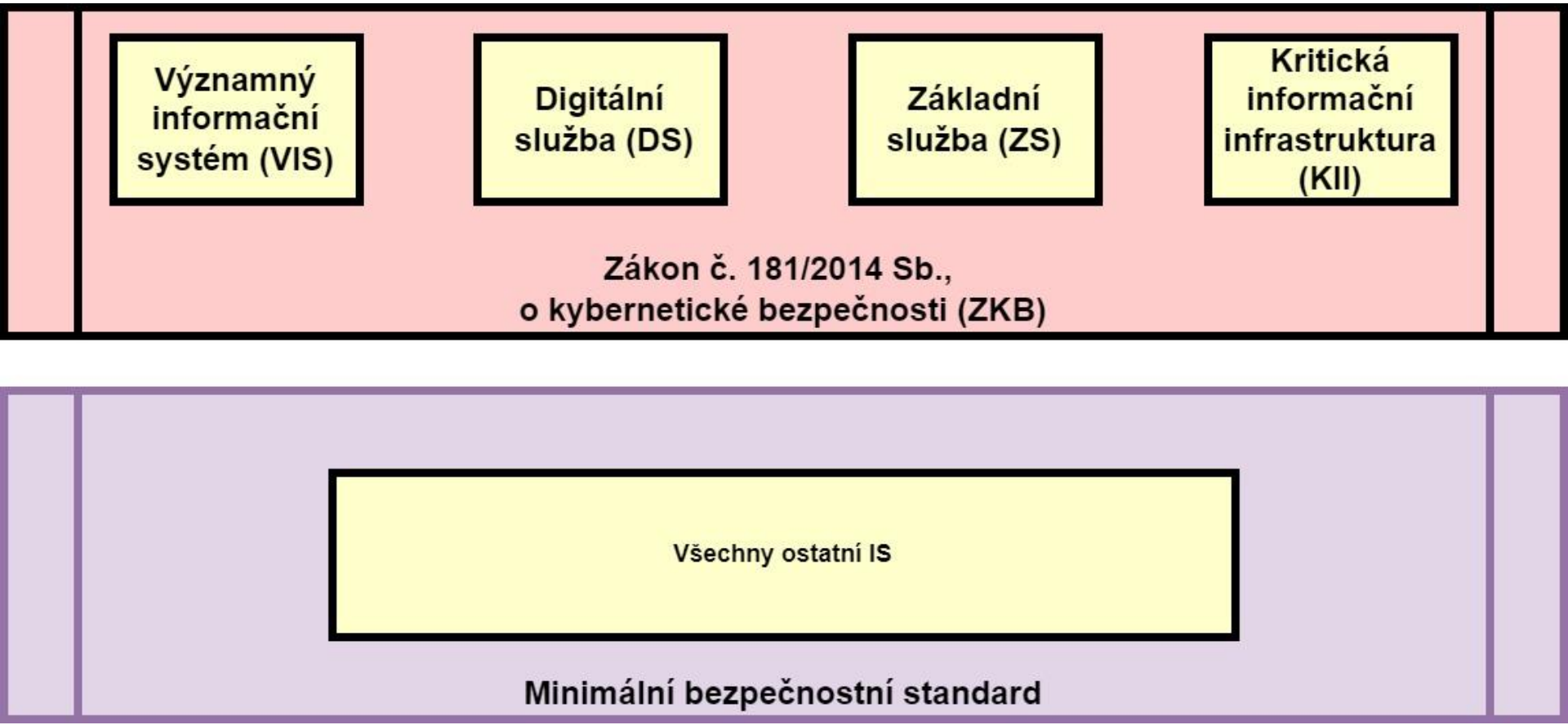
NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

Minimální bezpečnostní standard


Významný informační systém (VIS)
Digitální služba (DS)
Základní služba (ZS)
Kritická informační infrastruktura (KII)
Zákon č. 181/2014 Sb.,
o kybernetické bezpečnosti (ZKB)
Všechny ostatní IS
Minimální bezpečnostní standard

NAKIT

Jak Minimální bezpečnostní standard vznikl?

- součinnost:
  - NÚKIB
  - NAKIT
  - MV
  - odborná veřejnost
- první polovina roku 2020

MINIMÁLNÍ BEZPEČNOSTNÍ STANDARD

podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Verze 1.0, platná ke dni 17. července 2020

Proč Minimální bezpečnostní standard vznikl?

- nutnost chránit aktiva IS, která nespadají pod regulaci zákona č. 181/2014 Sb. (ZKB)
- správci menších IS nespadajících pod ZKB neměli k dispozici návodný metodický materiál sjednocující postupy
- potřeba mít alespoň rámcový přehled, co a jak z pohledu kybernetické bezpečnosti řešit

NAKIT

Co je Minimální bezpečnostní standard?

- jedná se o doporučení / pomůcku
- vychází z obecných standardů a ZKB
- základní bezpečnostní požadavky na IS
- dobrý začátek i tam, kde by v budoucnosti mohlo dojít k regulaci dle ZKB
- je psán zjednodušenou formou, aby byl snadno pochopitelný
- je otevřený budoucímu rozvoji

NAKIT

Co Minimální bezpečnostní standard naopak není?

- složitý na čtení a pochopení
- úplný a vyčerpávající
- závazný a nenahrazuje žádný ze zákonů ani prováděcích právních předpisů

NAKIT

Minimální bezpečnostní standard

- členěn do dvou částí:

1. Manažerská část

- určena pro vedoucí pracovníky
- zahrnuje popisy postupů, které by měla organizace zavést a dodržovat

Základní předpoklady

Plán zavádění bezpečnostních opatření

Klasifikace a ochrana informací

Řízení dodavatelů

Řízení lidských zdrojů

Řízení změn

Řízení kontinuity činností

Audit kybernetické bezpečnosti

2. Technická část

- určena pro IT specialisty
- obsahuje konkrétní návody, jak zajistit minimální úroveň bezpečnosti

Fyzická bezpečnost

Řízení přístupů

Požadavky v oblasti ochrany před škodlivým kódem

Kybernetické bezpečnostní události a incidenty

Požadavky v oblasti aplikační bezpečnosti

Kryptografické prostředky

Požadavky v oblasti zajišťování úrovně dostupnosti informací

Požadavky v oblasti cloudových služeb

Další požadavky

NAKIT

Závěr / Odkazy na dokumenty

- **Minimální bezpečnostní standard** k dispozici například zde:
  https://nakit.cz/experti-z-nukib-nakit-a-ministerstva-vnitra-spojili-sily-kvuli-zabezpeceni-mensich-organizaci/

- Pár dalších dokumentů:
  - **Bezpečnostní standard pro videokonference**
    https://nakit.cz/predstavujeme-bezpecnostni-standard-pro-videokonference/
  - **Doporučení pro bezpečné nakládání s e-identitou**
    https://nakit.cz/pruvodce-svetem-elektronicke-identity/
  - **Ransomware: Doporučení pro mitigaci, prevenci a reakci**
    https://www.nukib.cz/download/publikace/podpurne_materialy/Ransomware%20-%20Doporuceni_pro_mitigaci_prevenci_a_reakci.pdf
- Mnoho dalších doporučení a dokumentů naleznete například na stránkách NÚKIB.

NAKIT

Děkuji

Q&A

Vladimír Rohel

E: vladimir.rohel@nakit.cz
M: +420 725 755 418

W: www.nakit.cz

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.