Spisová služba a Zákon o kybernetické bezpečnosti (181/2014 Sb.)

Adam Kučínský

Národní bezpečnostní úřad

Národní centrum kybernetické bezpečnosti

DISCLAIMER

Prezentace vzhledem ke svému rozsahu nepostihuje kompletní šíři požadavků vyplývajících ze zákona o kybernetické bezpečnosti, ale pouze vybrané oblasti.

Povinné osoby podle zákona o kybernetické bezpečnosti (ZKB)

- §3 ZKB

a) poskytovatelé služeb elektronických komunikací, a subjekt 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

KII a VIS – rozdíl

- Kritická informační infrastruktura (KII)
  - Definována zákonem o KB a zákonem o krizovém řízení
  - Narušení takového systému by mohlo mít závažný dopad na fungování státu, život a zdraví obyvatel, ekonomiku nebo bezpečnost
  - KII musí plnit 100 % požadavků vyhlášky č. 316/2014 Sb.
- Významný informační systém (VIS)
  - Definovány pouze zákonem o KB
  - Narušení takového systému by mohlo mít dopad na výkon působnosti orgánu veřejné moci
  - VIS musí plnit cca 60 % požadavků vyhlášky č. 316/2014 Sb.

Kritická informační infrastruktura

- IS nebo KS naplňující **průřezová** a **odvětvová kritéria** v oblasti kybernetické bezpečnosti
  - stejně jako KI se týká veřejnoprávních i soukromoprávních subjektů
  - určování provádí NBÚ (§22, odst. 2 písm. m) a n) ZKB)
- Pro určování KII jsou důležité:
  - Zákon č. 181/2014 Sb., o kybernetické bezpečnosti **>>** definuje KII
  - Zákon č. 240/2000 Sb., krizový zákon >> stanoví proces určení KII
  - Nařízení vlády č. 432/2010 Sb. >> stanoví kritéria pro KII

Kritická informační infrastruktura – kritéria I.

- § 2 písmeno g) krizového zákona
  - narušení funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu
- Průřezová kritéria - § 1 nařízení vlády č. 432/2010 Sb.
  - oběti s mezní hodnotou více než **250 mrtvých** nebo více než **2500 osob s následnou hospitalizací** po dobu delší než 24 hodin, **NEBO**
  - ekonomického dopadu s mezní hodnotou hospodářské **ztráty státu vyšší než 0,5 % hrubého domácího produktu**, **NEBO**
  - dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování **nezbytných služeb** nebo jiného **závažného zásahu do každodenního života** postihujícího **více než 125000 osob**.
    - Vždy je hodnoceno narušení bezpečnosti informací IS/KS*

*Při posuzování naplnění kritérií je uvažováno narušení dostupnosti/důvěrnosti/integrity

Kritická informační infrastruktura - kritéria II.

- Odvětvová kritéria – příloha nařízení vlády č. 432/2010 Sb.
  - a) IS, který významně nebo zcela ovlivňuje činnost určeného prvku KI, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin **-> týká se již určených prvků KI**
  - b) KS, který významně nebo zcela ovlivňuje činnost určeného prvku KI, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin **-> týká se již určených prvků KI**
  - c) IS spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300 000 osobách **-> týká se orgánu veřejné moci**
  - d) KS zajišťující **připojení nebo propojení prvku kritické infrastruktury**, s kapacitou garantovaného datového přenosu nejméně 1 Gbit/s
  - e) odvětvová kritéria pro určení prvku kritické infrastruktury uvedená v písmenech A. až F. se použijí přiměřeně pro oblast kybernetické bezpečnosti, pokud je ochrana prvku naplňujícího tato kritéria nezbytná pro zajištění kybernetické bezpečnosti.

    -> umožňuje určení KII u subjektů, které nenaplňují kritéria a) – d) ale naplní průřezová kritéria a zároveň kritérium z odvětví VI. Komunikační a informační systémy (viz další slide)

Významné informační systémy obecně

- Definice VIS dle §2 písm. d) ZKB:
  - *„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**“*
- Pouze IS spravovaný **orgánem veřejné moci**
- Kritéria uvedena ve vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích*
- **Obce z VIS vyjmuty**

*VIS musí naplnit alespoň jedno dopadové a zároveň jedno oblastní kritérium

Významné informační systémy – dopadová kritéria I.

a) úplná nebo částečná nefunkčnost IS způsobená narušením bezpečnosti informací by mohla mít negativní vliv na:

1. **fungování orgánu veřejné moci**
2. **poskytování služeb nebo informací orgánem veřejné moci veřejnosti**
3. **hospodaření orgánu veřejné moci nebo hospodaření orgánu veřejné moci, který je správcem významného informačního systému, anebo hospodaření orgánu nebo osoby, která je správcem informačního nebo komunikačního systému kritické informační infrastruktury**
4. **provoz jiného významného informačního systému využívajícího služeb hodnoceného informačního systému, který je nefunkční**

přičemž omezení činnosti takového systému by mohlo mít za následek omezení výkonu působnosti orgánu veřejné moci po dobu delší než 3 pracovní dny, nebo výrazné ohrožení výkonu působnosti orgánu veřejné moci, které lze odvrátit za vynaložení nepřiměřených nákladů na provoz nebo obnovu informačního systému.

§ 4 písm. a) vyhlášky č. 317/2014 Sb.

*Při posuzování naplnění kritérií je uvažováno narušení dostupnosti/důvěrnosti/integrity

Významné informační systémy – dopadová kritéria II.

b) úplná nebo částečná nefunkčnost informačního systému způsobená narušením bezpečnosti informací by mohla způsobit:

1. **ohrožení nebo narušení prvku kritické infrastruktury**
2. **oběti na životech s mezní hodnotou více než 10 mrtvých nebo 100 zraněných osob vyžadujících lékařské ošetření, s případnou hospitalizací s dobou delší než 24 hodin**
3. **finanční nebo materiální ztráty s mezní hodnotou více než 5% stanoveného rozpočtu orgánu veřejné moci**
4. **zásah do osobního života nebo do práv fyzických nebo právnických osob postihující nejméně 50 000 osob**
5. **výrazné ohrožení nebo narušení veřejného zájmu**

přičemž následky podle bodů 1 až 4 nedosáhnou hodnot pro určení prvku kritické infrastruktury podle průřezových kritérií stanovených krizovým zákonem.

§ 4 písm. b) vyhlášky č. 317/2014 Sb.

*Při posuzování naplnění kritérií je uvažováno narušení dostupnosti/důvěrnosti/integrity

Významné informační systémy – oblastní kritéria

Příloha č. 2 k vyhlášce o významných informačních systémech

I. U orgánu veřejné moci

1. vedení správního řízení,
2. databáze obsahující osobní údaje,
3. hospodaření orgánu veřejné moci,
4. výkon spisové služby,
5. státní dozor,
6. kontrolní a inspekční činnost,
7. příprava na krizové situace a jejich řešení,
8. tvorba právních předpisů,
9. elektronická pošta,
10. vedení internetových stránek,
11. mezirezortní spolupráce,
12. mezinárodní spolupráce,
13. zadávání veřejných zakázek,
14. státní statistická služba.

II. U orgánu veřejné moci – kraje v rámci přenesené působnosti

1. databáze obsahující osobní údaje,
2. vedení správního řízení,
3. hospodaření orgánu veřejné moci,
4. elektronická pošta,
5. vedení internetových stránek,
6. příprava na krizové situace a jejich řešení,
7. mezinárodní spolupráce,
8. státní dozor,
9. kontrolní a inspekční činnost,
10. zadávání veřejných zakázek.

VIS – určení

- *„Naplnění určujících kritérií významného informačního systému, který není uveden v příloze č. 1 k této vyhlášce, posuzuje správce informačního systému“** (§ 3 vyhlášky č. 317/2014)
- Zákon výslovně nezmiňuje doklad o posouzení
- Ideálně: interní dokument - schválený statutárním zástupcem
- Doporučení k obsahu:
  - Identifikace organizace
  - Seznam posouzených IS
  - U IS naplňujících kritéria pro VIS – odkaz na naplněná kritéria
  - Identifikace odpovědné osoby za konkrétní VIS, úkoly, zodpovědnost
  - Datum schválení, podpis
  - Případné další informace – odkaz na dokumenty, analýzy, atd.

*Správce - orgán nebo osoba, které určují účel zpracování informací a podmínky provozování IS

KII a VIS – přehled povinností

- Nahlášení kontaktních údajů (§16 ZKB)
  - Do 30 dnů od určení/posouzení
- Hlášení kybernetických bezp. incidentů (§8 ZKB)
  - Do jednoho roku od určení/posouzení
  - Stanoveny typy a kategorie
- Činit opatření vydané NBÚ (§11 ZKB)
  - V případě, je vydáno (varování, reaktivní op., ochranné op.)
- **Zavést bezpečnostní opatření – standardizace**
  - **§4 a 5 ZKB > > blíže specifikuje vyhláška č. 316/2014 Sb.**
  - Do jednoho roku od určení/posouzení
- Kontrola spuštěna v závislosti na určení konkrétního VIS

Bezpečnostní opatření - organizační a administrativní opatření

- Zavést systém řízení bezpečnosti informací a v jeho rámci:
  - Řídit rizika
  - Stanovit bezpečnostní role
  - Vytvořit a schválit bezpečnostní politiku
  - Stanovit bezpečnostní požadavky na dodavatele (§ 7 VKB)
  - Řízení aktiv (§ 8 VKB)
  - Bezpečnost lidských zdrojů (§ 9 VKB)
  - Řízení přístupu a bezpečné chování uživatelů (§ 11 VKB)
  - Akvizice, vývoj a údržba (§ 12 VKB)
  - Řízení kontinuity činností (§ 14 VKB)

Organizační a administrativní opatření – řízení rizik

- Řízení rizik
  - Stanovit metodiku pro identifikaci a hodnocení aktiv a rizik
  - Identifikovat a hodnotit důležitost primárních aktiv
  - Identifikovat rizika, při kterých zohlední hrozby a zranitelnosti
  - Zpracovat prohlášení o aplikovatelnosti (přehled vybraných a zavedených bezpečnostních opatření)
  - Zpracovat plán zvládání rizik (cíle a přínosy opatření, termíny,…)
  - Zohlednit případná reaktivní a ochranná opatření vydaná NBÚ
- Bezpečnostní politika
  - oblasti ve kterých má být stanovena uvádí VKB v § 5 odst. 2

Organizační a administrativní opatření – bezpečnostní role

- Výbor pro řízení kybernetické bezpečnosti – KII i VIS povinně
  - Stanoví práva a povinnosti a určí bezpečnostní role
- Garant aktiva – povinně KII i VIS povinně
  - Osoba pověřená k zajištění rozvoje, použití a bezpečnosti aktiva
- Další bezpečnostní role – správce VIS je určí přiměřeně:
  - manažer kybernetické bezpečnosti
    - Vyškolení pro tuto činnost + praxe 3 roky v oblasti řízení bezpečnosti informací
  - architekt kybernetické bezpečnosti,
    - Vyškolení pro tuto činnost + praxe 3 roky v oblasti navrhování bezp. architektury
  - auditor kybernetické bezpečnosti – neslučitelné s ostatními rolemi
    - Vyškolení pro tuto činnost + praxe 3 roky v oblasti auditů kybernetické bezpečnosti

Prokázání certifikace (§ 29 VKB)

- VIS je zcela zahrnut do rozsahu systému řízení bezpečnosti informací
- Rozsah byl certifikován podle normy ISO 27001 akreditovaným certifikačním orgánem
- Správce VIS vede dokumenty obsahující
  - popis rozsahu systému řízení bezpečnosti informací,
  - prohlášení politiky a cílů systému řízení bezpečnosti informací
  - popis použité metody hodnocení rizik a zprávu o hodnocení rizik,
  - prohlášení o aplikovatelnosti,
  - certifikát systému řízení bezpečnosti informací splňující požadavky normy,
  - záznam o přezkoumání systému řízení bezpečnosti informací včetně souvisejících vstupů a výstupů přezkoumání
  - zprávu z auditů provedených certifikačním orgánem včetně příslušných záznamů o nápravě zjištěných neshod s příslušnou normou,

Užitečné odkazy a informace

Blokové schéma k zákonu o kybernetické bezpečnosti:
http://www.govcert.cz/cs/kii--vis/kii--vis/

Proces určování kritické informační infrastruktury:
http://www.govcert.cz/cs/kii--vis/kriticka-informacni-infrastruktura/

Proces určování významných informačních systémů:
http://www.govcert.cz/cs/kii--vis/vyznamne-informacni-systemy/

Pomůcka k auditu/kontrole bezpečnostních opatření podle zákona, přehled lhůt pro plnění povinností, povinnosti podle zákona, bezpečnostní role:
http://www.govcert.cz/cs/kii--vis/dalsi-materialy-ke-stazeni/

Národní strategie kybernetické bezpečnosti a akční plán:
http://www.govcert.cz/cs/informacni-servis/strategie-a-akcni-plan/

Výkladový slovník kybernetické bezpečnosti - třetí vydání:
http://www.govcert.cz/cs/informacni-servis/vykladovy-slovnik/

Děkuji za pozornost!

Diskuze a dotazy?

Adam Kučínský

a.kucinsky@nbu.cz

www.nbu.cz
www.govcert.cz