Představení výzvy č. 10 IROP Kybernetická bezpečnost

ISSS 2016

Adam Kučínský

Národní bezpečnostní úřad

Národní centrum kybernetické bezpečnosti

Povinné osoby podle ZKB

- a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací,
- b) orgán nebo osoba zajišťující významnou síť,
- c) správce informačního systému kritické informační infrastruktury,
- d) správce komunikačního systému kritické informační infrastruktury
- e) správce významného informačního systému

10. Výzva IROP (pouze OSS, Kraje a jimi zřízené organizace, obce, státní podniky)

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
  - KII určuje/navrhuje 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 správci KII až po určovacím procesu
  - ZKB na ně dřív může dopadat jen v rámci jiných povinných osob
- NBÚ ve spolupráci se subjektem (správcem) provede zhodnocení 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 projednají příslušné pracovní orgány vlády
  - Poté je seznam předložen vládě ČR
  - Určení usnesením vlády ČR
- Ostatní:
  - NBÚ určí prvky KII opatřením obecné povahy (OOP)

Kritická informační infrastruktura – určování

- Určování prvků KII rozděleno do tří základních vln
- 1. vlna: Ministerstva a ústřední správní úřady
  - 25. května 2015 vládou schváleno 45 prvků KII, které spravují tyto instituce
- 2. vlna: zbývající část státní správy
  - 15. září 2015 předloženy ke schválení další prvky KII u organizačních složek státu
  - Stále probíhá
- 3. vlna: soukromý sektor (zahrnuje i státní podniky)
  - Stále probíhá

Kritická informační infrastruktura – Shrnutí

- Od účinnosti zákona dosud proběhlo ohledně určování KII přes 160 jednání se soukromými i státními subjekty
- KII veřejný sektor
  - Určeno 48 prvků u 17 správců
  - O dalších probíhají jednání
- KII soukromý sektor
  - Určeno 50 prvků u 19 správců (OOP účinné)
  - Dokončována další jednání s dalšími potencionálními správci KII
- Určování je kontinuální proces

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.

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 alespoň 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 č. 317/2014 Sb., 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 (stačí hlášení kontaktních údajů NBÚ – 1. zákonná povinnost)
- Fakultativně 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

Významné informační systémy – současný stav

- Současný stav VIS:
  - V příloze č. 1 vyhlášky o VIS uvedeno 92 systémů
    - Probíhá novelizace této přílohy
  - Některé původní VIS přeřazeny do KII a některé vyřazeny
  - Nově určeny další systémy jako VIS (zejména kraje)
  - Nyní NBÚ eviduje cca 150 VIS (nejde o konečný počet)
- Seznam ve vyhlášce bude aktualizován

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

Povinnosti: Organizační a administrativní zajištění úkolů

- Povinnost v rámci systému řízení bezpečnosti informací
  - Řídit rizika
  - Hodnotit aktiva
  - Vytvořit a schválit bezpečnostní politiku
  - Nejméně jednou za tři roky nebo v souvislosti s prováděnými nebo plánovanými změnami aktualizovat
    - hodnocení aktiv a rizik
    - bezpečnostní politiku
    - plán zvládání rizik
    - plán rozvoje bezpečnostního povědomí

Organizační a administrativní zajištění úkolů

- Řízení rizik
  - Stanovit metodiku pro identifikaci a hodnocení aktiv a rizik
  - Identifikovat a hodnotit důležitost primárních a podpůrných 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

Některé povinnosti - Organizační bezpečnost (§ 6 VKB)

- Výbor pro řízení kybernetické bezpečnosti – KII i VIS povinně
  - Stanoví práva a povinnosti a určí bezpečnostní role
- Garant aktiva – KII i VIS povinně
  - Osoba pověřená k zajištění rozvoje, použití a bezpečnosti aktiva
- Další bezpečnostní role – KII určí povinně, VIS 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

Některé povinnosti – Organizační opatření

- Stanovení bezpečnostních požadavků na dodavatele (§ 7 VKB)
  - Zavést pravidla pro dodavatele zohledňující řízení bezp. informací
  - Ve smlouvách zavést ustanovení o bezpečnosti informací
- Řízení aktiv (§ 8 VKB)
  - Identifikovat a evidovat primární a podpůrná aktiva
  - Určit garanty aktiv, kteří jsou odpovědní za primární aktiva
  - Hodnot důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti
- Bezpečnost lidských zdrojů (§ 9 VKB)
  - Plán rozvoje bezpečnostního povědomí – plán školení + provádění vstupních a průběžných školení
  - Kontrola dodržování bezpečnostní politiky
  - Odebírání přístupů a aktiv při rozvázání prac. poměru

Některé povinnosti – Organizační opatření (pokrač.)

- Řízení provozu a komunikací (§ 10 VKB)
  - Detekovat kybernetické bezpečnostní události
  - Zajišťovat bezpečný provoz VIS – stanovit provozní pravidla a postupy
  - Zálohování
- Řízení přístupu a bezpečné chování uživatelů (§ 11 VKB)
  - Řídit přístup k VIS a zajistit ochranu přístupových údajů
- Akvizice, vývoj a údržba (§ 12 VKB)
  - Stanovit bezpečnostní požadavky na změny informačního systému spojených s jeho akvizicí, vývojem a údržbou a zahrnout je do projektu
- Zvládání kybernetických bezpečnostních událostí a incidentů (§ 13)
  - Zavést povinnost oznamovat incidenty
  - Klasifikovat incidenty a zavádět opatření na odvracení incidentů

Některé povinnosti – Organizační opatření (pokrač.)

- Řízení kontinuity činností (§ 14 VKB)
  - Určit minimální úroveň služeb nutných pro užívání, provoz a správu VIS
  - Určit dobu obnovení chodu a termín obnovení dát po incidentu
- Kontrola a audit kritické informační infrastruktury a významných informačních systémů (§ 15 VKB)
  - Posuzovat soulad bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky
  - Provádět a dokumentovat pravidelné kontroly dodržování bezpečnostní politiky a výsledky zohlednit v plánu rozvoje bezp. povědomí

TECHNICKÁ OPATŘENÍ (§ 16 – 26 VKB)

- Možno žádat o dotaci z IROP Výzva č. 10: Kybernetická bezpečnost

(více http://strukturalni-fondy.cz/cs/Microsites/IROP/Vyzvy/Vyzva-c-10-Kyberneticka-bezpecnost)

Některé povinnosti – Obsah bezpečnostní dokumentace (§ 28)

- Bezpečnostní politika
- Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik
- Zpráva o hodnocení aktiv a rizik
- Prohlášení o aplikovatelnosti

Doporučená struktura bezpečnostní dokumentace – příloha č. 4 VKB

- Plán zvládání rizik
- Plán rozvoje bezpečnostního povědomí
- Zvládání kybernetických bezpečnostních incidentů
- Strategie řízení kontinuity činností
- Přehled právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků

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