Kritická informační infrastruktura
Významné informační systémy

Adam Kučínský

Národní bezpečnostní úřad

Národní centrum kybernetické bezpečnosti

Disclaimer

Prezentaci a informace v ní obsažené není možné považovat za oficiální stanoviska Národního bezpečnostního úřadu.
Prezentaci není možné šířit bez písemného souhlasu autora.

Obsah přednášky

- Zákon o kybernetické bezpečnosti - na koho dopadá
- Hlavní povinnosti ze zákona
- Současný stav implementace ZKB a některé otázky s tím spojené
- Krizové řízení a kybernetická bezpečnost

Úvod do legislativy kybernetické bezpečnosti

- Právní předpisy směřují 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

Vybraná legislativa související se zajištěním kybernetické bezpečnosti – širší pojetí

Zákon č. 181/2014 Sb., **o kybernetické bezpečnosti**

Zákon č. 127/2005 Sb., **o elektronických komunikacích**

Zákon č. 412/2005 Sb., **o ochraně utajovaných informací**

Zákon č. 227/2000 Sb., **o elektronickém podpisu**

Zákon č. 365/2000 Sb., **o informačních systémech veřejné správy**

Zákon č. 300/2008 Sb., **o elektronických úkonech a autorizované konverzi dokumentů**

Zákon č. 40/2009 Sb., **trestní zákoník**

Zákon č. 89/2012 Sb., **občanský zákoník**

Zákon č. 90/2012 Sb., **o obchodních korporacích**

…a další…

Kybernetické předpisy – užší pojetí

Legislativa kybernetické bezpečnosti

- Hlavní
  - Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů (dále také „**ZKB**“)
  - 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., o významných informačních systémech a jejich určujících kritériích (dále také „**VVIS**“)
  - Novelizované nařízení vlády ze dne 22. prosince 2010 č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (dále také „**NKI**“)

Kybernetické předpisy – užší pojetí

Legislativa kybernetické bezpečnosti

- 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**“)

Specifické důvody přijetí ZKB

- Kybernetická bezpečnost řešena prostřednictvím soukromých / akademických subjektů, bez 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 zejména u důležitých systémů pro stát
  - Nezbytnost regulace zákonem

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)

Povinné osoby podle 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

Poskytovatelé služeb el. komunikací, subjekty zajišťující síť el. komunikací - §3 písm. a) ZKB

- zákon č. 127/2005 Sb., o elektronických komunikacích
  - §2 písm. f) ZEK – *„zajišťováním sítě elektronických komunikací zřízení této sítě, její provozování, dohled nad ní nebo její zpřístupnění“*
  - §2 písm. n) ZEK – *„službou elektronických komunikací služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací“* --> ISP
- určování neprobíhá – osoby definovány zák. o el. komunikacích
- sféra Národního CERTu

Orgán nebo osoba zajišťující významnou síť §3 písm. b) ZKB

- významná síť (§2 písm. g ZKB)
  - „síť elektronických komunikací zajišťující **přímé zahraniční propojení** do veřejných komunikačních sítí nebo zajišťující **přímé připojení ke kritické informační infrastruktuře**“
- určování neprobíhá – povinný subjekt určen přímo ZKB
- sféra Národního CERTu

Správce KS nebo IS KII
§3 písm. c) a d) ZKB

- Systémy důležité pro chod státu
- Sféra Vládního CERTu
- 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

- Pojmy:
  - Kritická infrastruktura/prvek kritické infrastruktury
  - Kritická informační infrastruktura
  - Průřezová a odvětvová kritéria
  - Princip „prvek v prvku“

Správce KS nebo IS KII
§3 písm. c) a d) ZKB

Určení

- Subjekty se stanou KII až po určovacím procesu – ZKB na ně dřív může dopadat jen v rámci jiných povinných osob (např. jako na správce významných sítí, významného informačního systému apod.)
- Pokud IS nebo KS splní kritéria, pak je určen jako KII
  - usnesením vlády v případě organizačních složek státu
  - OOP vydaným NBÚ v případě ostatních subjektů
- Po vydání usnesení vlády nebo OOP běží přechodná doba k zavedení povinností dle ZKB

Kritická informační infrastruktura
určování - 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 hodnocen dopad narušení bezpečnosti informací IS/KS*

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

Kritická informační infrastruktura
určování - kritéria

- 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:

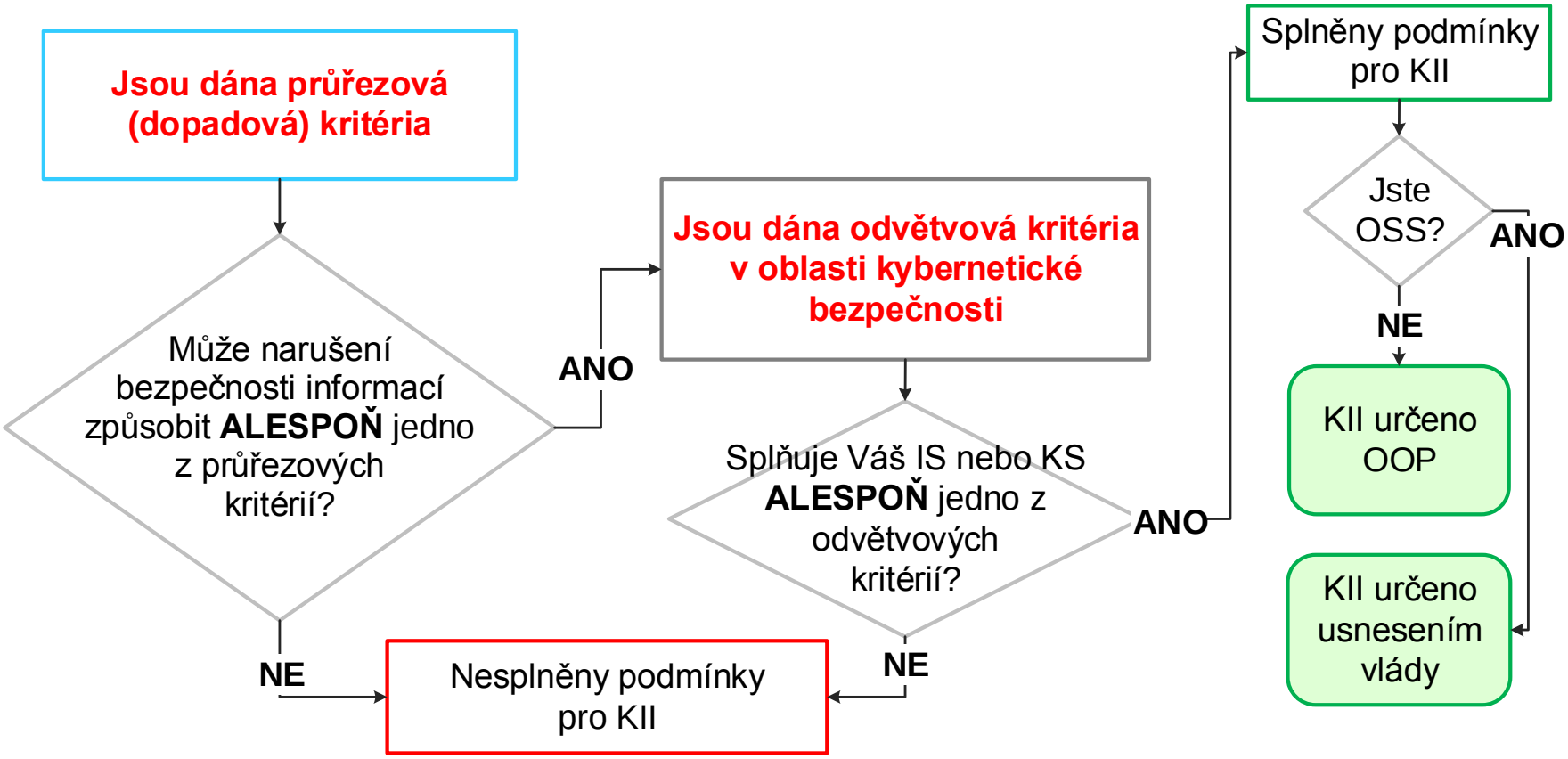
a) řídicí centrum,
b) datové centrum,
c) síť elektronických komunikací,
d) technologický prvek zajišťující provoz registru doménových jmen „CZ“ a zabezpečení provozu domény nejvyšší úrovně „CZ“.

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

Proces určování



Kritická informační infrastruktura
Průběh určování

- NBÚ kontaktuje pravděpodobný subjekt KII
- Subjekt provede ve spolupráci s NBÚ zhodnocení svých IS a KS, zda naplňují kritéria pro určení jako KII
- Pokud IS nebo KS splní kritéria, pak se určí jako KII
  - Usnesením vlády v případě organizačních složek státu
  - OOP vydaným NBÚ v případě ostatních subjektů
- Po vydání usnesení vlády nebo OOP běží přechodná doba k zavedení povinností dle ZKB

Příklad
Určení prvku KII

- Prověřována společnost, zajišťující chod produktovodu
- Produktovod je řízen SCADA systémem (Supervisory Control And Data Acquisition), bez něhož by byl nefunkční
- Produktovod je již určen prvkem kritické infrastruktury
- Krok I: Obecný dopad narušení bezpečnosti informací v tomto systému je následující:
  - V případě neoprávněného uzavření armatury může dojít k prasknutí produktovodu
  - Mohlo by být způsobeno omezení či zastavení dodávek produktů

Příklad - pokračování
Určení prvku KII

- Krok II: Po analýze obecných dopadů následuje prověření naplnění průřezových kritérií:
  - Je naplněno průřezové kritérium dle § 1, písm. c) „dopad na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob
- Krok III: Po prověření naplnění průřezových kritérií následuje prověření naplnění odvětvových kritérií:
  - Je naplněno kritérium podle písm. a) přílohy NV č. 432/2010 Sb., odvětví VI. Komunikační a informační systémy, G. Oblast kybernetické bezpečnosti: *„informační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin“*
- Krok IV: Tímto jsou naplněna potřebná kritéria a SCADA systém bude určen kritickou informační infrastrukturou opatřením obecné povahy vydaným Národním bezpečnostním úřadem

§3 písm. e) ZKB
Správce VIS

Významné informační systémy

- Definice 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 (mimo obce)
- Není KII
- Identifikace konkrétních VIS závislá na vyhlášce o významných informačních systémech a jejich určujících kritériích
- Oproti KII je mířeno směrem k zajištění působnosti OVM

§3 písm. e) ZKB
Správce VIS

Identifikace VIS

VIS přímo stanovené v příloze č. 1 VVIS

- zjevné VIS, u kterých není pochyb o jejich významnosti
- nyní 35 subjektů, 92 systémů

VIS posouzené správcem na základě určujících kritérií

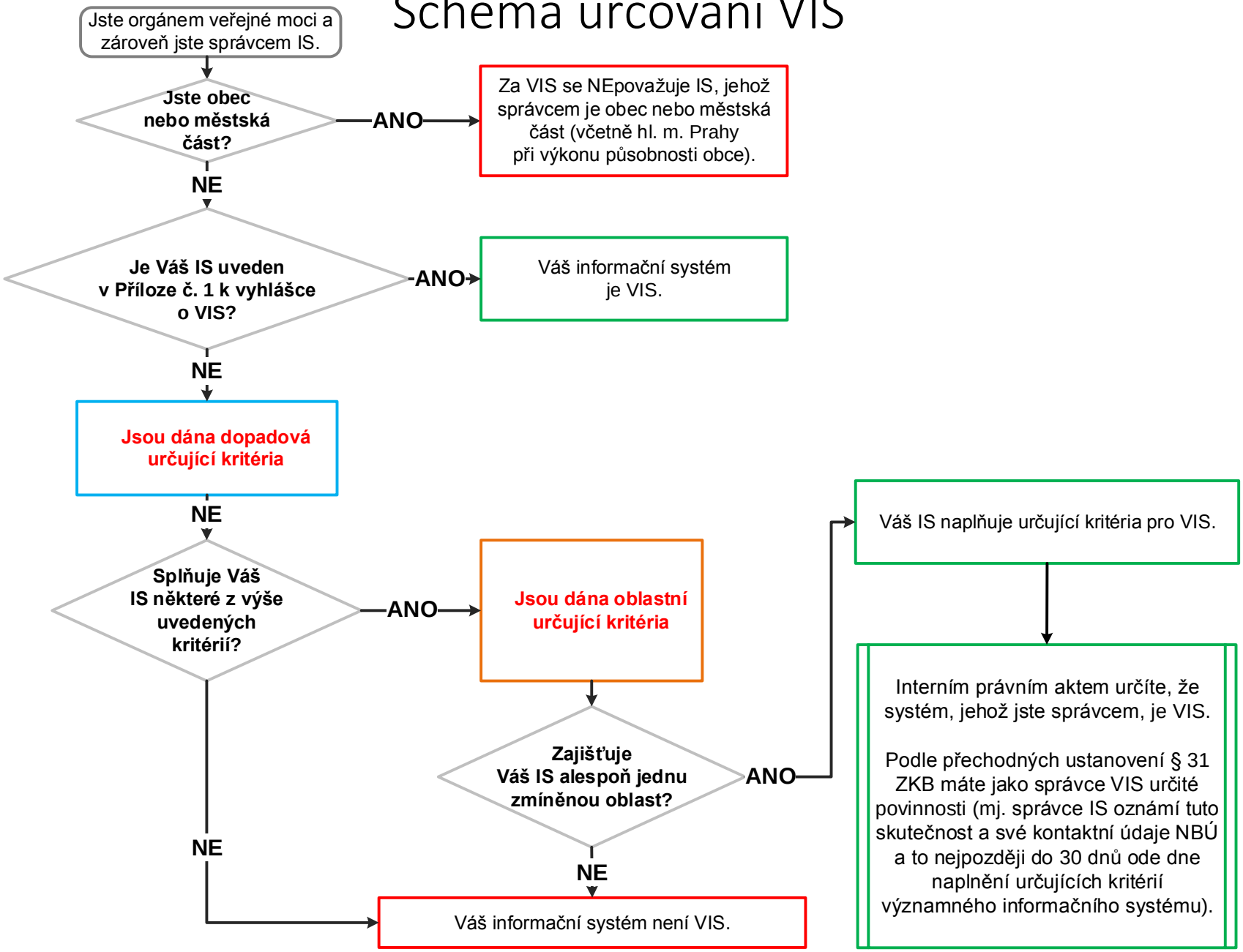
- ostatní IS splňující určující kritéria
- určující kritéria **dopadová** a **oblastní**
- splnění kritérií posuzuje sám správce hodnoceného IS
- IS je určen jako VIS interním aktem
- správce nahlásí NBÚ tuto skutečnost společně s kontaktními údaji

➢ Přechodné období pro plnění povinností obdobně jako u KII

Významné informační systémy (VIS) – Současný stav posuzování

- Naplnění kritérií posuzuje správce systému – kritéria dopadová a oblastní
- NBÚ/NCKB poskytuje podporu při posuzování
- Zjevné VIS jsou uvedené v příloze č. 1 vyhlášky č. 317/2014 Sb.
  - Nyní 92 systémů, které spravuje 35 subjektů
  - Některé jsou na základě určování KII přeřazeny a v následující novele budou z přílohy vyjmuty
  - Nové systémy, posouzené jako VIS, budou do přílohy přidány
- Další VIS jsou postupně jednotlivými orgány veřejné moci nahlašovány
- **Současný stav VIS, které NBÚ eviduje činí cca 110 systémů**

Schéma určování VIS



VIS – 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.

VIS – oblastní kritéria

(Příloha č. 2 k vyhlášce o významných informačních systémech a jejich určujících kritériích)

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.

Příklad: 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
- Jejich systémy naplňují podobná kritéria
  - Koordinovaný postup při posuzování a určování VIS
- Spolupráce na úrovni Asociace krajů – komise informatiky
- Proběhlo několik jednání se zástupci krajů (pracovní úroveň)
- NBÚ/NCKB poskytlo metodické materiály a podporu
- Na tomto základě vytipovány systémy, které splňují kritéria pro VIS
- Navrženy IS k projednání na úrovni komise AKČR s návrhem, aby byly plošně určeny jako VIS

Shrnutí určování povinných osob ze ZKB

§ 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

- Nahlášení kontaktních údajů
- 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 ve VKB (316/2014 Sb.)

Hlavní pilíře ZKB

Organizační opatření – organizační bezpečnost

- Některé organizační opatření:
  - Bezpečnostní role
  - systém řízení bezpečnosti informací
  - řízení rizik
  - bezpečnostní politika
  - stanovení bezpečnostních požadavků pro dodavatele
  - bezpečnost lidských zdrojů, atd.

Hlavní pilíře ZKB

Hlášení kybernetického bezpečnostního incidentu (§ 8 ZKB)

- Hlášení
  - KII a VIS hlásí vládnímu CERT
  - Ostatní povinné a 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 (§ 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

Povinnosti subjektů - shrnutí

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

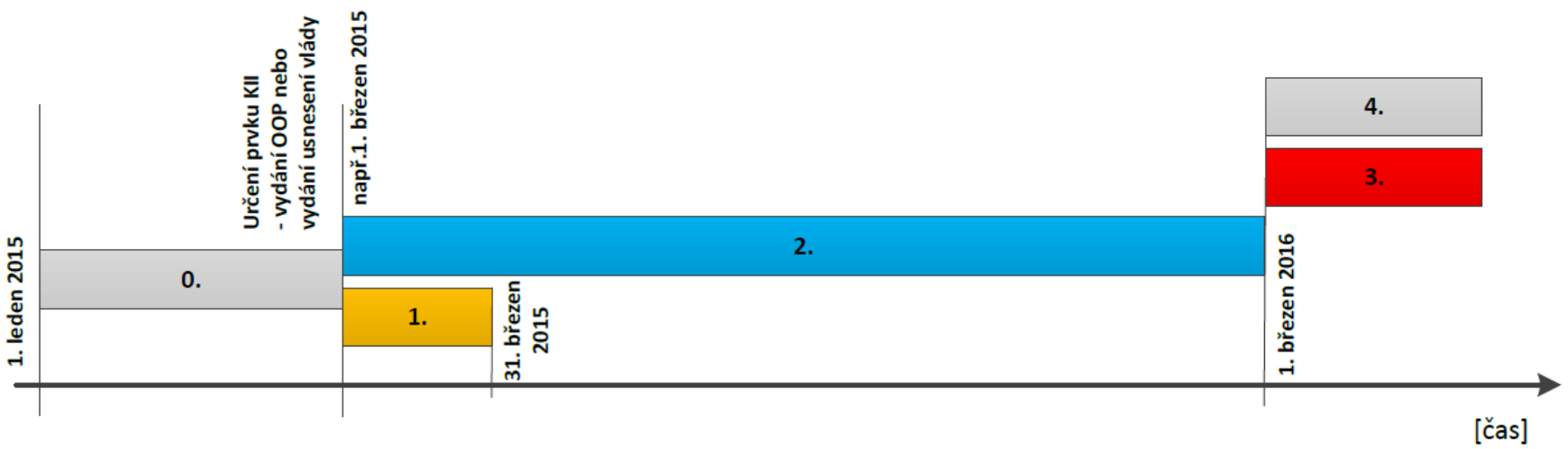
Přechodná období

- 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 detekce a hlášení incidentů – **do 1 roku od**:
  - určení (KII)
  - dne naplnění určujících kritérií (VIS)
  - dne nabytí účinnosti ZKB (významné sítě, poskytovatelé služeb el. komunikací)

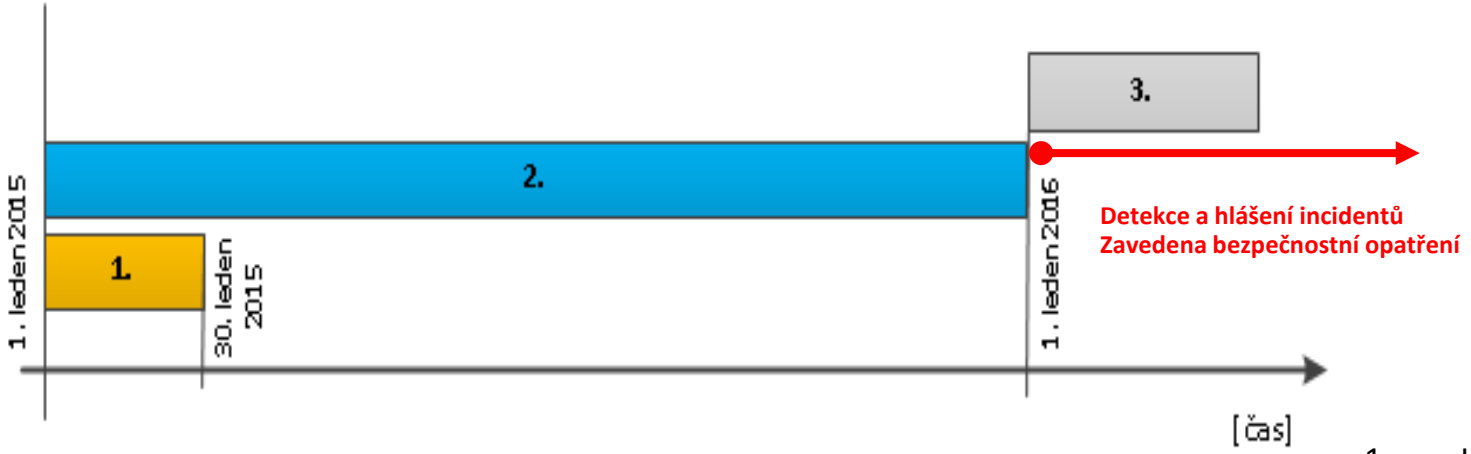
- Subjekty, které se stanou povinnými v průběhu
  - lhůty běží bezprostředně po naplnění definice

Plnění povinností – KII (časová osa)



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

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.

Kontrola a další činnosti v oblasti KB

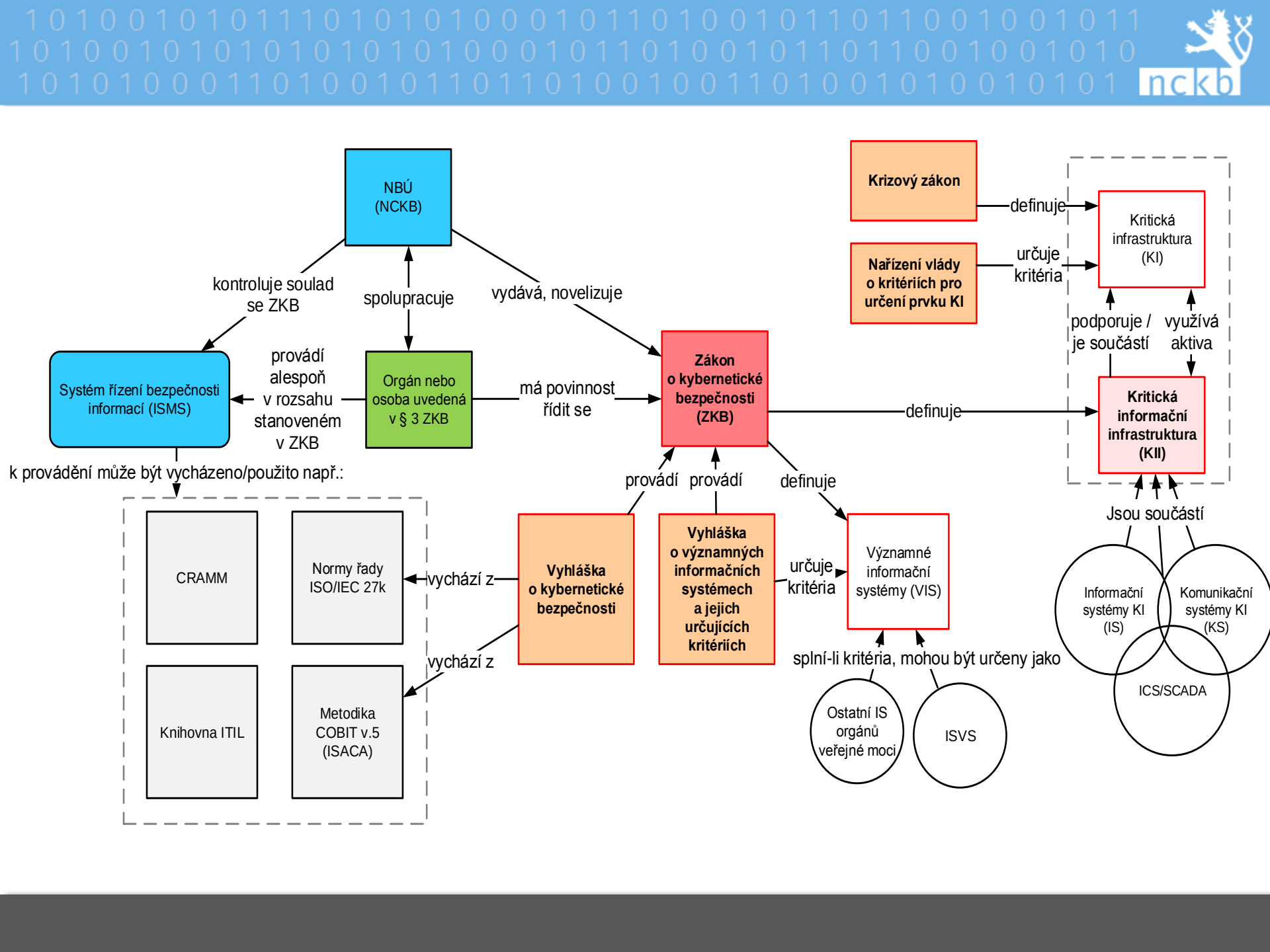
- NBÚ vykonává kontrolu v oblasti kybernetické bezpečnosti.
- Při výkonu kontroly Úřad zjišťuje, jak povinné osoby plní povinnosti stanovené ZKB, prováděcími právními předpisy, rozhodnutími a opatřeními obecné povahy vydanými Úřadem.

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

Sankce v oblasti KB

- 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.


NBÚ
(NCKB)
kontroluje soulad se ZKB
spolupracuje
vydává, novelizuje
Krizový zákon
definuje
Kritická infrastruktura (KI)
Nařízení vlády o kritériích pro určení prvku KI
určuje kritéria
podporuje / je součástí
využívá aktiva
Systém řízení bezpečnosti informací (ISMS)
provádí alespoň v rozsahu stanoveném v ZKB
Orgán nebo osoba uvedená v § 3 ZKB
má povinnost řídit se
Zákon o kybernetické bezpečnosti (ZKB)
definuje
Kritická informační infrastruktura (KII)
k provádění může být vycházeno/použito např.:
provádí
provádí
definuje
Jsou součástí
CRAMM
Normy řady ISO/IEC 27k
Knihovna ITIL
Metodika COBIT v.5 (ISACA)
vychází z
vychází z
Vyhláška o kybernetické bezpečnosti
Vyhláška o významných informačních systémech a jejich určujících kritériích
určuje kritéria
Významné informační systémy (VIS)
Informační systémy KI (IS)
Komunikační systémy KI (KS)
ICS/SCADA
splní-li kritéria, mohou být určeny jako
Ostatní IS orgánů veřejné moci
ISVS

KII a VIS - některé otázky

- 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, nikoli o skutečnost, která by vylučovala či snižovala kritičnost takových systémů.
- „Bílá místa KI“ – např. odvětví zdravotnictví – kritérium 2 500 lůžek nesplňuje žádná nemocnice, chemický průmysl
- Nedostatečná provazba na zákon o veřejných zakázkách (§4 odst. 3 ZKB) – vyloučení nákupu rizikových technologií
- V některých případech je rozdílná terminologie z pohledu ZKB a IT praxe – „správce informačního systému“

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

Užitečné odkazy

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/

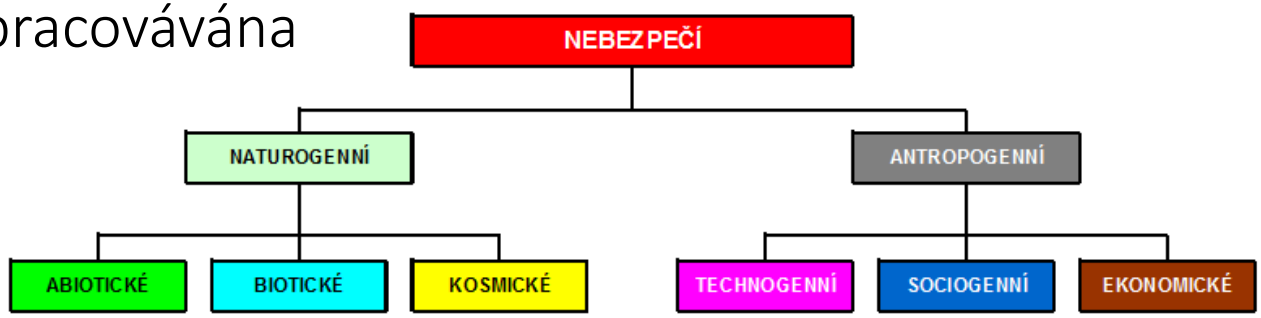
Krizové plánování v kybernetické oblasti

Krizové plánování v kybernetické oblasti

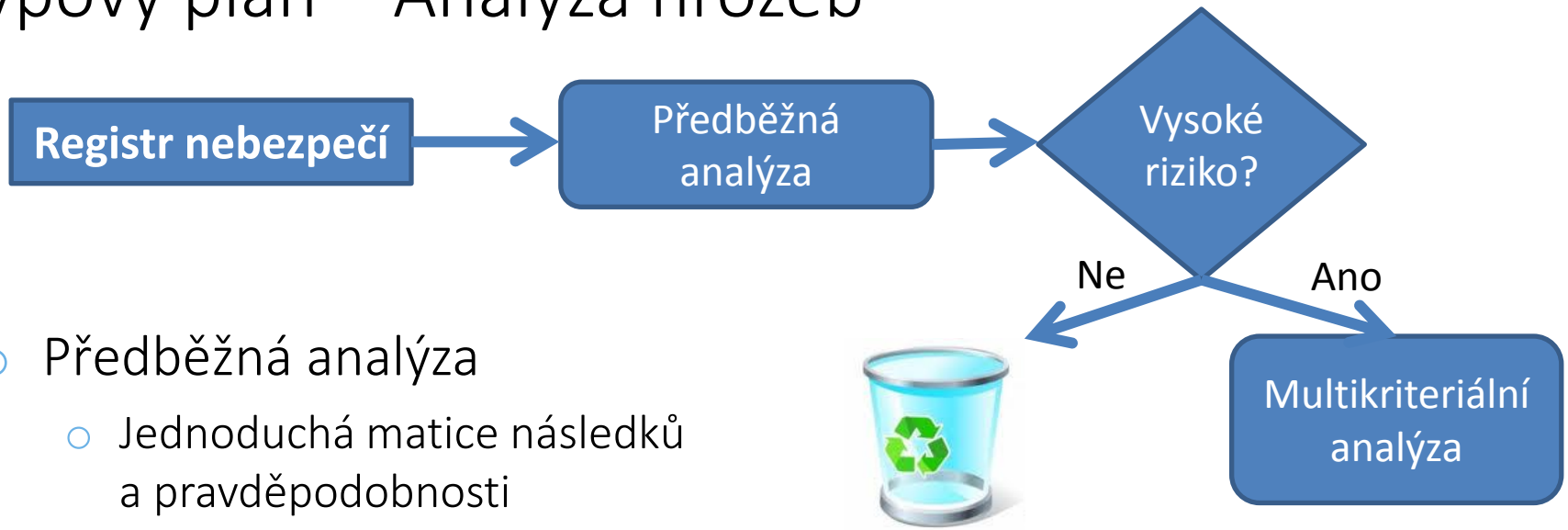
- Orgány veřejné správy všech úrovní vypracovávají soustavu plánů na odvrácení krizových situací
- Krizový plán
  - Zpracovávají v ministerstva a jiné správní úřady, kraje a ORP
  - Dokument obsahující souhrn opatření a postupů k řešení krizových situací
  - Tři části - základní, operativní, pomocná
  - Důležitou částí jsou typové plány na řešení konkrétních hrozeb konkrétních druhů hrozících krizových situací identifikovaných v analýze hrozeb
- Typový plán
  - dokument, ve kterém jsou pro určitý druh krizové situace stanoveny doporučené (typové) postupy, zásady a opatření pro její řešení.
  - zpracování typových plánů mají za úkol jednotlivé ústřední správní úřady v rámci své působnosti

Typový plán

- Obecný návod jakým způsobem řešit krizové situace.
- Obecná metodika, jak přistupovat ke krizové situaci a jak ji co nejefektivněji vyřešit.
- Vzor pro zpracování konkrétních krizových plánů krajů a ústředních správních úřadů, příp. dalších povinných subjektů.
- Existuje tzv. registr nebezpečí - zde jsou identifikována nebezpečí
- Na základě definovaných nebezpečí je zpracovávána analýza rizik



Typový plán – Analýza hrozeb



- Předběžná analýza
  - Jednoduchá matice následků a pravděpodobnosti
  - Vyřazení typů nebezpečí, které mohou vyvolat pouze nízké riziko
- Multikriteriální analýza
  - stanovení úrovně rizika pro jednotlivé typy nebezpečí
  - kvantitativní kritéria
  - metoda expertního odhadu v kombinaci s dostupnými historickými daty

Typový plán – Analýza hrozeb

- **Předběžná analýza**
  - Pro každý typ nebezpečí se stanovuje riziko (R) dle vztahu R = P x N.
  - Základní nastavení kritérií :

Pravděpodobnost (P)		
1	Málo pravděpodobné	Existuje téměř jen teoretická možnost.
2	Pravděpodobné	Je to možné, ojedinělý výskyt.
3	Velmi pravděpodobné	Častý výskyt.

Následky (N)		
1	Nízké	Malý lokální dopad na životy a zdraví osob, majetek, životní prostředí.
2	Významné	Větší dopad na životy a zdraví osob, majetek, životní prostředí regionálního charakteru.
3	Katastrofické	Velmi rozsáhlé dopady na životy a zdraví osob, majetek, životní prostředí nebo ekonomickou či společenskou stabilitu celostátního významu.

  - Typy nebezpečí se rozdělují do 2 skupin – „s nízkým rizikem“ a „s vysokým rizikem“
  - Typy nebezpečí spadající do oblasti s nízkým rizikem se vyřadí a nejsou dále podrobeny detailní multikriteriální analýze. Jedná se o typy nebezpečí s hodnotou rizika 3 a méně
  - Postup není dogmatický - gestor může rozhodnout, že i typy nebezpečí s nízkým rizikem budou podrobeny multikriteriální analýze

Typový plán – Analýza hrozeb

- **Multikriteriální analýza – princip hodnocení**
  - Vztah: R = F x N - Frekvence (četnost) x Následky (dopady)
  - Následky se posuzují z pohledu dopadů:
    - Na životy a zdraví osob ($\mathbf{K_O}$); váhový koeficient $\mathbf{VK_O}$ = 0,4
    - Životní prostředí ($\mathbf{K_{ŽP}}$); váhový koeficient $\mathbf{VK_{ŽP}}$= 0,2
    - Ekonomické ($\mathbf{K_E}$); váhový koeficient $\mathbf{VK_E}$= 0,2
    - Společenské $\mathbf{(K_S)}$; váhový koeficient$\mathbf{VK_S}$= 0,2
  - N= $\mathbf{(K_O \times VK_O) + (K_{ŽP} \times VK_{ŽP}) + (K_E \times VK_E) + (K_S \times VK_S)}$
  - Pro hodnotové vyjádření pravděpodobnosti je využito četnosti (frekvence) možné aktivace nebezpečí

Typový plán – Analýza hrozeb

Časové údobí frekvence možného vzniku MU	F
1 x za několik měsíců (cca 1-6 a častěji)	10
1 x za více měsíců až 1 rok (cca 7 až 12 měsíců)	9
1 x za několik málo let (cca 2-4 roky)	8
1 x za více let (cca 5-10 let)	7
1 x za několik málo desetiletí (cca 2-3 desetiletí = cca 1 generace)	6
1 x za více desetiletí (cca 4-9 desetiletí = cca 2-3 generace)	5
1 x za cca 100 let	4
1 x za několik málo století (cca 2-4 století)	3
1 x za více století	2
1 x za 1000 let a více	1

Typový plán v kybernetické oblasti

- **Narušení bezpečnosti informací kritické informační infrastruktury**
  - Antropogenní – technogenní hrozba
  - Typový plán vztahující se k základním kybernetickým hrozbám
  - Stanovení hrozeb a incidentů by vycházelo z vyhlášky o kybernetické bezpečnosti
  - Plán reakce na jednotlivé hrozby by měl vycházet ze standardů pro DRP (disaster recovery plan)
  - Metodika popisující postupy zvládání účinku těchto hrozeb
  - Subjekty si zapracují do svých typových plánů postupy v případě jednotlivých útoků, reflektující jejich specifika
- **Budoucí cíle**
  - „Vytvořit národní, koordinovaný postup pro zvládání incidentů“
  - „Vytvořit metodologii pro hodnocení rizik v ČR na úrovni státu“
  - Na základě těchto skutečností bude v budoucnu vytvořena metodika, která by rozšiřovala sestavený typový plán.

Děkuji za pozornost

Adam Kučínský

Národní bezpečnostní úřad

Národní centrum kybernetické bezpečnosti

govcert.cz

Kybernetické útoky
- příklad – Ashley Madison

- Seznamka založená v Kanadě v roce 2001
- Sociální síť pro zadané, kteří chtěli mít aféru
- Slogan „Life is short. Have an affair.“
- Návštěvnost : 124 milionů shlédnutí měsíčně (údaj z roku 2015)
- Útok:
  - 15. července 2015 útočníci skupiny „Impact team“ ukradli data o 33 milionech účtů obsahující mimo jiné jména, adresy a údaje o kreditních kartách
  - V případě neuzavření stránek hrozili zveřejněním dat
  - 18. 8. zveřejnili na dark webu odkaz ke stažení 60 GB dat z této seznamky

Kybernetické útoky
- příklad – Stuxnet

- Počítačový červ objevený v červnu 2010 běloruskou firmou VirusBlokAda
- První známý červ soustředěný na kontrolu průmyslových systémů - systémy SCADA
- Umí přeprogramovat programovatelné logické automaty a své změny skrýt
- Cíl útoku:
  - pravděpodobně jaderná elektrárna Búšehr (Irán)
  - závod na obohacování uranu v Natanzu (Irán)
- 45 000 napadených počítačů
  - 60 % Irán, 18 % Indonésie, 8 % Indie

Kybernetické útoky
- příklad – Estonsko 2007 – 1

- Do roku 2007 byly státní informační systémy a databáze propojeny do jednotného informačního systému s vlastní specifickou infrastrukturou
- Součástí bylo 150 informačních systémů veřejného sektoru s více než 1000 různých elektronických služeb
- V roce 2005 se stalo Estonsko první zemí světa, které volilo zástupce do veřejných funkcí přes internet
- Estonsko se postupně stalo zemí, která nejenže ICT využívá jako určitý nadstandard řízení země, ale začala na něm být závislá
- ICT staly natolik důležité, že jejich správné fungování má vliv na bezpečnost celé země

Kybernetické útoky
- příklad – Estonsko 2007 – 2

- V lednu 2007 oznámila estonská vláda úmysl přesunout pomník druhé světové války z centra Tallinnu na vojenský hřbitov v okrajové části města
- Socha – bronzový monument sovětského vojáka - předmětem sporů mezi etnickými Rusy a Estonci
- Přesunutí sochy bylo jednou z hlavních témat v rámci vrcholící kampaně prezidentských voleb
- Ruskou horní komorou parlamentu přijata rezoluce odmítající přestěhování sochy, následně byl navrhnut i bojkot estonského zboží a služeb.

Kybernetické útoky
- příklad – Estonsko 2007 – 3

- Přesun sochy vyvolal nesouhlas části ruské veřejnosti a řady ruských osobností
- V den přesunu sochy - demonstrace, která vyústila v násilnosti, trvající několik dní
- Stovky zraněných a jedna oběť
- Zatčeno 1300 lidí. Odhadované škody nepokojů dosáhly 4,5 milionů eur
- Kybernetické útoky započaly paralelně s demonstracemi proti odstranění sochy

Kybernetické útoky
- příklad – Estonsko 2007 – 4

- První fáze útoku začala 27. dubna 2007 a směřovala proti vládním stránkám a sítím
  - Napadeny zejména webové stránky vlády, premiéra, prezidenta, parlamentu a jednotlivých ministerstev
  - Napaden web vedoucí strany vládní koalice
- Výsledkem byla několikadenní nefunkčnost portálů a další omezení jejich dostupnosti
- Ze soukromého sektoru zasaženy zejména zpravodajské portály
- Výrazné útoky na bankovní sektor
  - V určitých momentech musely být pozastaveny služby dvou největších bank kontrolující v té době 75-80 % trhu

Kybernetické útoky
- příklad – Estonsko 2007 – 5

- Vedle veřejných webů bylo cíleno také na specifické servery, které byly zdrojem dat pro fungování telefonní a zejména mobilní sítě, platebních karet nebo internetové adresáře
- Zasaženy byly také subjekty zajišťující sítě elektronických komunikací, se specifickým zamířením na administrátora národní domény (správce základních internetových serverů pro estonskou vládu a vzdělávací instituce)
- Dopady
  - Socha „uklizena“ na hřbitov
  - Estonsko se začalo více věnovat otázkám kybernetické bezpečnosti a obrany

Kybernetické útoky
- některé útoky na uživatele

- Phishing
  - Jedna z technik sociálního inženýrství
  - Získávání citlivých údajů a hesel
  - Šíří se emailem a snaží se z uživatele k zadání osobních údajů a hesel na falešnou stránku podobnou oficiální
  - „spear phishing“ = cílený phishing na určité uživatele - konkrétní zaměstnance, management
- Botnet
  - síť počítačů infikovaných speciálním software
  - provádí nežádoucí činnost, jako je rozesílání spamu, DDoS útoky, apod.
- Ransomware
  - Zabrání v přístupu k PC a požaduje zaplacení výkupného (ransom) za odblokování
  - Zašifruje data na disku nebo uzamkne PC

Kybernetické útoky - příklad ransomware „PČR“