Výzva IROP:
„Kybernetická bezpečnost“

Seminář pro veřejnost 11. 11. 2015

Adam Kučínský

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
  - 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 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 (240/2000 Sb.)
- Organizační složky státu:
  - 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
- Ostatní:
  - NBÚ určí prvky KII opatřením obecné povahy (OOP)

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
  - 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

- KII - 3. vlna: soukromý sektor (zahrnuje i státní podniky)
  - Jednání se společnostmi poskytujícími klíčové služby
  - V srpnu 2015 vydáno 10 návrhů OOP určujících 17 prvků KII u 10 soukromoprávních subjektů (účinnost OOP - 9. října 2015)
  - V říjnu 2015 vydáno 5 návrhů OOP určujících 11 prvků KII u 5 soukromoprávních subjektů (běží lhůty pro účinnost OOP)
- Příprava na určení dalších prvků:
  - Aktuálně připraveno k určení dalších 21 prvků KII (OOP budou vydány v listopadu)
  - Dokončována jednání s dalšími 8 pravděpodobnými správci KII

Kritická informační infrastruktura – Shrnutí

- Od účinnosti zákona dosud proběhlo ohledně určování KII přes 120 jednání se soukromými i státními subjekty
- KII veřejný sektor
  - 45 prvků určeno
  - Další prvky v procesu určení (schválení vládou očekáváme v listopadu)
- KII soukromý sektor
  - 17 prvků u 10 správců určeno (OOP účinné)
  - 11 prvků u 5 správců určeno (Návrhy OOP vydány)
  - Dokončována jednání s dalšími 8 potencionálními správci KII
  - Kontaktovány další subjekty

Kritická informační infrastruktura - kritéria

- § 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 (pokrač.)

- 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)

KII - Odvětvová kritéria – oblast KB

A. Technologické prvky pevné sítě elektronických komunikací:

a) centrum řízení a podpory sítě,
b) řídící ústředna,
c) mezinárodní ústředna,
d) transitní ústředna,
e) datové centrum,
f) telekomunikační vedení.

B. Technologické prvky mobilní sítě elektronických komunikací:

a) centrum řízení a podpory sítě,
b) ústředna mobilní sítě,
c) základnová řídící jednotka sítě pokrývající strategickou lokalitu,
d) základnová stanice sítě pokrývající strategickou lokalitu,
e) datové centrum.

C. Technologické prvky sítí pro rozhlasové a televizní vysílání:

a) vysílací zařízení pro šíření televizního nebo rozhlasového signálu určených
pro informaci obyvatelstva za krizových situací vysílacím výkonem nad 1 kW
k zajištění rozhlasového a televizního vysílání veřejnoprávního provozovatele,
b) řídící pracoviště provozu,
c) datové centrum,
d) síť pro rozhlasové a televizní vysílání k zajištění provozu rozhlasového a televizního vysílání veřejnoprávního provozovatele.

D. Technologické prvky pro satelitní komunikaci:

a) hlavní pozemní satelitní přijímací a vysílací stanice,
b) Evropský globální navigační družicový systém,
c) pozemní řídící a komunikační středisko,
d) pozemní propojovací síť.

E. Technologické prvky pro poštovní služby:

a) centrální a regionální výp. středisko, středisko centrálního snímání a úložiště dat,
b) sběrný přepravní uzel,
c) řídící a mezinárodní pošta,
d) poštovní dopravní infrastruktura.

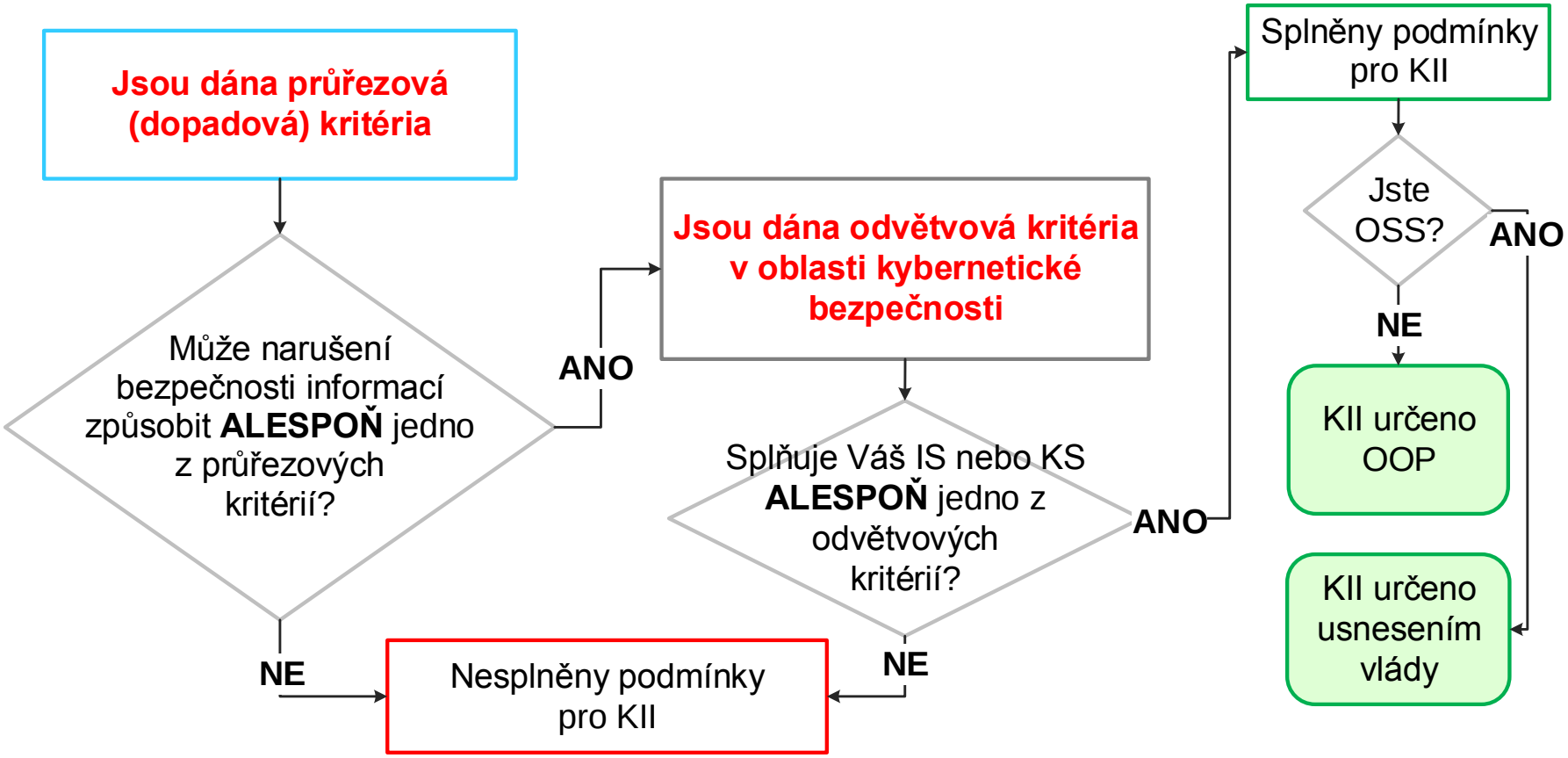
F. Technologické prvky informačních systémů:

a) řídicí centrum,
b) datové centrum,
c) síť elektronických komunikací,
d) technologický prvek zajišťující provoz registru doménových jmen „CZ“ a zabezpečení provozu domény nejvyšší úrovně „CZ“.

G. Oblast kybernetické bezpečnosti

a) Ovlivňuje Váš IS významně nebo zcela činnost určeného prvku KI a zároveň je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období delším jak 8 hodin?
b) Ovlivňuje Váš KS významně nebo zcela činnost určeného prvku KI a zároveň je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období delším jak 8 hodin?
c) Je Váš IS spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300 tis. osobách?
d) Je Váš systém komunikačním systémem, který zajišťuje připojení nebo propojení prvku KI spravovaným orgánem veřejné moci s kapacitou přenosu min. 1 Gbit/s?
e) Odvětvová kritéria pro určení prvku KI uvedená v písm. A. – F., odvětví VI. přílohy nařízení vlády č. 432/2010 Sb., ve znění novely č. 315/2014 Sb., se použijí **přiměřeně** pro oblast KB, pokud je ochrana prvku naplňujícího tato kritéria nezbytná pro zajištění kybernetické bezpečnosti.

Kritická informační infrastruktura – určování - schéma



Ke stažení: http://www.govcert.cz/cs/kii--vis/kriticka-informacni-infrastruktura/

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 určovány další systémy jako VIS (zejména kraje)
  - Nyní NBÚ eviduje cca 100 VIS (nejde o konečný počet)
- Předpoklad je, že by kritéria pro VIS mohly naplnit i některé univerzity
- 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)

Významné informační systémy – dopadová kritéria

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.

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.

Významné informační systémy – oblastní kritéria

Příloha č. 2 k vyhlášce o významných informačních systémech

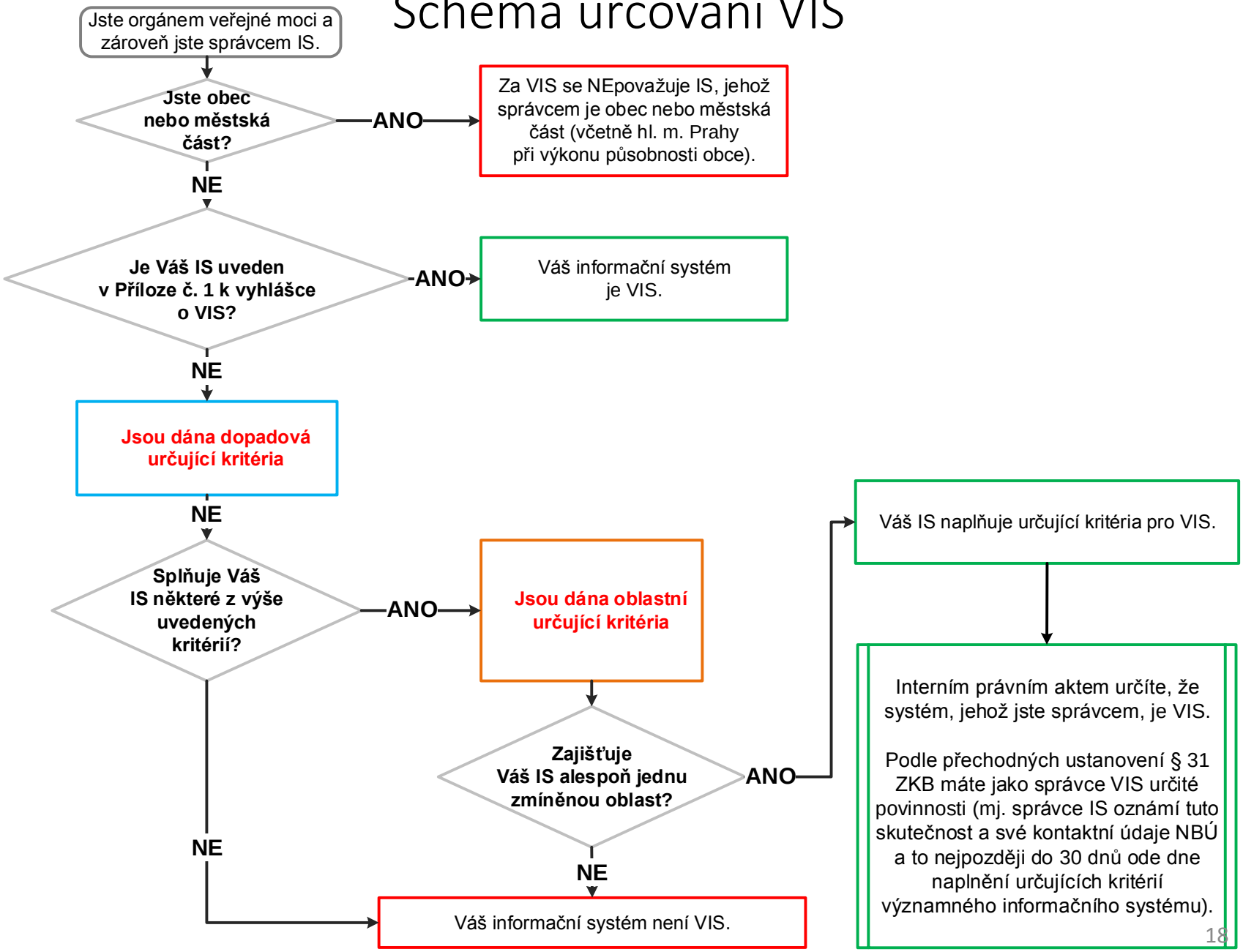
I. U orgánu veřejné moci

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.

Schéma určování VIS



Ke stažení: http://www.govcert.cz/cs/kii--vis/vyznamne-informacni-systemy/

VIS – určení - interní právní akt

- Zákon výslovně nezmiňuje
- Interní dokument
- Schválený a podepsaný statutárním zástupcem
- Doporučení k obsahu:
  - Identifikace organizace
  - Seznam posouzených IS
  - U IS naplňujících kritéria pro VIS – popis naplněných kritérií
  - Identifikace odpovědné osoby za konkrétní VIS
  - Úkoly, které má osoba plnit
  - Datum schválení
  - Podpis
  - Případné doplňující informace – odkaz na dokumenty, analýzy, atd.

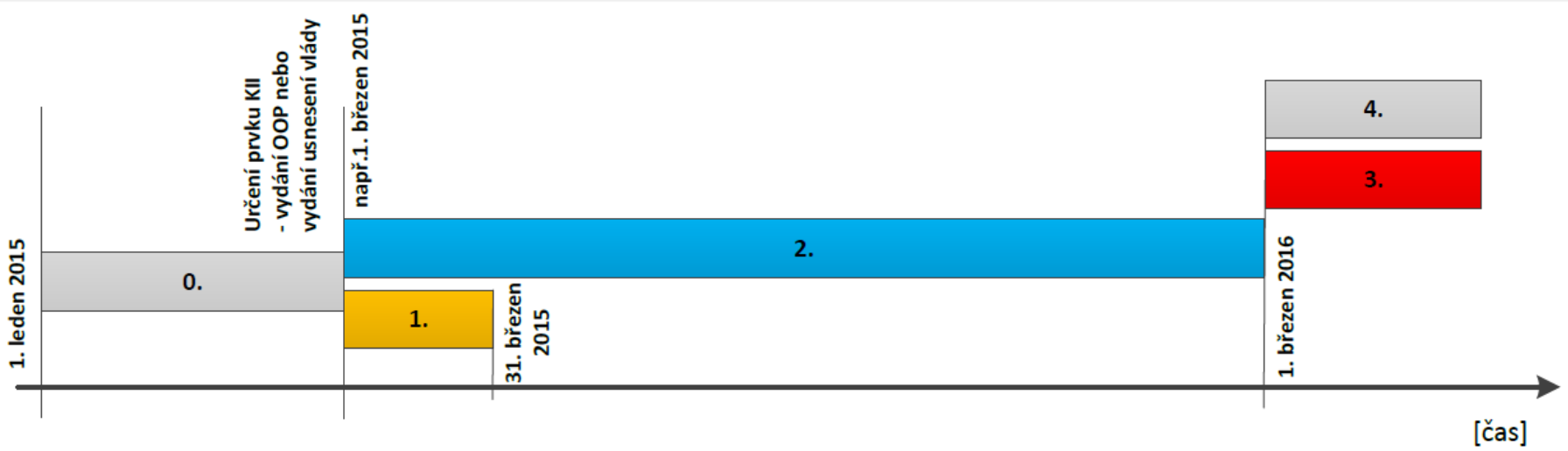
KII a VIS – rozdíl

- **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 by mohlo míz mít dopad na výkon působnosti orgánu veřejné moci
  - VIS musí plnit cca 60 % požadavků vyhlášky č. 316/2014 Sb.

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 a 5 ZKB > > blíže specifiku vyhláška č. 316/2014 Sb.**
  - Do jednoho roku od určení
- Činit opatření vydané NBÚ (§11 ZKB)
  - V případě, že je opatření vydáno

KII – lhůty pro plnění povinností



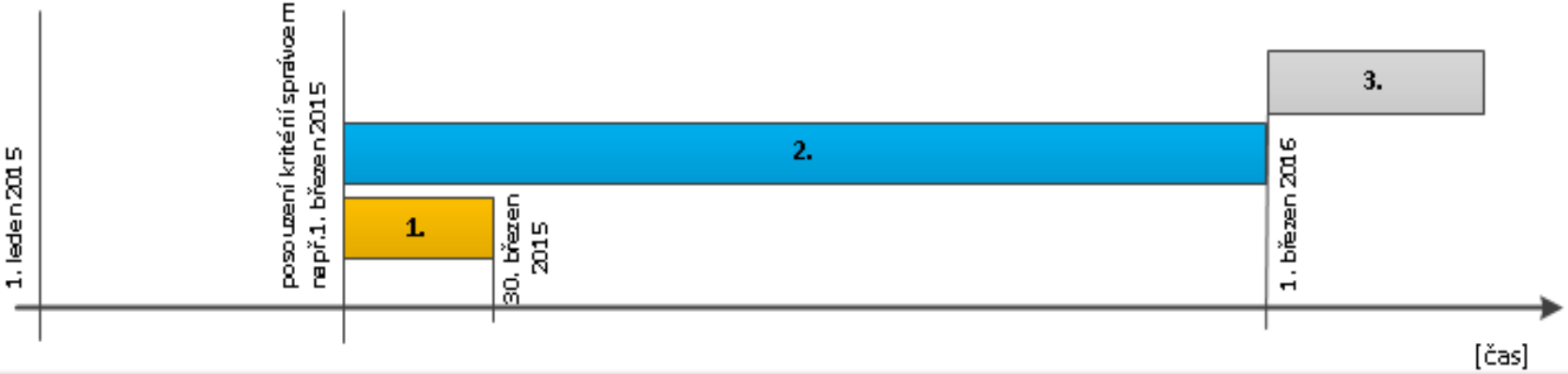
0. Proces určování prvků KII (oboustranné jednání) – viz. schéma na www.govcert.cz
1. Lhůta pro nahlášení kontaktních údajů
2. Přechodná lhůta (implementace bezpečnostních opatření podle vyhlášky č. 316/2014 Sb.)
3. Plnění povinností podle ZKB (hlášení kybernetických bezpečnostních incidentů, provádění 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

- 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)
  - Není možné požadovat ISO 27k po dodavateli

KII a VIS – problematické oblasti (pokrač.)

- Argument, 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

KII a VIS – Podpůrné materiály

- Blokové schéma k zákonu o kybernetické bezpečnosti:
  http://www.govcert.cz/cs/kii--vis/kii--vis/
- Schéma procesu určování kritické informační infrastruktury:
  http://www.govcert.cz/cs/kii--vis/kriticka-informacni-infrastruktura/
- Schéma procesu 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/
- Formuláře pro hlášení kontaktních údajů a incidentů:
  http://www.govcert.cz/cs/kii--vis/formulare/
- 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!

www.nbu.cz
www.govcert.cz