

Zákon o kybernetické bezpečnosti *a směrnice NIS*

Adam Kučínský

Národní bezpečnostní úřad

Národní centrum kybernetické bezpečnosti



DISCLAIMER

- *Prezentace má pouze informativní charakter.*
- *Prezentace odráží stav problematiky k datu jejího vytvoření.*
- *Prezentaci není možné šířit bez předchozího písemného souhlasu autora.*

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
- Cíle novely:
 - Transpozice Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, (směrnice NIS)
 - Odstranění některých nedostatků současné úpravy

Legislativa kybernetické bezpečnosti – současnost

- Hlavní
 - Zákon č. 181/2014 Sb., o kybernetické bezpečnosti („ZKB“)
 - Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti („VKB“)
 - Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích („VVIS“)
 - Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (dále také „NKI“)
- Vedlejší
 - Zákon č. 127/2005 Sb., o elektronických komunikacích („ZEK“)
 - Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů

Povinné osoby podle ZKB – současnost

○ §3 ZKB

- a) poskytovatelé služeb elektronických komunikací, a subjekt zajišťující síť 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

- 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
 - Pouze povinnost hlásit kontaktní údaje
- Změny se v souvislosti s novelou ZKB neplánují

Orgán nebo osoba zajišťující významnou síť

- 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 definicí v ZKB
- Sféra Národního CERTu
 - Povinnost hlásit kontaktní údaje
 - Povinnost detekovat kybernetické bezpečností události
 - Povinnost hlásit incidenty
- Změny se v souvislosti s novelou ZKB neplánují

Kritická informační infrastruktura I.

- Systémy důležité pro chod státu
- Sféra Vládního CERTu
- Určuje/navrhuje NBÚ
- 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
- Nejprísnejší regulace – povinnost plnit celý ZKB:
 - Hlásí kontaktní údaje
 - Detekuje a hlásí incidenty
 - Povinnost zavést bezpečnostní opatření podle vyhlášky č. 316/2014 Sb.
 - Provádí ochranná a reaktivní opatření vydaná NBÚ

Kritická informační infrastruktura II.

- KII určována NBÚ na základě naplnění určujících kritérií
- § 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.
 - Kritérium obětí
 - Kritérium ekonomické ztráty
 - Kritérium dopadu na veřejnost
- Odvětvová kritéria – příloha NV
 - energetika, finanční sektor, **komunikační a informační systémy**, veř. správa,...
- Změny se v souvislosti s novelou ZKB neplánují

Významné informační systémy I.

- 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
- Změny se v souvislosti s novelou ZKB neplánují

Významné informační systémy II.

- VIS posouzené správcem na základě určujících kritérií
 - IS splňující určující oblastní a dopadová kritéria (vyhláška č. 317/2014)
 - **splnění kritérií posuzuje sám správce hodnoceného IS**
 - IS je určen jako VIS interním aktem
 - správce nahlásí NBÚ tuto skutečnost společně s kontaktními údaji
 - V současné době evidujeme 155 VIS u 58 správců
- VIS přímo stanovené v příloze č. 1 VVIS
 - Původně 92 systémů u 36 správců, příloha průběžně novelizována
 - **Zařazení do přílohy nemá konstitutivní charakter pro plnění povinností** – rozhodující je posouzení
- Povinnosti
 - Hlásí kontaktní údaje, Detekuje a hlásí incidenty, zavádí bezp. opatření

Směrnice NIS obecně

- Směrnice stanovuje opatření pro bezpečnost sítí a informačních systémů v rámci Unie s cílem zlepšit fungování vnitřního trhu
- **Některé důvody přijetí směrnice:**
 - IS a KS hrají zásadní roli a jsou nezbytné pro ekonomické a společenské činnosti (čl. 1 preambule)
 - Zvyšuje se rozsah, četnost a dopad bezpečnostních incidentů (čl. 2 pr.)
 - Stávající schopnosti nejsou v Unii dostačující (čl. 5 pr.)
- **Průběh přijetí směrnice**
 - Návrh směrnice je na půdě Evropské unie řešen již od roku 2013
 - Finální znění přijato 6. července 2016, publikace 19. července 2016
 - Platnost od 8. srpna 2016

Jaké povinnosti směrnice NIS přináší

- Státy musí přijmout národní strategii pro bezpečnost sítí a informačních systémů
- Státy musí určit vnitrostátní příslušné orgány pro oblast regulace, jednotná kontaktní místa a týmy CSIRT
- Státy musí určit provozovatele základních služeb (PZS)
 - Stanovení konkrétního datumu - do 9. listopadu 2018
- Směrnice přímo definuje **poskytovatele digitálních služeb (DSP)** – povinnost zpracovat do právního řádu
- PZS s DSP budou muset přijmout a zavést bezpečnostní opatření a hlásit incidenty
- Směrnice dále ustavuje síť skupin pro reakci na incidenty (CSIRT) a skupinu pro spolupráci na úrovni EU

Průběh transpozice NIS na národní úrovni

- ČR musí přijmout úpravu do 21 měsíců od vstupu směrnice v platnost – tedy nejpozději do května 2018
- **Nutno novelizovat ZKB**
 - březen 2016 – svolána pracovní skupina pro transpozici NIS na úrovni jednotlivých resortů
 - duben 2016 - vytvořena pracovní skupina pro transpozici NIS na úrovni odborné veřejnosti
 - 18. července 2016 - návrh novely ZKB odeslán do MPŘ
 - 15. srpna 2016 - MPŘ ukončeno
 - Nyní probíhá vypořádání připomínek
 - Plán: 4. Q/2016 – předložení transpozičních právních předpisů PS

Směrnice NIS – povinné subjekty

- Směrnice zavádí dva druhy povinných subjektů

I. Provozovatelé základních služeb (PZS)

- Klíčové subjekty pro fungování společenských a ekonomických činností
- Určování členskými státy na základě stanovených kritérií
- Kritéria rámcově stanovena směrnicí – dopady a odvětví
- Podobné KII – jsou zde ale rozdíly (PZS orientovány na vnitřní trh x KII na bezpečnosti státu, kritéria KII plně nepokryjí kritéria pro PZS,...)

II. Poskytovatelé digitálních služeb (DSP)

- Regulování nově
- Typově se jedná o vyhledávače, on-line tržiště, cloud computing
- Povinnosti jsou mírnější než u PZS - princip maximální harmonizace

Provozovatel základní služby (PZS) - definice

- **Základní služba** = služba, jejíž poskytování je **závislé na sítích nebo informačních systémech** a jejíž narušení by mohlo mít významný dopad na zabezpečení činností v některém z těchto odvětví:
 - 1. energetika
 - 2. doprava
 - 3. bankovníctví
 - 4. infrastruktura finančních trhů
 - 5. zdravotnictví
 - 6. dodávky a rozvody pitné vody
 - 7. digitální infrastruktura
 - 8. chemický průmysl
- **Informační systém základní služby** = systém, na jehož fungování je závislé poskytování základní služby
- **provozovatel základní služby** = orgán nebo osoba, která je odpovědná za poskytování základní služby a která je určena Národním bezpečnostním úřadem

Určování PZS – kritéria I.

- Pro to, aby byla služba považována za základní je nutné:
 - Aby její **poskytování** bylo **závislé na sítích nebo informačních systémech**
 - **Narušení systému** by mohlo mít **významný dopad na zabezpečení** klíčových společenských nebo ekonomických **činností v některém z vyjmenovaných odvětví** (viz dále)
- Ke každému odvětví NIS uvádí dále pododvětví, kterých se týká
- Pododvětví jsou definována prostřednictvím již schválených odvětvových směrnic či nařízení
- Směrnice nastavuje rozsah povinných subjektů poměrně široce
- V prováděcí vyhlášce bude tento rozsah omezen dopadovými kritérii – **vyhláška zatím nevydána**

Určování PZS – kritéria II.

- Směrnice NIS uvádí odvětví, ve kterých budou PZS určováni:
 - 1. energetika
 - 2. doprava
 - 3. bankovníctví
 - 4. infrastruktura finančních trhů
 - 5. zdravotnictví
 - 6. dodávky a rozvody pitné vody
 - 7. digitální infrastruktura
 - + nad rámec směrnice přidán 8. chemický průmysl
- Směrnice dále v čl. 6 stanoví okolnosti, které mají státy při určení zvážit (jde o období průřezových kritérií u KII):
 - a) **počet uživatelů**, kteří jsou závislí na službě
 - b) **závislost dalších odvětví** na službě poskytované daným subjektem
 - c) možný **dopad incidentů**
 - d) **podíl** daného subjektu **na trhu**
 - e) zeměpisný **rozsah oblasti**, která by mohla být incidentem dotčena
 - f) **důležitost subjektu**, pokud jde o udržování dostatečné úrovně dané služby, s přihlédnutím k **dostupnosti alternativ**

Určování provozovatelů základních služeb (PZS)

- PZS budou určováni opatření obecné povahy vydaným NBÚ
- Určující kritéria stanoví prováděcí vyhláška k ZKB
- Vyhláška zatím není zpracována – zveřejněny pouze teze vyhlášky
- Odvětví budou kopírovat NIS, dopadová kritéria budou respektovat požadavky směrnice a zohledňovat národní podmínky
- Pro určení bude nutné naplnit jak dopadová tak odvětvová kritéria
- **Na konkrétním nastavení kritérií bude spolupracováno s odborníky z veřejné i soukromé sféry**
- **Kritéria je nutno nastavit tak, aby regulace pokryla pouze systémy nezbytné pro zajištění služeb (ne fakturační či marketing. systémy)**

Určování PZS – možná kritéria (jedna z variant)

- Dopadová kritéria pro určování PZS by mohly vypadat následovně:
 - a) omezení základní služby postihující více než 50 000 osob
 - b) omezení či narušení jiné základní služby, nebo omezení či narušení provozu prvku kritické infrastruktury
 - c) hospodářskou ztrátu vyšší než XXX % HDP
 - d) nedostupnost služby, která není nahraditelná jinou službou
 - e) oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření
 - f) ohrožení veřejné bezpečnosti v minimálním rozsahu správního území obce s rozšířenou působností
 - g) kompromitaci citlivých údajů o 200 000 osobách
- Mnoho vitálních systémů již určeno jako KII – nepředpokládáme výrazné množství PZS
- V případě, že systém naplní kritéria pro PZS i KII – určí se jako KII



Odvětví PZS podle NIS – I. Energetika

- Pododvětví Elektřina
 - elektroenergetický podnik
 - provozovatel distribuční soustavy a provozovatel přenosové soustavy
- Pododvětví Ropa
 - provozovatel ropovodů
 - provozovatelé zařízení na zpracování, rafinaci a úpravu ropy a skladovacích a přenosových zařízení
- Pododvětví Zemní plyn
 - fyzická nebo právnická osoba, která provádí dodávky
 - provozovatel distribuční a přepravní soustavy
 - provozovatel skladovacího zařízení
 - provozovatel zařízení LNG
 - plynárenský podnik a provozovatel zařízení na rafinaci a úpravu plynu



Odvětví PZS podle NIS – II. Doprava

- Pododvětví Letecká doprava
 - letečtí dopravci
 - letiště
 - řízení letového provozu
- Pododvětví Železniční doprava
 - provozovatelé infrastruktury
 - železniční podniky
- Pododvětví Vodní doprava
 - podniky vnitrozemské, námořní a pobřežní osobní a nákladní vodní dopravy
 - řídicí orgány přístavů
- Pododvětví Silniční doprava
 - silniční orgány a provozovatelé inteligentních dopravních systémů

Odvětví PZS podle NIS – III. Bankovníctví, IV. Infrastruktura finančních trhů

- Bankovníctví
 - úvěrové instituce (podnik, jehož činnost spočívá v přijímání vkladů nebo jiných splatných peněžních prostředků od veřejnosti a poskytování úvěrů na vlastní účet)
- Pododvětví Infrastruktura finančních trhů
 - provozovatelé obchodních systémů (regulovaný trh, mnohostranný obchodní systém nebo organizovaný obchodní systém)
 - ústřední protistrana (právnícká osoba, která vstupuje mezi strany smluv uzavíraných na jednom či na několika finančních trzích, a stává se tak kupujícím pro každého prodávajícího a prodávajícím pro každého kupujícího)



Odvětví PZS podle NIS – V. Zdravotnictví

- Poskytovatelé zdravotní péče
 - poskytovatel zdravotní péče = fyzická nebo právnická osoba nebo jiný subjekt, který zákonným způsobem poskytuje zdravotní péči na území členského státu

Odvětví PZS podle NIS – VI. Dodávky a rozvody pitné vody

- Dodavatel a distributor „vody určené k lidské spotřebě“
 - „vodou určenou k lidské spotřebě“ se rozumí:
 - veškerá voda, v původním stavu nebo po úpravě, určená k pití, vaření, přípravě potravin nebo k jiným účelům v domácnosti, bez ohledu na její původ či zda je dodávána z rozvodné sítě, ze zásobníků cisteren, v lahvích nebo kontejnerech;
 - veškerá voda používaná v potravinářských zařízeních k výrobě, zpracování, konzervaci nebo uvádění výrobků nebo látek určených k lidské spotřebě na trh



Odvětví PZS podle NIS – VII. Digitální infrastruktura

- Výměnné uzly internetu
- Poskytovatelé služeb systému doménových jmen
- Rejstříky internetových domén nejvyšší úrovně

Provozovatel základní služby (PZS) – povinnosti

- NIS stanovuje následující okruhy povinností pro PZS:
 - Přijmout **technická** a **organizační opatření** k řízení rizik
 - Přijmout opatření k **předcházení incidentům** narušujícím bezpečnost
 - **Oznamovat incidenty** včetně případných přeshraničních dopadů
 - Poskytovat národní regulační autoritě informace pro posouzení bezpečnosti včetně bezpečnostní politiky
 - **Provádět nápravu** zjištěných **nedostatků**
- Povinnosti jsou stejné jako u KII - rozsah povinností bude stejný
- KII má navíc povinnosti vyplývající z krizového zákona
- PZS bude regulována jako samostatná kategorie - nebude zahrnuta pod krizový zákon

Poskytovatel digitálních služeb (DSP) - definice

- Poskytovatel digitální služby poskytuje službu:
 - **On-line tržiště** - umožňuje on-line uzavírat kupní smlouvu nebo smlouvu o poskytnutí služeb prostřednictvím internetové stránky on-line tržiště nebo prostřednictvím internetové stránky prodávajícího, která využívá službu on-line tržiště
 - **Internetového vyhledávače**
 - **Cloud computingu** - umožňuje přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů, jež je možno sdílet
- Tyto definice vycházejí přímo ze směrnice
- Regulace se netýká malých a mikro podniků

Poskytovatel digitálních služeb (DSP) – povinnosti

- **§ 4 odst. 3 NZKB:** zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě a informační systémy, které využívá v souvislosti se zajišťováním své služby
- **§ 8 odst. 2 NZKB:** hlásit kybernetický bezpečnostní incident s významným dopadem na poskytování jeho služeb
- **§ 16 odst. 2 písm. h) NZKB:** oznamovat kontaktní údaje Nár. CERTu
- Uplatňuje se princip maximální harmonizace – povinnosti nad rámec NIS se neukládají, kontrola pouze při podezření neplnění požadavků
- DSP tedy musí:
 - Přijmout vhodná a přiměřená technická a organizační opatření k řízení rizik
 - Přijatá opatření musí odpovídat míře existujícího rizika
 - Přijmout opatření k předcházení incidentů a incidenty oznamovat

Co dále přináší novela ZKB

- **§ 3a:** pokud DSP nemá zástupce v členském státu EU musí jej zřídit
- **§ 4 odst. 6:** KII, VIS a PZS kteří jsou orgánem veřejné moci, jsou povinni si smluvně ošetřit vlastnictví dat a možnost jejich kontroly s poskytovatelem cloud comp.
- **§4a odst. 2:** Pokud KII, VIS nebo PZS není provozovatelem svého systému, musí provozovatele informovat o tom, že IS/KS byl určen
- **§4a odst. 2:** KII musí informovat své ISP o tom, že se tito ISP stávají významnou sítí
- **§ 12 odst. 3:** Právo NBÚ informovat veřejnost o incidentu
- **§ 25:** Změna sankcí za správní delikty a zavedení nových deliktů
- Změna zákona o svobodném přístupu k informacím

Co dále přináší NIS

- Mezinárodní spolupráce – směrnice vytváří unijní kooperační struktury pro usnadnění výměny informací a osvědčených postupů (skupina pro spolupráci a síť CSIRT)
- Národní struktury a rámce – zavádí povinnost vytvořit příslušné orgány odpovědné za kybernetickou bezpečnost na vnitrostátní úrovni, zřídit týmy CSIRT a jednotné kontaktní místo -> **v ČR již zavedeno**
- Bezpečnost sítí a informačních systémů – zavádí povinnosti týkající se bezpečnosti sítí a informačních systémů, které musí povinné subjekty splňovat a které mohou být vymáhány příslušnými orgány -> **v ČR již zavedeno**

NIS x ZKB – srovnání požadavků

Směrnice NIS	Zákon o kybernetické bezpečnosti
Národní strategie bezpečnosti sítí a informací	Národní strategie kybernetické bezpečnosti 
Zavádí požadavky na bezpečnost a oznamování incidentů	Povinnost zavést bezp. opatření a hlásit incidenty 
Ustavuje síť skupin pro reakci na incidenty (CSIRT)	Zakotvil činnosti Vládního a Národního CERT 
Povinnost zřídit vnitrostátní orgány, které budou mít bezpečnost sítí a IS v gesci	NBÚ gestorem Kybernetické bezpečnosti 
Určit jednotné kontaktní místo v regulované oblasti	NBÚ je kontaktním místem pro nár. i mezinár. spolupráci v oblasti KB 
Určení PZS	Částečně zavedeno (KII) 
Určení DSP	Nezavedeno 



Legislativa KB – současnost vs. budoucnost

- Hlavní
 - Zákon č. 181/2014 Sb., o kybernetické bezpečnosti („ZKB“)
 - **Probíhá novelizace – 15. srpna skončilo MPŘ**
 - Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti („VKB“)
 - **Bude novelizována (pouze formální doplnění povinných osob)**
 - Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích („VVIS“) – beze změny
 - Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (dále také „NKI“) – beze změny
 - + **Bude vydána nová vyhláška o poskytovatelích základních služeb (určovací kritéria)**
- Vedlejší
 - Zákon č. 127/2005 Sb., o elektronických komunikacích („ZEK“)
 - Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů

Struktura povinných podle ZKB – současnost vs. budoucnost

○ §3 NZKB

- a) poskytovatelé služeb elektronických komunikací, a subjekt zajišťující síť elektronických komunikací
- b) orgán nebo osoba zajišťující významnou síť
- c) **Poskytovatel digitálních služeb**
- d) správce IS KII
- e) správce KS KII
- f) správce VIS
- g) **správce a provozovatel IS základní služby**
- h) **provozovatel základní služby**

NÁRODNÍ CERT

VLÁDNÍ CERT

Přehled povinností podle novely ZKB

- Nahlášení kontaktních údajů (§16 ZKB)
 - Všechny povinné osoby, **nově i DSP a PZS**
- Hlášení kybernetických bezpečnostních incidentů (§8 ZKB)
 - KII, VIS, významné sítě, **nově i DSP a PZS**
- Zavedení bezpečnostních opatření (standardizace) (§4 ZKB)
 - KII, VIS, **nově i PZS, DSP pouze některá opatření**
- Činit opatření vydané NBÚ (§11 ZKB)
 - KII, VIS, **nově i PZS**
 - Významné sítě a poskytovatelé služby el. komunikací pouze za stavu kybernetického nebezpečí, pouze reaktivní opatření



Děkuji za pozornost

Adam Kučínský

Národní bezpečnostní úřad

Národní centrum kybernetické bezpečnosti

nbu.cz

govcert.cz

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/kontrolě bezpečnostních opatření podle zákona:
<http://www.govcert.cz/cs/kii--vis/dalsi-materialy-ke-stazeni/>
- Výkladový slovník kybernetické bezpečnosti - třetí vydání:
<http://www.govcert.cz/cs/informacni-servis/vykladovy-slovník/>
- **Návrh novely zákona o KB** (vč. úplného znění): <https://apps.odok.cz/veklep-detail?pid=ALBSABVH86O2>
- **Směrnice NIS v ČJ** (Úřední věstník EU, 19. 7. 2016, L194): <http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=EN>