NÁVRH ZÁKONA o KYBERNETICKÉ BEZPEČNOSTI

JUDr. Radomír Valica
ředitel odboru právního a legislativního NBÚ
3. října 2013, Praha

Převzetí gesce nad problematikou kybernetické bezpečnosti

Usnesení vlády ze dne 19. října 2011 č. 781

o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.

- ustavuje Národní bezpečnostní úřad gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast;
- zřizuje Radu pro kybernetickou bezpečnost,
- schvaluje vznik Národního centra kybernetické bezpečnosti, jako součásti Národního bezpečnostního úřadu,

- schvaluje Statut Rady pro kybernetickou společnost,
- schvaluje personální a finanční zabezpečení činnosti NCKB.
- Ukládá řediteli Národního bezpečnostního úřadu

a) vypracovat a do 31. března 2012 předložit vládě návrh věcného záměru zákona o kybernetické bezpečnosti,

b) vybudovat do 31. prosince 2015 plně funkční Národní centrum kybernetické bezpečnosti a jako jeho součást vládní koordinační místo pro okamžitou reakci na počítačové incidenty (vládní CERT - Computer Emergency Response Team),

c) ve spolupráci s ministry vnitra a obrany a ředitelem Bezpečnostní informační služby a vládě do 31. července 2013 předložit návrh zákona o kybernetické bezpečnosti,

d) vedoucím ústředních orgánů státní správy a řediteli Bezpečnostní informační služby vyvíjet potřebnou součinnost při plnění úkolů Rady pro kybernetickou bezpečnost.

Věcný záměr zákona o kybernetické bezpečnosti

Usnesení vlády ze dne 30. května 2012 č. 382 k návrhu věcného záměru zákona o kybernetické bezpečnosti.

- ukládá řediteli Národního bezpečnostního úřadu zpracovat na základě věcného záměru zákona uvedeného v bodě I tohoto usnesení a předložit vládě do 31. července 2013 návrh zákona o kybernetické bezpečnosti.

Návrh zákona o kybernetické bezpečnosti v Legislativní radě vlády (LRV)

Jednání LRV proběhlo dne 8. srpna 2013 a jednání bylo s ohledem na předčasné volby přerušeno.

Hlavní zásady a pilíře návrhu zákona

- minimalizace zásahů do práv soukromoprávních subjektů
- individuální odpovědnost za bezpečnost vlastní sítě

- bezpečnostní opatření (standardizace)
- hlášení kybernetických bezpečnostních incidentů
- protiopatření

Zákon o kybernetické bezpečnosti (ZKB)

Předmět úpravy - § 1

- Předmětem je úprava práv a povinností fyzických a právnických osob, stanovení působnosti a pravomoci orgánů veřejné moci a jejich vzájemná spolupráce v oblasti kybernetické bezpečnosti.

- Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

- Výjimka zohledňující specifika činnosti zpravodajských služeb a Policie České republiky.

Pojmy ZKB

Kybernetický prostor

Kybernetickým prostorem se rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.

Pojmy ZKB

Kybernetická bezpečnost

Kybernetickou bezpečností se rozumí souhrn právních, organizačních, technických a vzdělávacích prostředků k zajištění ochrany kybernetického prostoru.

Pojmy ZKB

Kritická informační infrastruktura a významný informační systém

Kritickou informační infrastrukturou se rozumí prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti.

Významným informačním systémem se rozumí informační systém spravovaný orgánem veřejné správy, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může ohrozit nebo výrazně omezit výkon působnosti orgánu veřejné moci.

Kritická informační infrastruktura

Národní bezpečnostní úřad:

- navrhuje podle krizového zákona Ministerstvu vnitra prvky kritické informační infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jejichž provozovatelem je organizační složka státu a

- určuje podle krizového zákona prvky kritické informační infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jejichž provozovatelem není organizační složka státu.

- Kritická infrastruktura – definice v zákoně č. 240/2000 Sb.

Kritická informační infrastruktura

Krizový zákon § 2

g) kritickou infrastrukturou se rozumí prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu,

i) prvkem kritické infrastruktury se rozumí zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií.

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Toto nařízení bude novelizováno a do odvětví komunikační a informační systémy bude doplněn nový bod Kybernetická bezpečnost.

Povinné osoby (Orgány a osoby) ZKB

Poskytovatelé § 3

Povinnými osobami v oblasti kybernetické bezpečnosti jsou

a) poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací, pokud nespadá pod písmeno b),
b) Subjekty (orgán nebo osoba) zajišťující významné sítě elektronických komunikací, pokud nespadají pod písmeno d).

Významnou sítí se rozumí síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře.

Povinné osoby ZKB

Kritická informační infrastruktura

Významný IS § 3

Povinnými osobami v oblasti kybernetické bezpečnosti jsou

c) správci informačních systémů zařazených do kritické informační infrastruktury,
d) správci komunikačních systémů zařazených do kritické informační infrastruktury a
e) správci významných informačních systémů.

Správcem se rozumí u
informačních systémů ten subjekt, který určuje účel zpracování informací a podmínky jeho provozování,
komunikačních systémů ten subjekt, který určuje účel KS a podmínky jeho provozování.

Systém zajištění kybernetické bezpečnosti

Systém zajištění kybernetické bezpečnosti tvoří:

- **bezpečnostní opatření,**
- **hlášení kybernetických bezpečnostních incidentů,**
- **protiopatření,**
- **oznamování kontaktních údajů a**
- **činnost dohledových pracovišť.**

Systém zajištění kybernetické bezpečnosti

Bezpečnostní opatření § 5

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.**

Systém zajištění kybernetické bezpečnosti

Organizační opatření § 5 odst. 2

- systém řízení bezpečnosti informací,
- řízení rizik,
- bezpečnostní politika,
- organizační bezpečnost,
- stanovení bezpečnostních požadavků pro dodavatele,
- řízení aktiv,
- bezpečnost lidských zdrojů,
- řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,
- řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému,
- akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,
- zvládání kybernetických událostí a kybernetických incidentů,

řízení kontinuity činností a

- kontrola a audit kritické informační infrastruktury a významných informačních systémů.

Systém zajištění kybernetické bezpečnosti

Technickými opatření § 5 odst. 3

- fyzická bezpečnost,
- nástroj pro ochranu integrity komunikačních sítí,
- nástroj pro ověřování identity uživatelů,
- nástroj pro řízení přístupových oprávnění,
- nástroj pro ochranu před škodlivým kódem,
- nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,
- nástroj pro detekci kybernetických událostí,
- nástroj pro sběr a vyhodnocení kybernetických událostí,
- aplikační bezpečnost,
- kryptografické prostředky,
- nástroj pro zajišťování úrovně dostupnosti informací a
- bezpečnost průmyslových a řídících systémů.

Systém zajištění kybernetické bezpečnosti

Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident § 8

- Kybernetickou /bezpečnostní/ událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti a integrity služeb a sítí elektronických komunikací.
- Kybernetickým /bezpečnostním/ incidentem je kybernetická bezpečnostní událost, která představuje narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti a integrity služeb a sítí elektronických komunikací.
- Stanovena povinnost detekce událostí a hlášení kybernetických bezpečnostních incidentů.

Systém zajištění kybernetické bezpečnosti

Hlášení kybernetického bezpečnostního incidentu § 9

Povinné osoby uvedené v § 3 písm. b) až e) jsou povinny hlásit kybernetické bezpečnostní incidenty v jejich informačních systémech nebo službách a sítích elektronických komunikací.

Povinné osoby uvedené v § 3 písm. b) hlásí kybernetické bezpečnostní incidenty provozovateli národního CERTu.

Povinné osoby uvedené v § 3 písm. c) až e) hlásí kybernetické bezpečnostní incidenty NBÚ - vládnímu CERTu.

Systém zajištění kybernetické bezpečnosti

Protiopatření § 13

Protiopatřeními 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 protiopatření:

- **varování,**
- **reaktivní protiopatření,**
- **ochranné protiopatření.**

Systém zajištění kybernetické bezpečnosti

Varování § 14

- Varováním se rozumí varování před hrozbou, která může způsobit kybernetický bezpečnostní incident.

- Úřad vydá varování, dozví-li se z vlastní činnosti nebo z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o hrozbě v oblasti kybernetické bezpečnosti.

- Varování Úřad oznámí povinným osobám a zveřejní jej na internetových stránkách vládního CERT. Součástí varování může být doporučení, jak čelit hrozbě v oblasti kybernetické bezpečnosti.

Systém zajištění kybernetické bezpečnosti

Reaktivní protiopatření § 15

- Reaktivním protiopatřením se rozumí úkony, které Úřad ukládá za účelem řešení kybernetického bezpečnostního incidentu.

- Úřad vydá reaktivní protiopatření rozhodnutím nebo opatřením obecné povahy.

- Úřad může dále vydat povinné osobě rozhodnutí v řízení na místě obsahující pokyny k řešení kybernetického bezpečnostního incidentu.

Systém zajištění kybernetické bezpečnosti

Ochranné protiopatření § 16

- Ochranným protiopatřením se rozumí úkony, které Úřad ukládá na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu za účelem zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací.

- Úřad vydá ochranné protiopatření opatřením obecné povahy.

Systém k zajištění kybernetické bezpečnosti

Kontaktní údaje § 18

Kontaktními údaji se rozumí

- u právnické osoby obchodní firma nebo název včetně odlišujícího dodatku nebo dalšího označení, adresa sídla, identifikační číslo osoby nebo obdobné číslo přidělované v zahraničí,
- u podnikající fyzické osoby obchodní firma nebo název včetně odlišujícího dodatku nebo dalšího označení, adresa místa podnikání a identifikační číslo osoby,
- u orgánu veřejné moci jeho název, adresa sídla, identifikační číslo.

U všech subjektů se hlásí:
údaje o fyzické osobě, která je za povinnou osobu pověřena jednat ve věcech upravených tímto zákonem, v rozsahu jméno, příjmení, telefonní číslo a adresa elektronické pošty.

Systém k zajištění kybernetické bezpečnosti

Dohledová pracoviště § 19 až § 22

Národní CERT – osoba soukromého práva – právnická osoba.

Vládní CERT - provozuje Úřad.

Systém k zajištění kybernetické bezpečnosti

Národní CERT

•Národní CERT - je k výkonu své činnosti oprávněn na základě veřejnoprávní smlouvy uzavírané s Úřadem,

- je vybrán Úřadem v řízení o výběru žádosti podle správního řádu.

• Národní CERT je pracoviště, které zajišťuje sdílení informací na národní i mezinárodní úrovni v oblasti kybernetické bezpečnosti, a to zejména pro osoby soukromého práva.

Systém zajištění kybernetické bezpečnosti

Podmínky výběru provozovatele Národního CERT

- Nevyvíjí ani nevyvíjela činnost proti zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací,
- provozuje nebo spravuje informační systémy nebo služby a sítě elektronických komunikací[1)] anebo se na jejich provozu a správě podílí, a to nejméně po dobu 5 let,
- má technické předpoklady v oblasti kybernetické bezpečnosti,
- je členem nadnárodní organizace působící v oblasti kybernetické bezpečnosti,
- nemá v evidenci daní u orgánů Finanční správy České republiky ani orgánů Celní správy České republiky ani v evidenci daní, pojistného na sociální zabezpečení a pojistného na veřejné zdravotní pojištění evidovány nedoplatky,
- nebyla pravomocně odsouzena za spáchání trestného činu uvedeného v § 7 zákona o trestní odpovědnosti právnických osob a řízení proti nim.

Systém k zajištění kybernetické bezpečnosti

Vládní CERT (výběr)

- Pracoviště provozované NBÚ jako součást NCKB,
- Přijímá oznámení kontaktních údajů od povinných osob uvedených v § 3 písm. c) až e),
- přijímá hlášení o kybernetických bezpečnostních incidentech od povinných osob uvedených v § 3 písm. c) až e),
- vyhodnocuje údaje o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech z kritické informační infrastruktury, z významných informačních systémů, a dalších informačních systémů veřejné správy,
- poskytuje součinnost povinným osobám uvedeným v § 3 písm. c) až e) při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události,
- přijímá podněty a údaje od povinných osob a od subjektů, které nejsou uvedeny v § 3, a tyto podněty a údaje vyhodnocuje,
- přijímá údaje o kybernetických bezpečnostních incidentech od provozovatele národního CERT a tyto údaje vyhodnocuje,

Stav kybernetického nebezpečí

§ 24

- Stav mimořádný, speciální oproti mimořádným stavům vyhlašovaným podle ústavního zákona č. 110/1998 Sb. o bezpečnosti České republiky nebo podle krizového zákona č. 240/2000 Sb.
- Možno vyhlásit pokud je ve velkém rozsahu ohrožena bezpečnost informací v IS, bezpečnost služeb nebo sítí elektronických komunikací a tím dojde k ohrožení nebo porušení zájmu České republiky.
- Stav KN vyhlašuje předseda vlády (ředitel NBÚ).
- Vyhlašován na dobu nejdéle 7 dnů, souhrnná doba nesmí přesáhnout 30 dnů.
- Za stavu kybernetického nebezpečí a za nouzového stavu[4)] je Úřad oprávněn vydat opatření podle § 15 (reaktivní opatření) rovněž orgánům a osobám uvedeným v § 3 písm. a) a b).

Kontrola v oblasti KB

§ 27 a § 28

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

Kontrolu v oblasti kybernetické bezpečnosti dále vykonává Ministerstvo vnitra. Kontroluje zavedení bezpečnostních opatření u významných IS.

Sankce v oblasti KB (výběr)

§ 29

Povinná osoba uvedená v § 3 písm. c) až e) se dopustí správního deliktu tím, že

a) v rozporu s § 5 odst. 2 nezavede bezpečnostní opatření nebo nevede bezpečnostní dokumentaci,

b) neohlásí kybernetický bezpečnostní incident podle § 9 odst. 3,

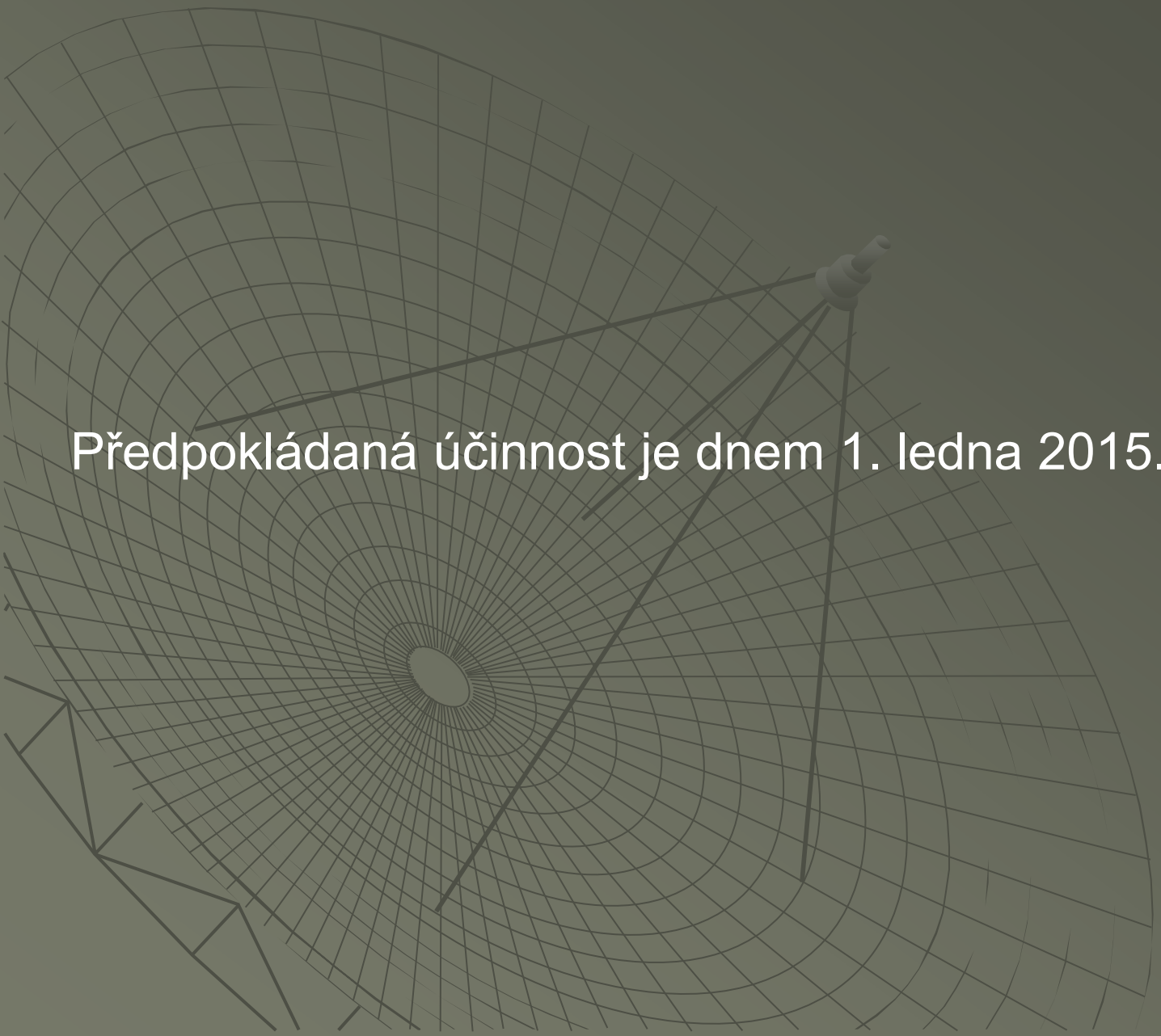
c) neprovede protiopatření vydané Úřadem podle § 15 nebo 16,

d) neoznámí kontaktní údaje nebo jejich změnu podle § 18 odst. 2 písm. b) nebo

e) nesplní některou z povinností uloženou nápravným opatřením podle § 28.

Za správní delikt lze uložit pokutu do 100 000 Kč s výjimkou deliktu podle písmene d), kde hrozí sankce až 10 000 Kč.

Účinnost



Předpokládaná účinnost je dnem 1. ledna 2015.

Děkuji za pozornost

Kontakt – r.valica@nbu.cz