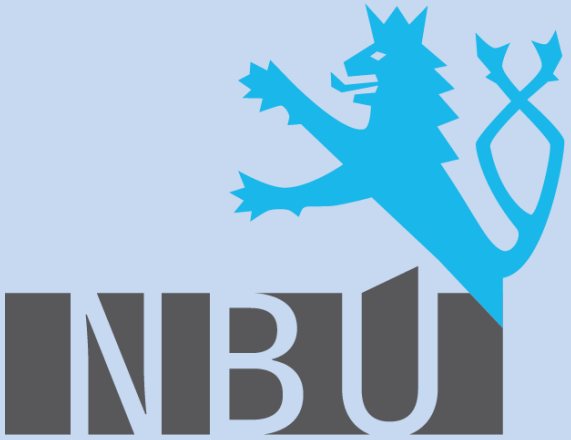

Zákon o kybernetické bezpečnosti a související předpisy

PSP ČR, listopad 2014

SEMINÁŘ
Zákon o kybernetické bezpečnosti a
řízení bezpečnosti informačních systémů
ve veřejné správě a ve zdravotnictví

Václav Borovička
NBÚ / NCKB

Důvody právní úpravy

- 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

GOVCERT.CZ

nckb

Kybernetická bezpečnost v současnosti

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

- Nutnost zajistit koordinovaný postup zajištění kybernetické bezpečnosti u důležitých systémů pro stát

  → Nezbytnost regulace zákonem

GOVCERT.CZ

nckb

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 (národní CERT a vládní CERT)

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

Hlavní principy ZKB

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

Kybernetické předpisy

1) zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů („**ZKB**“)
2) vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) („**VKB**“)
3) vyhláška, kterou se stanoví významné informační systémy a jejich určující kritéria („**VVIS**“)
4) nařízení vlády ze dne 22. prosince 2010 č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury („**NKI**“) (novela)

Zákon o kybernetické bezpečnosti

GOVCERT.CZ

nckb

Povinné osoby (§3)

- Subjekty KII (veřejnoprávní i soukromoprávní subjekty)
  - Správce komunikačního systému KII (§3 písm. d))
  - Správce informačního systému KII (§3 písm. c))
- Správci VIS (pouze orgány veřejné moci) (§3 písm. e))
- Orgán nebo osoba zajišťující významnou síť (§3 písm. b))
- Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací (§3 písm. a))

Povinné osoby (§3)

Kritická informační infrastruktura (KII)

Kritickou informační infrastrukturou se rozumí prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti.

- KII se týká veřejnoprávních i soukromoprávních subjektů
- Určovány pomocí novelizovaného nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
- KII např. systémy, které ovlivňují fungování již určeného prvku kritické infrastruktury dle zák. č. 240/2000 Sb., krizový zákon
- Vyhláška v současné době vytvářena

Povinné osoby (§3)

Významný informační systém (VIS)

Významným informačním systémem informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

- Stanoveny vyhláškou, kterou se stanoví významné informační systémy a jejich určující kritéria
- Správcem VIS může být pouze orgán veřejné moci
- Dle současného návrhu obce nebudou správci VIS
- Stanovení základních VIS a určujících kritérií VIS
- Vyjma systémů uvedených v příloze č. 1, VIS mohou být pouze ty systémy, které určí jeho správce (!)

Jaké jsou jejich povinnosti?

- Nahlášení kontaktních údajů
  - Všechny povinné osoby
- Hlášení kybernetických bezpečnostních incidentů
  - KII, VIS, významné sítě
- Zavést bezpečnostní opatření (standardizace)
  - KII a VIS
- Činit opatření vydané NBÚ
  - KII a VIS
  - Významné sítě a poskytovatelé služby el. komunikací pouze za stavu kybernetického nebezpečí, pouze reaktivní opatření (viz dále)

Hlavní pilíře ZKB

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

GOVCERT.CZ

nckb

Systém zajištění kybernetické bezpečnosti

Bezpečnostní opatření (§ 4 a § 5)

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.

Systém zajištění kybernetické bezpečnosti

Hlášení kybernetického bezpečnostního incidentu (§ 8)

Důvod povinnosti poskytnout kontaktní údaje dle § 16

Hlášení

- KII a VIS hlásí vládnímu CERT
- Soukromoprávní osoby hlásí národnímu CERT

GOVCERT.CZ

nckb

Systém zajištění kybernetické bezpečnosti

Opatření (§ 11)

Opatřeními se rozumí úkony, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu.

Druhy opatření:

- varování,
- reaktivní opatření,
- ochranné opatření.

Vyhláška o kybernetické bezpečnosti

- Vyhláška určuje:
  - základní požadavky na obsah a strukturu bezpečnostní dokumentace,
  - obsah bezpečnostních opatření a rozsah jejich zavedení,
  - typy a kategorie kybernetických bezpečnostních incidentů,
  - náležitosti a způsob hlášení kybernetického bezpečnostního incidentu
  - náležitosti oznámení o provedení reaktivního opatření a jeho výsledku a vzor oznamování kontaktních údajů a jeho formu

→ Standardizace zabezpečení systémů a komunikace s CERTy
→ z velké části vychází z již používaných standardů řízení bezpečnosti informací a řízení rizik (ISO 27000 apod.)

Stav kybernetického nebezpečí

§ 21 ZKB

- 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).

Systém zajištění kybernetické bezpečnosti

Dohledová pracoviště (§ 17 až § 20)

Národní CERT – osoba soukromého práva – právnická osoba

Vládní CERT – provozuje NBÚ

GOVCERT.CZ

nckb

Systém zajištění kybernetické bezpečnosti

Národní CERT

- je k výkonu své činnosti oprávněn na základě veřejnoprávní smlouvy uzavírané s Úřadem,
- je vybrán Úřadem v řízení o výběru žádosti podle správního řádu.

Národní CERT je pracoviště, které zajišťuje sdílení informací na národní i mezinárodní úrovni v oblasti kybernetické bezpečnosti, a to zejména pro osoby soukromého práva.

GOVCERT.CZ

nckb

Systém zajištění kybernetické bezpečnosti

Vládní CERT

Pracoviště provozované NBÚ jako součást NCKB,

- Přijímá oznámení kontaktních údajů od povinných osob uvedených v § 3 písm. c) až e),
- přijímá hlášení o kybernetických bezpečnostních incidentech od povinných osob uvedených v § 3 písm. c) až e),
- vyhodnocuje údaje o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech z kritické informační infrastruktury, z významných informačních systémů, a dalších informačních systémů veřejné správy,
- přijímá údaje o kybernetických bezpečnostních incidentech od provozovatele národního CERT a tyto údaje vyhodnocuje,

GOVCERT.CZ

nckb

Kontrola a další činnost v oblasti KB

§22, § 23 a § 24 ZKB

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.

Vedle toho také NBÚ v oblasti kybernetické bezpečnosti zajišťuje také:

- výzkum a vývoj
- prevenci, vzdělávání
- metodickou podporu

GOVCERT.CZ

nckb

Sankce v oblasti KB (výběr)

!! 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.

Přechodné období

Oznámení kontaktních údajů – **do 30 dnů od**:

- určení (KII)
- dne naplnění určujících kritérií (VIS)
- dne nabytí účinnosti ZKB (významné sítě, poskytovatelé služeb el. komunikací)

Zavedení bezpečnostních opatření a

detekovat a hlásit incidenty – **do 1 roku od**:

- určení (KII)
- dne naplnění určujících kritérií (VIS)
- dne nabytí účinnosti ZKB (významné sítě, poskytovatelé služeb el. komunikací

Kybernetické předpisy

1) zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů
2) vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
3) vyhláška, kterou se stanoví významné informační systémy a jejich určující kritéria
4) novela nařízení vlády ze dne 22. prosince 2010 č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Účinnost k 1. lednu 2015

Děkuji za pozornost

http://www.govcert.cz/

GOVCERT.CZ

nckb