Národní bezpečnostní úřad

Národní
bezpečnostní
úřad

Legislativa ČR v oblasti kybernetické bezpečnosti

Václav Borovička

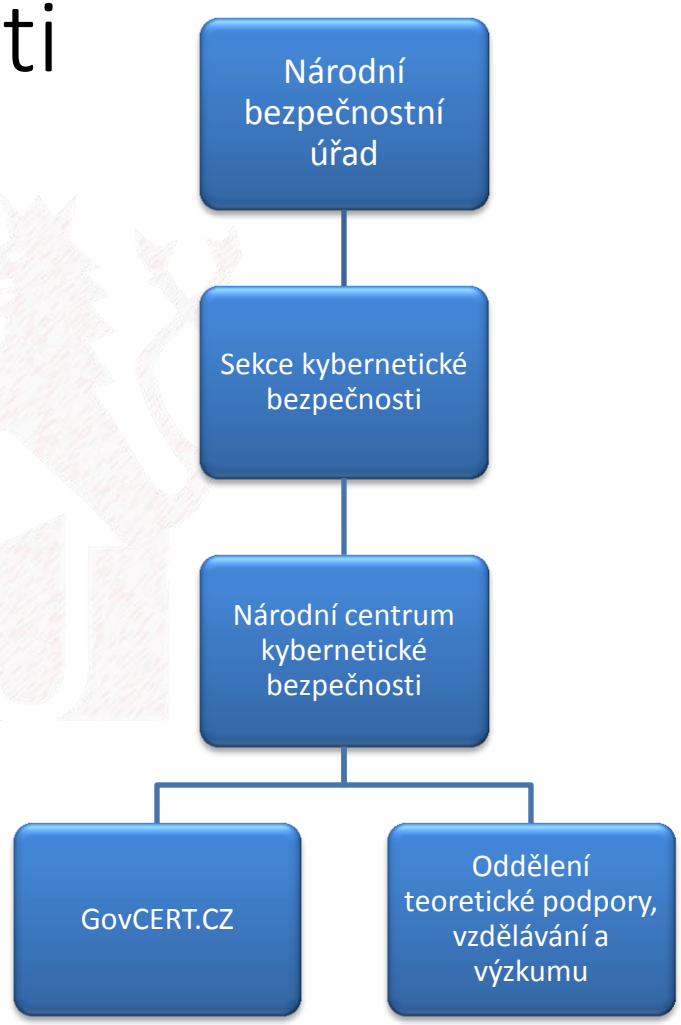
IDET AFCEA
Květen 2015, Brno

Obsah přednášky

- Úvod do legislativy kybernetické bezpečnosti
- Kybernetické předpisy – zákon č. 181/2014 Sb., o kybernetické bezpečnosti (dále také „ZKB“)
- První zkušenosti se ZKB
- Možný budoucí vývoj

Národní centrum kybernetické bezpečnosti

- OTPVV
  - „Strategy and policy unit“
  - netechnická část NCKB
- GovCERT.CZ
  - vládní CERT
  - technická část



Úvod do legislativy kybernetické bezpečnosti

„Kybernetická bezpečnost představuje ***souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů*** *směřujících* ***k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice****, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost. Kybernetická bezpečnost pomáhá* ***identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže*** *ve smyslu* ***posilování důvěrnosti, integrity a dostupnosti dat, systémů*** *a dalších prvků informační a komunikační infrastruktury.* ***Hlavním smyslem kybernetické bezpečnosti je pak ochrana prostředí k realizaci informačních práv člověka.“***

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020

Úvod do legislativy kybernetické bezpečnosti

- … právní předpisy směřující k posílení důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury…

!! nejedná se pouze o ZKB !!

- legislativa kybernetické bezpečnosti
  - **širší pojetí**
    - občanské, obchodní, správní, trestní, ústavní právo
  - **užší pojetí**
    - ZKB a prováděcí předpisy

Obecné důvody zajištění KB
Ústavní základy, mezinárodní závazky

- informační sebeurčení člověka
- ochrana nedistributivních práv
- obecná odpovědnost státu
  - due diligence – prevenční působení státu
- Evropská směrnice o bezpečnosti sítí a informací (NIS)
- Spojenecké závazky (NATO)

Obecné důvody zajištění KB
Změny ve společnosti

- Vzrůstající závislost státu na ICT
- Vzrůstající kritičnost narušení ICT
- Zvyšující se propojenost systémů a služeb
- Závislost obyvatelstva a celé ekonomiky na ICT
- Rostoucí počet kybernetických útoků

Specifické důvody přijetí ZKB

- Kybernetická bezpečnost řešena prostřednictvím soukromých / akademických subjektů, bez právní regulace
- Nedostatek koordinace / nedostatečné sdílení informací
- Kybernetická ochrana roztříštěná a neefektivní
- Nebyly stanoveny povinné bezpečnostní standardy kybernetické bezpečnosti pro důležité systémy pro stát (s výjimkou ICT s utajovanými informacemi)

- Nutnost zajistit koordinovaný postup zajištění kybernetické bezpečnosti zejména u důležitých systémů pro stát
  - Nezbytnost regulace zákonem

Kybernetické předpisy

- Hlavní
  - **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti** a o změně souvisejících předpisů
  - Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (**vyhláška o kybernetické bezpečnosti**) (dále také „VKB“)
  - Vyhláška č. 317/2014 Sb., kterou se stanoví **významné informační systémy a jejich určující kritéria** (dále také „VVIS“)
  - Novelizované nařízení vlády ze dne 22. prosince 2010 č. 432/2010 Sb., **o kritériích pro určení prvku kritické infrastruktury**

Kybernetické předpisy

- Související
  - Zákon č. 127/2005 Sb., o elektronických komunikacích (dále také „ZEK“)
  - Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (dále také „KrZ“)

Cíle právní úpravy

- Stanovit základní úroveň bezpečnostních opatření
- Zlepšit detekci kybernetických bezpečnostních incidentů
- Zavést hlášení kybernetických bezpečnostních incidentů
- Zavést systém opatření k reakci na kybernetické bezpečnostní incidenty
- Upravit činnost dohledových pracovišť

- NENÍ CÍLEM zasahovat do obsahu
  - pouze zabezpečit informační kanály, jimiž člověk realizuje své právo na informační sebeurčení, proti úmyslným nebo nahodilým bezpečnostním incidentům

Co ZKB (ne)upravuje

- §1 odst. 1 ZKB:

„Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.“

- §1 odst. 2 ZKB:

„Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.“

- Zakotvuje hlavní pilíře zajištění kybernetické bezpečnosti
- Upravuje práva a povinnosti některých osob v oblasti kybernetické bezpečnosti
- Poskytuje oprávnění NBÚ v oblasti kybernetické bezpečnosti (§22 ZKB)

Hlavní principy ZKB

1) Individuální odpovědnost za bezpečnost vlastní sítě
   - důležitost spolupráce a důvěry soukromého sektoru
2) Autonomie vůle regulovaných subjektů
3) Technologická neutralita
   - striktní zaměření k technologickým aspektům fungování nezasahování do informačního obsahu
   - užití obecných kritérií pro standardní zabezpečení IS a sítí el. komunikací
4) Minimalizace zásahů do práv soukromoprávních subjektů
5) Minimalizace státního donucení
6) Právo na informačního sebeurčení člověka
7) Ochrana nedistributivních práv
8) Princip bdělosti ve vztahu k ostatním státům a k mezinárodnímu společenství

Dohledová pracoviště

Rozdělení gesce

- Dohledová pracoviště
  - **Vládní CERT** a **Národní CERT**
  - Hlavní úkol:
    - vyhodnocování kybernetické bezpečnostní situace v informačních a komunikačních systémech, a
    - ochrana těchto systémů před kybernetickými bezpečnostními incidenty.
  - Základním smyslem fungování obou dohledových pracovišť je vyhodnocování informací o výskytu kybernetických bezpečnostních incidentů z pokud možno co největšího množství informačních a komunikačních systémů.
  - Soukromoprávní X Veřejnoprávní
    - Výhody ?
  - Spolupráce

Povinné osoby

- §3 ZKB

a) poskytovatelé služeb elektronických komunikací, a subjekty zajišťující sít elektronických komunikací, b) orgán nebo osoba zajišťující významnou síť	NÁRODNÍ CERT
c) správce IS KII d) správce KS KII e) správce VIS	VLÁDNÍ CERT

Určování

§ 3 ZKB:

a) poskytovatelé služeb elektronických komunikací, a subjekt zajišťující sít elektronických komunikací,

b) orgán nebo osoba zajišťující významnou síť

Proces určování neprobíhá

---

§ 3 ZKB:

c) správce IS KII

d) správce KS KII

Určování dle krizového zákona

---

§ 3 ZKB:

c) správce VIS

Přímá identifikace + posuzování správcem

Hlavní pilíře ZKB

- Bezpečnostní opatření (standardizace)
- Hlášení kybernetických bezpečnostních incidentů
- Opatření NBÚ

Hlavní pilíře ZKB

Bezpečnostní opatření (§§ 4 a 5 ZKB)

- Bezpečnostním opatřením se rozumí souhrn úkonů a postupů, jejichž cílem je zajištění bezpečnosti informací a dostupnosti a spolehlivosti služeb a sítí v kybernetickém prostoru.

- Druhy bezpečnostních opatření:
  - organizační opatření,
  - technická opatření.

- Specifikováno v VKB

Hlavní pilíře ZKB

Hlášení kybernetického bezpečnostního incidentu (§ 8 ZKB)

- Navázáno na povinnost poskytnout kontaktní údaje (§16 ZKB)
  - vytvoření přehledu důležitých subjektů KB v ČR
  - aktualizované údaje na osoby zodpovědné za dané systémy

- Hlášení
  - KII a VIS hlásí vládnímu CERT
  - Soukromoprávní osoby hlásí národnímu CERT
  - Ve VKB stanoveny:
    - typy a kategorie kybernetických bezpečnostních incidentů,
    - náležitosti a způsob hlášení kybernetického bezpečnostního incidentu.

Hlavní pilíře ZKB

Opatření (§§ 4 a 5 ZKB)

- varování
  - oficiální publikace informací o bezpečnostní hrozbě, tj. preventivní informování povinných osob
- reaktivní opatření
  - okamžitá reakce na výskyt kybernetického bezpečnostního incidentu
  - obsahem mohou být povinnosti provést konkrétní úkony nutné k odvrácení kybernetického bezpečnostního incidentu nebo ke zmírnění jeho následků
- ochranné opatření
  - nutnost reagovat na vyřešený kybernetický bezpečnostní incident a na základě získaných zkušeností obecně zvýšit kvalitu ochrany informačních systémů, služeb a sítí elektronických komunikací u povinných osob

Povinnosti subjektů

- Nahlášení kontaktních údajů (§16 ZKB)
  - Všechny povinné osoby
- Hlášení kybernetických bezpečnostních incidentů (§8 ZKB)
  - KII, VIS, správcové významných sítí
- Zavést bezpečnostní opatření (standardizace) (§4 ZKB)
  - KII a VIS
- Činit opatření vydané NBÚ (§11 ZKB)
  - KII a VIS
  - Správci významných sítí a poskytovatelé služby el. komunikací pouze za stavu kybernetického nebezpečí, pouze reaktivní opatření (viz dále)

Stav kybernetického nebezpečí

- Stav mimořádný, speciální oproti mimořádným stavům vyhlašovaným podle ústavního zákona č. 110/1998 Sb. o bezpečnosti České republiky nebo podle krizového zákona č. 240/2000 Sb.
- Možno vyhlásit pokud je **ve velkém rozsahu ohrožena bezpečnost informací v IS, bezpečnost služeb nebo sítí elektronických komunikací a tím dojde k ohrožení nebo porušení zájmu České republiky**.
- Stav KN vyhlašuje ředitel NBÚ.
- Vyhlašován na dobu nejdéle 7 dnů, souhrnná doba nesmí přesáhnout 30 dnů.
- Za stavu kybernetického nebezpečí a za nouzového stavu je Úřad oprávněn vydat opatření podle § 15 (reaktivní opatření) rovněž orgánům a osobám uvedeným v § 3 písm. a) a b).

Kontrola a další činnost v oblasti KB

- NBÚ vykonává kontrolu v oblasti kybernetické bezpečnosti. Při výkonu kontroly Úřad zjišťuje, jak povinné osoby plní povinnosti stanovené ZKB, prováděcími právními předpisy, rozhodnutími a opatřeními obecné povahy vydanými Úřadem.

- Nápravná opatření - § 24 ZKB

- Vedle toho také NBÚ v oblasti kybernetické bezpečnosti zajišťuje také:
  - výzkum a vývoj
  - prevenci, vzdělávání,
  - metodickou podporu

Sankce v oblasti KB

!! Princip minimalizace zásahů do práv třetích osob, minimalizace státního donucení !!

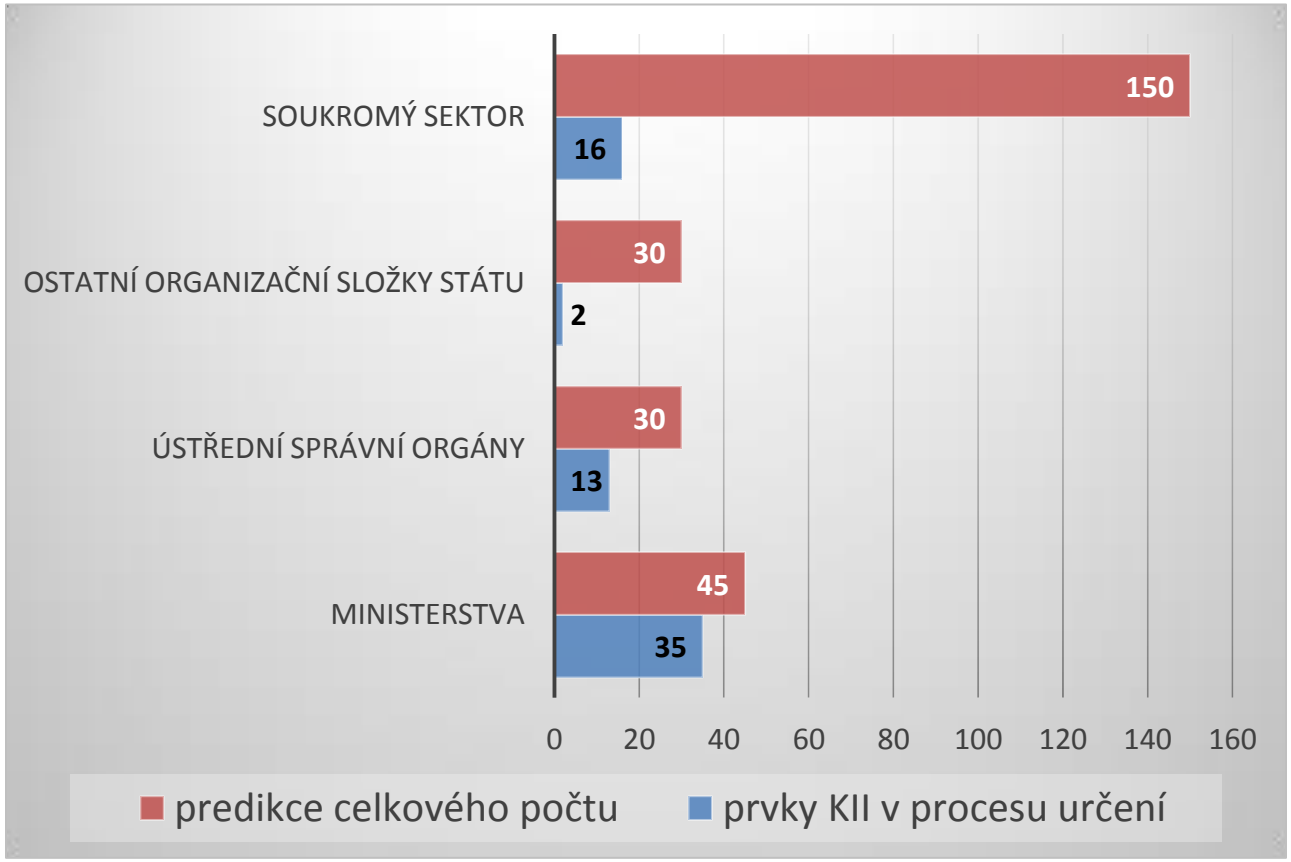
- Povinná osoba uvedená v § 3 písm. c) až e) se dopustí správního deliktu tím, že
  a) v rozporu s § 4 odst. 2 nezavede nebo neprovádí bezpečnostní opatření anebo nevede bezpečnostní dokumentaci,
  b) neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 3,
  c) nesplní povinnost uloženou Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13 nebo § 14,
  d) neoznámí kontaktní údaje nebo jejich změnu podle § 16 odst. 2 písm. b) nebo
  e) nesplní některou z povinností uloženou nápravným opatřením podle § 24.

- Za správní delikt lze uložit pokutu **do** 100 000 Kč s výjimkou deliktu podle písmene d), kde hrozí sankce **až** 10 000 Kč.

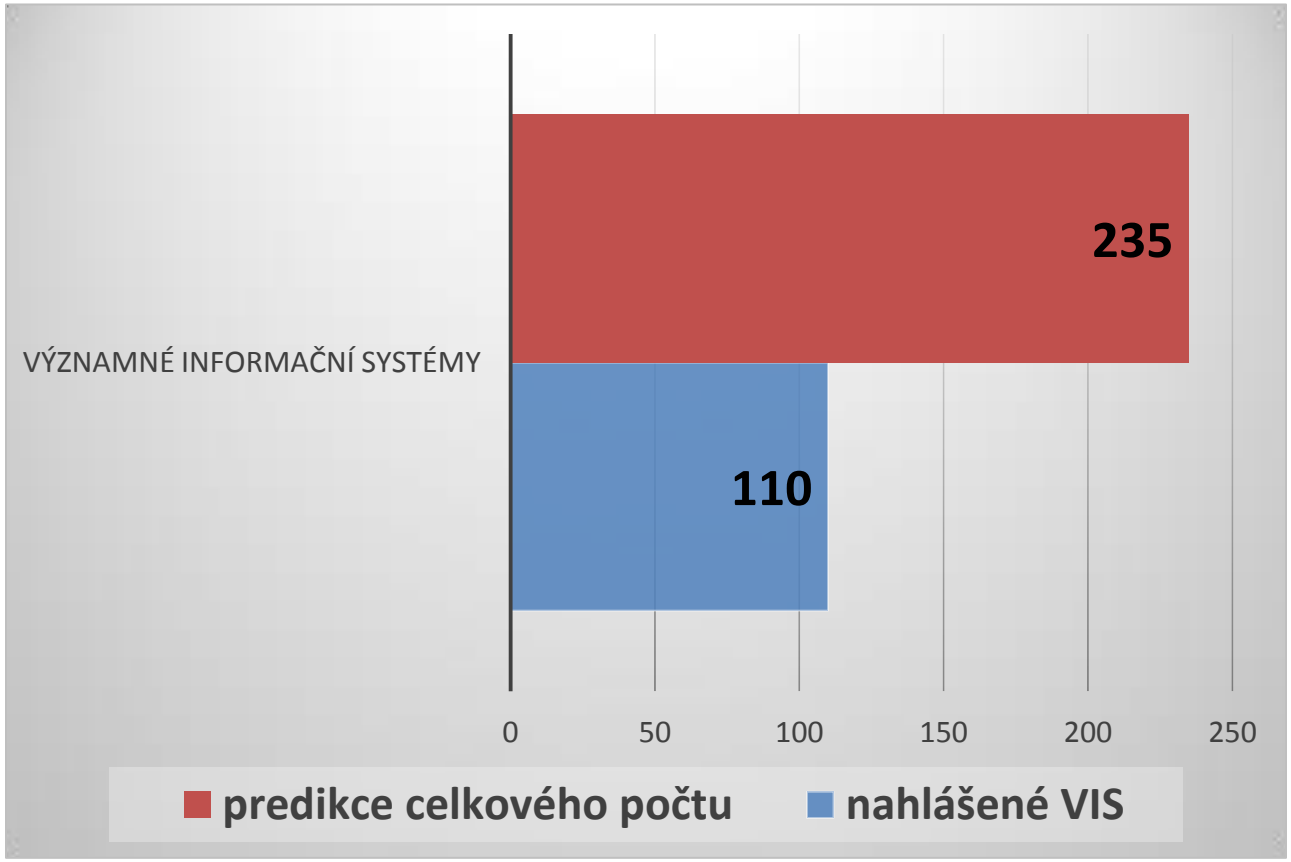
První zkušenosti

- Určování KII
  - Ukončeny první fáze – určování KII u veřejnoprávních subjektů
  - Nyní určována KII u soukromoprávních subjektů + druhá část veřejné správy
- Identifikace VIS
  - komunikace a pomoc orgánům veřejné moci, jejichž systémy splňují určující kritéria avšak nejsou uvedeny v příloze č. 1 vyhlášky
- Fungování NCKB

Současný stav a predikce určování KII prvků v daných oblastech



Současný stav a predikce počtu VIS



Možný budoucí vývoj

- Úprava vyhlášky o VIS – určování nepříliš návodné
- Úprava určujících kritérií pro KII
  - v současné době chybí chemický průmysl, nemocnice apod.
  - do určujících kritériích zahrnout časové hledisko nefunkčnosti ?
- Spolupráce s EU – NIS směrnice a implementace
- Rozšíření metodické pomoci

Dotazy?

Národní bezpečnostní úřad

Děkuji za pozornost

Mgr. Václav Borovička
e-mail: v.borovicka@nbu.cz
www.govcert.cz