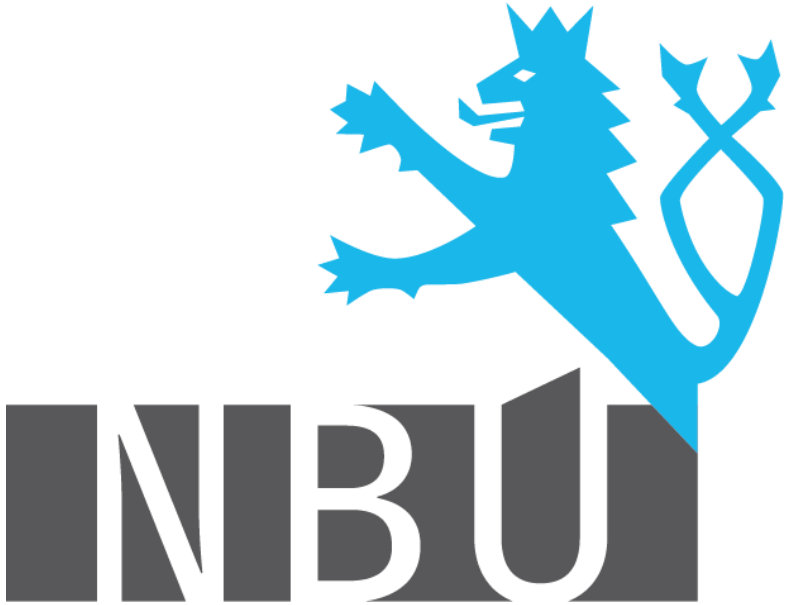
Zkušenosti a výsledky určování KII a VIS



Kritická informační infrastruktura obecně

- IS nebo KS naplňující **průřezová** a **odvětvová kritéria** v oblasti kybernetické bezpečnosti
  - stejně jako KI se týká veřejnoprávních i soukromoprávních subjektů

- 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 proces určování

- Subjekty se stanou KII až po určovacím procesu
  - ZKB na ně dřív může dopadat jen v rámci jiných povinných osob
- NBÚ kontaktuje pravděpodobný subjekt KII
- Subjekt provede ve spolupráci s NBÚ zhodnocení svých IS a KS, zda naplňují kritéria pro určení za KII
  - Předpokládá se úzká spolupráce mezi tímto subjektem a NBÚ
- Pokud IS nebo KS splní kritéria, pak se určí jako KII

Kritická informační infrastruktura proces určování (pokrač.)

- Proces určování rozdílný podle povahy subjektů
  - Postup podle krizového zákona
- Státní prvky:
  - Seznam navrhovaných prvků NBÚ předloží MV
  - Seznam následně projedná Výbor pro civilní a nouzové plánování a Bezpečnostní rada státu
  - Poté seznam předložen vládě ČR ke schválení
- Soukromé prvky:
  - NBÚ určí prvky KII opatřením obecné povahy

KII a VIS – rozdíl

- **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.
- **VIS**
  - Definovány pouze zákonem o KB
  - Narušení takového systému bude mít dopad na výkon působnosti orgánu veřejné moci
  - VIS musí plnit cca 60 % požadavků vyhlášky č. 316/2014 Sb.

Kritická informační infrastruktura – veřejná správa

- Určování prvků KII rozděleno do tří základních vln
- 1. vlna: Ministerstva a ústřední správní úřady
- Ministerstva a ÚSÚ určeny jako KI
  - Jako KI určeno cca 80 státních prvků
  - Pravděpodobné naplnění kritérií pro KII
  - Ne všichni určení jako KI naplnili kritéria pro KII
  - Jednání využita i pro konzultace naplnění kritérií pro VIS

Kritická informační infrastruktura – veřejná správa (pokrač.)

- 1. vlna: Ministerstva a ústřední správní úřady
  - 25. května 2015 vládou schváleno 45 prvků KII, které spravují organizační složky státu
- Zahájena 2. vlna: zbývající část státní správy
  - 15. září 2015 předloženy ke schválení další prvky KII u organizačních složek státu
  - Stále probíhá
- Příprava na určení dalších prvků KII
  - Probíhají další jednání

Kritická informační infrastruktura – soukromý sektor

- 3. vlna: soukromý sektor
  - Jednání se společnostmi poskytujícími klíčové služby
    - Odvětví: energetika, bankovnictví, telekomunikace,…
  - V srpnu 2015 vydáno 10 návrhů opatření obecné povahy určujících 17 prvků KII u 10 soukromoprávních subjektů
  - Datum nabytí účinnosti těchto OOP - 9. října 2015
- Příprava na určení dalších prvků:
  - Aktuálně připraveno k určení dalších 17 prvků KII u 6 správců
  - Dokončována jednání s dalšími 8 správci KII
  - Kontaktováni další potencionální správci KII

Kritická informační infrastruktura – Shrnutí

- Od účinnosti zákona dosud proběhlo ohledně určování KII přes 100 jednání se soukromými i státními subjekty
- KII veřejný sektor
  - 45 prvků určeno
  - další prvky v procesu určení – schválení cca do měsíce
- KII soukromý sektor
  - 17 prvků u 10 správců určeno (OOP vydáno)
  - 17 prvků u 6 správců připraveno k určení (OOP připravováno)
  - Dokončována jednání s dalšími 8 potencionálními správci KII
  - Kontaktováni další potencionální správci KII

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
- Identifikace konkrétních VIS závislá na vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
- Obce z VIS vyjmuty

Významné informační systémy – současný stav

- Současný stav VIS:
  - V příloze č. 1 vyhlášky o VIS uvedeno 92 systémů
  - Do KII přeřazeno 22 systémů
  - Nově určeno 19 systémů jako VIS
  - Nyní NBÚ eviduje 89 VIS (nejde o konečný počet)
- Předpoklad je, že by kritéria pro VIS mohly naplnit i některé univerzity
- Finalizuje se určení VIS ve správě krajů
- Seznam ve vyhlášce bude aktualizován

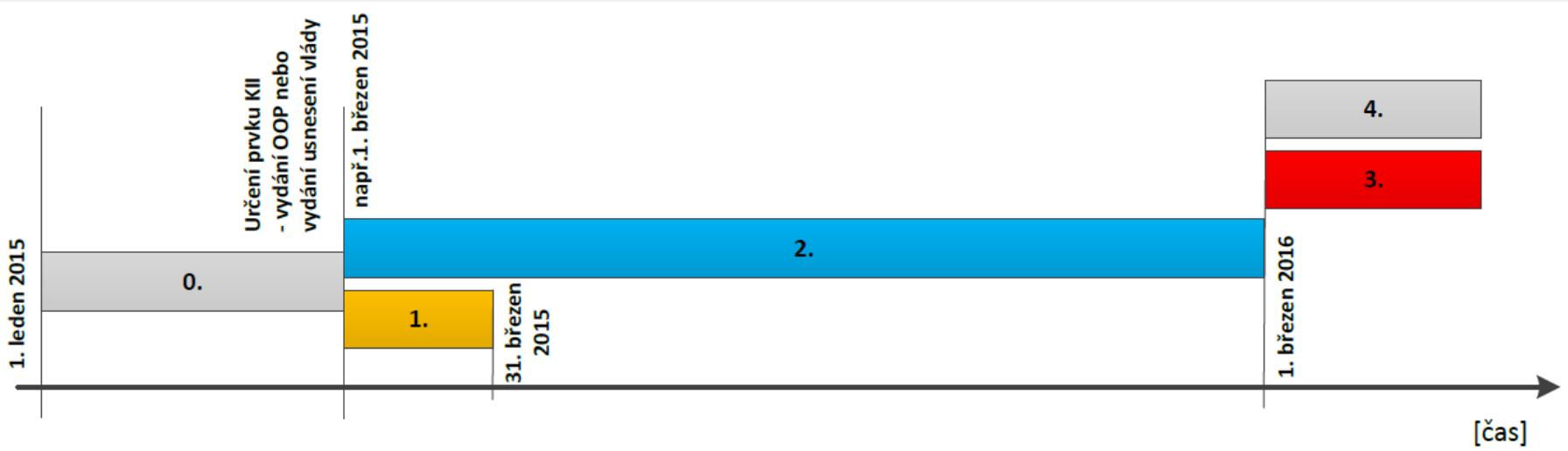
Významné informační systémy – Kraje

- Prozatím nebyl identifikován IS/KS jehož správcem je kraj a splňuje kritéria pro KII – kraje budou mít spíše VIS
- Kraje mají stejné kompetence a působnost – využívají podobné informační systémy - systémy naplňují podobná kritéria
  - Koordinovaný postup při posuzování a určování VIS
- Spolupráce na úrovni Asociace krajů – komise informatiky
- Proběhlo několik jednání se zástupci krajů
- NBÚ/NCKB poskytlo metodické materiály a podporu
- Na tomto základě vytipovány systémy, které splňují kritéria pro VIS (systémy vybírány z ISoISVS)
- Navrženy IS k projednání na úrovni komise AKČR s návrhem, aby byly určeny jako VIS

KII a VIS – přehled povinností

- Nahlášení kontaktních údajů (§16 ZKB)
  - Do 30 dnů od určení
- Hlášení kybernetických bezpečnostních incidentů (§8 ZKB)
  - Do jednoho roku od určení
- Zavést bezpečnostní opatření (standardizace) (§4 ZKB)
  - Do jednoho roku od určení
- Činit opatření vydané NBÚ (§11 ZKB)
  - V případě, že se tak stane

KII – lhůty pro plnění povinností



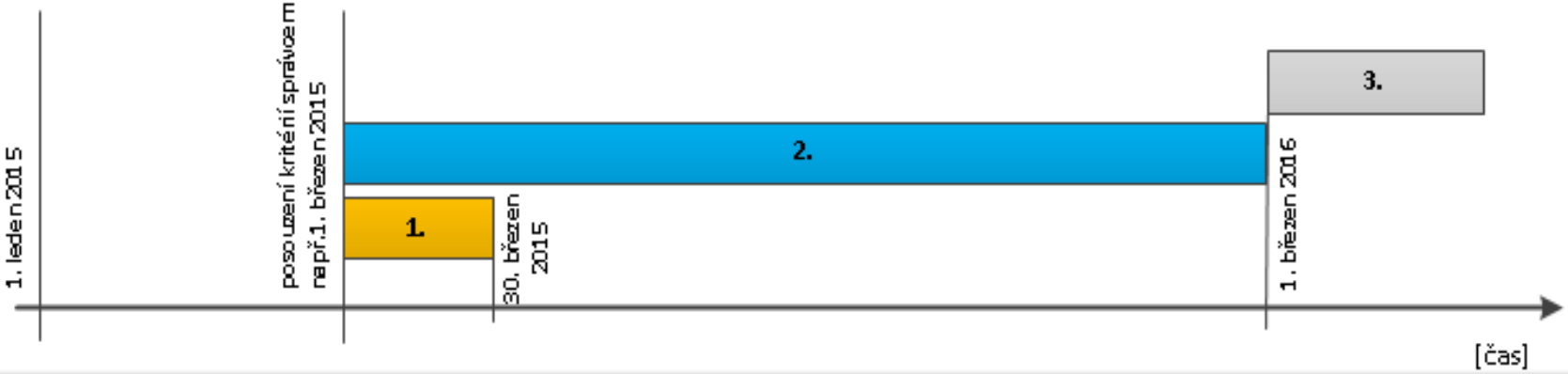
0. Proces určování prvků KII (oboustranné jednání) – viz. schéma na www.govcert.cz
1. Lhůta pro nahlášení kontaktních údajů
2. Přechodná lhůta (implementace bezpečnostních opatření podle vyhlášky č. 316/2014 Sb.)
3. Plnění povinností podle ZKB (hlášení kybernetických bezpečnostních incidentů, provádění bezp. opatření)
4. Možnost státního dozoru (auditu) ze strany NBÚ – kontrola souladu se zákonem o kybernetické bezpečnosti

VIS – lhůty pro plnění povinností

Významné informační systémy uvedené v příloze č. 1 vyhlášky č. 317/2014 Sb.

1. Lhůta 30 dní pro nahlášení kontaktních údajů
2. Přechodné období
3. Možnost auditu/kontroly

Významné informační systémy, které nejsou uvedeny v příloze č. 1 vyhlášky č. 317/2014 Sb.



Sankce

- Správce KII a VIS se dopustí správního deliktu pokud
  - 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.

Kontrola plnění povinností

- Kontrolu plnění povinností vykonává NBÚ
- Kontrola bude spuštěna v závislosti na určení konkrétního prvku
  - Od 1. 1. 2016 – kontroly u správců VIS uvedených ve vyhlášce
  - Ostatní VIS - rok od určení
  - Od 25. 5. 2016 – kontroly u správců 45 prvků KII určených v první vlně
  - Prvky KII v soukromém sektoru – rok od právní moci OOP

Kontrola plnění povinností (pokrač.)

- Co bude kontrolováno?
  - Při výkonu kontroly Úřad zjišťuje, jak povinné osoby plní povinnosti stanovené ZKB, prováděcími právními předpisy, rozhodnutími a opatřeními obecné povahy vydanými Úřadem
  - Nebude stačit pouhé předložení dokumentace
- Metodický dozor
  - Cílem zákona není represe – jde o zajištění požadované úrovně zabezpečení důležitých systémů, nikoli o ukládání sankcí
  - Metodický dozor může provést kontrolu bez uložení případné sankce

KII a VIS – problematické oblasti určování

- **KII**
  - Bílá místa krizového zákona
  - Zdravotnictví – kritérium pro KI „2 500 lůžek“ – žádná nemocnice není kritická
  - V odvětvových kritériích pro KI chybí chemický průmysl
- **VIS**
  - Vyloučena velká města, i když spravují důležité systémy
  - Někteří správci důležitých informačních systémů nejsou orgánem veřejné moci
- **Určování do značné míry ovlivňuje přístup subjektů**

KII a VIS – problematické oblasti

- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
  - Transparentnost na úkor bezpečnosti?
  - Prolomení:
    - § 9 - ochrana obchodního tajemství
    - § 11 , odst. 4 písm. f) - údaje vedené v evidenci incidentů podle zákona o kybernetické bezpečnosti
    - Krizový zákon § 27 „Zvláštní skutečnosti“ – údaje z oblasti krizového řízení - případné zneužití by mohlo vést k znemožnění nebo omezení činnosti orgánu krizového řízení, ohrožení života, zdraví, majetku, životního prostředí nebo podnikatelského zájmu
      - Problém s použitím v praxi

KII a VIS – problematické oblasti (pokrač.)

- Zákon o veřejných zakázkách:
  - Problém vyloučení rizikových dodavatelů
  - Je třeba řídit rizika v průběhu celé zakázky
  - Co nejpřesněji vydefinovat požadavky v zadání
  - SLA (service-level agreement)

KII a VIS – problematické oblasti (pokrač.)

- Subjekty namítají, že systémům nehrozí výpadek (narušení dostupnosti), neboť jsou redundantní
  - Pokud se však jedná o redundanci v kyberprostoru (např. zálohování, záložní servery apod.) jedná se o již zavedené opatření podle standardizační vyhlášky
  - Nejedná se o skutečnost, která by vylučovala či snižovala kritičnost takových systémů
- Při hodnocení dopadu někdy bývá řešena pouze **dostupnost** - je třeba hodnotit i **důvěrnost** a **integritu**

KII a VIS – některé podněty pro budoucí vývoj

- Úprava vyhlášky o VIS – určování nepříliš návodné
- Úprava určujících kritérií pro KII
  - v současné době chybí chemický průmysl, nemocnice apod.
- Spolupráce s EU – NIS směrnice a její implementace
- Rozšíření metodické pomoci
- Navázání ZKB a ZVZ – střet bezpečnostního a ochraně-hospodářského náhledu
- Navázání ZKB a zák. o svobodném přístupu k informacím

Děkuji za pozornost!

www.nbu.cz
www.govcert.cz