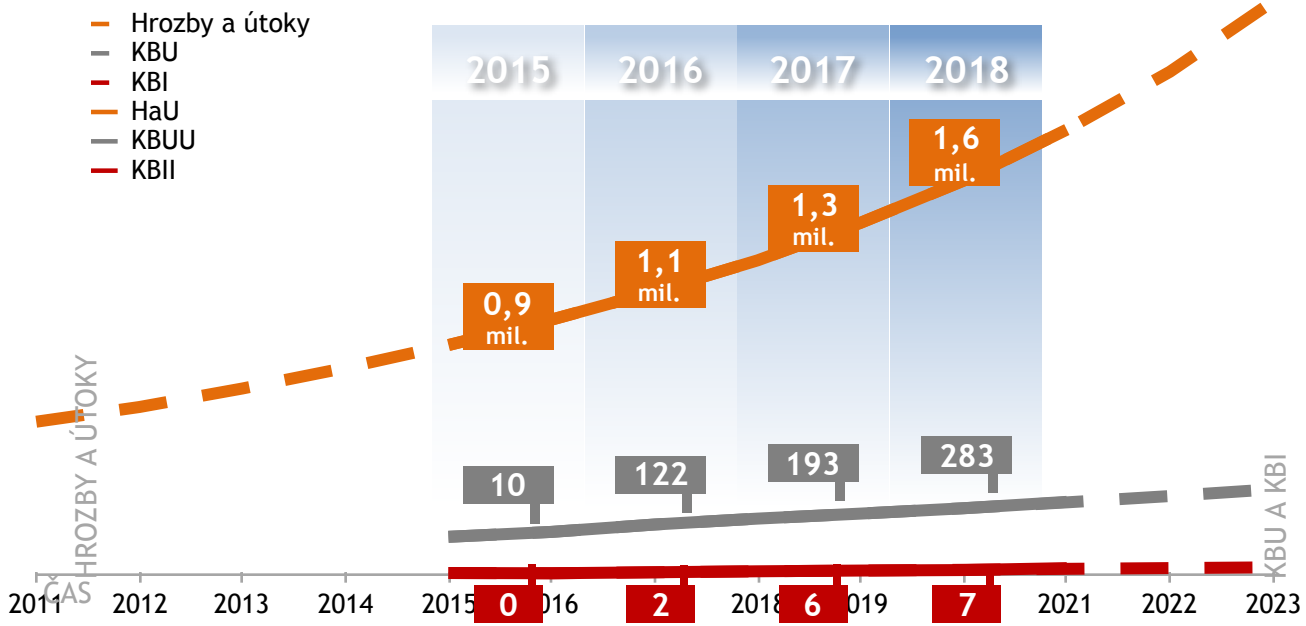
- Celkový počet tiketů na DCeGOV: **53.365.**
- Celkový počet bezpečnostních tiketů na DCeGOV: **6671.**
- Počet **kybernetických bezpečnostních událostí** vzrostl v roce 2018 proti roku 2017 o 43 % na **276.**
- Počet **kybernetických bezpečnostních incidentů** se zvýšil o 1, konkrétně na **7.**



Vývoj KBU a KBI v letech 2016-2018

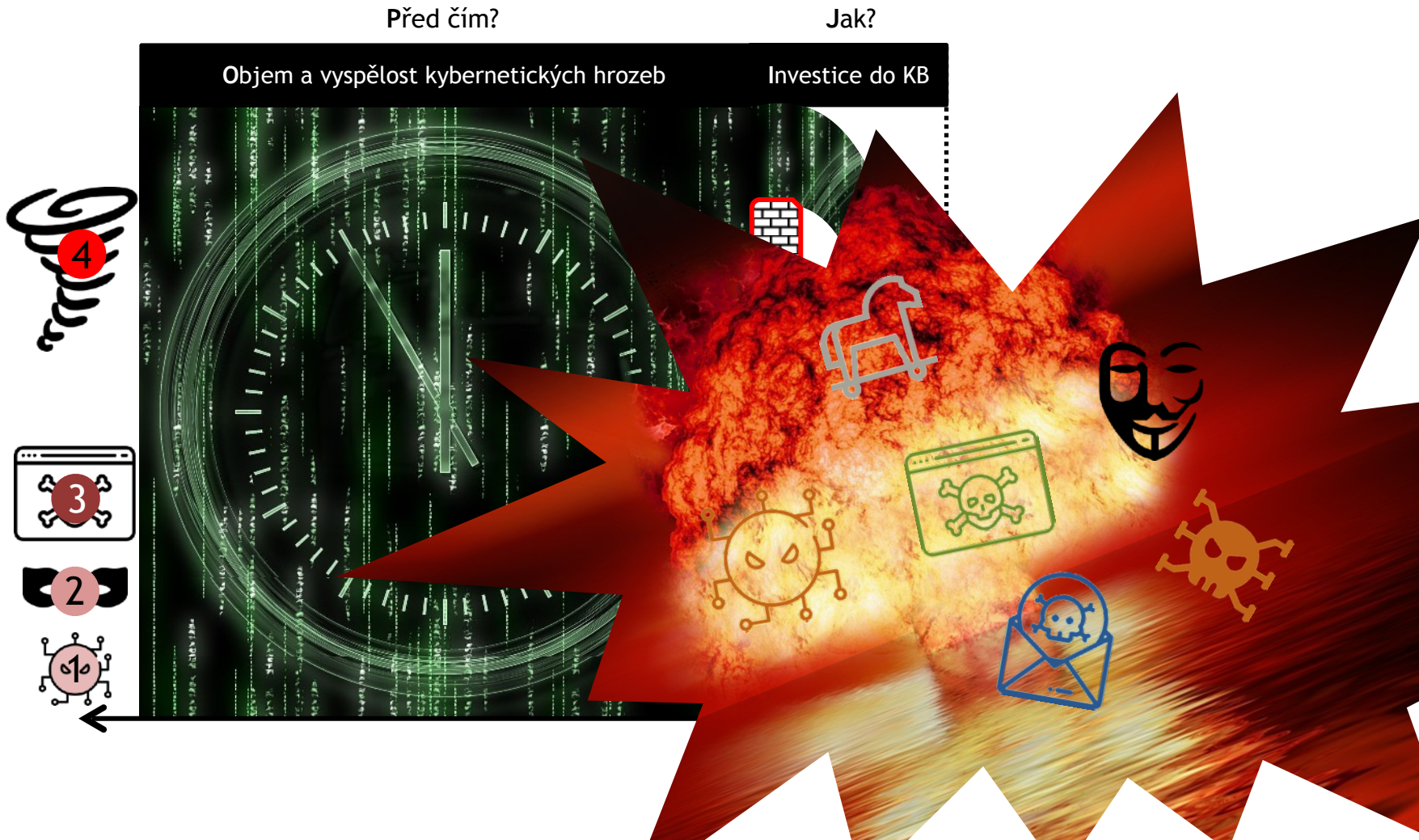


	2018	2017	2016
Největší počet KBU a KBI	Pondělí	Pondělí	Úterý
Nejmenší počet KBU a KBI	Neděle	Neděle	Sobota

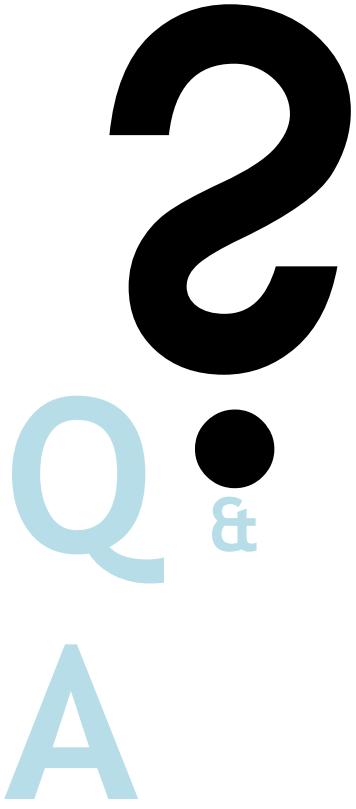


Hrozby a události v kybernetickém prostoru resortu MV

Hrozby a investice do zabezpečení



Diskuze



Děkuji za pozornost a Váš čas.

Ing. Miroslav Tůma, Ph.D.

Ředitel odboru kybernetické bezpečnosti a koordinace ICT