Novela ZKB
–
změny v zákoně, nové povinné osoby a jejich povinnosti

Adam Kučínský
Vedoucí oddělení regulace
Sekce NCKB

Národní úřad
pro kybernetickou
a informační bezpečnost

Plnění ZKB před novelou

- Počet KII – cca 110 systémů u cca 40 subjektů
- Počet VIS – 169 systémů u cca 63 subjektů
  - Celkem pod ZKB spadá cca 280 systémů
- Audity/Kontroly plnění povinností
  - Od roku 2016 provedeno 15 auditů správců KII/VIS a 18 metodických kontrol ÚSÚ
- Mnoho dalších aktivit
  - Kybernetická cvičení, mezinárodní spolupráce, EU agendy, vzdělávání…
- Více: Zprava o stavu KB ČR za rok 2016

  https://nukib.cz/cs/informacni-servis/publikace/
- Zpráva o stavu KB ČR za rok 2017 v přípravě

Legislativa kybernetické bezpečnosti - změny

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti („ZKB“)
  - ***Novelizován*** *– novely účinné od 1. 7. 2017 a od 1. 8. 2017*
- Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti („VKB“)
  - ***Probíhá novelizace*** *– draft zde: https://nukib.cz/cs/nova-vkb/*
  - *Předpokládaná účinnost novely – květen 2018*
- Vyhláška č. 317/2014 Sb., o významných informačních systémech
  - *Zatím beze změny – novelizace v r. 2018?*
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku KI
  - *Beze změny*
- **Nová vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby**
  - *Určovací kritéria*
  - *Účinnost – únor 2018*

Zákon o kybernetické bezpečnosti – změny v r. 2017

- **ZKB byl v r. 2017 novelizován ve dvou liniích:**
  - **„Velká novela“ – transpozice směrnice NIS**
    - **Novela účinná od 1. 8. 2017** (Novela cestou zákona č. 205/2017 Sb.)
    - **Úpravy ZKB:** nové definice (§ 2), nové povinné osoby (§ 3), vznik „Národního úřadu pro kybernetickou a informační bezpečnost“, změny správních deliktů (§ 25)…
  - **„Malá novela“ – změna novelou zákona č. 365/2000 Sb., o ISVS**
    - **Novela účinná od 1. 7. 2017** (Novela cestou z. č. 104/2017)
    - **Úpravy ZKB:** nový pojem provozovatel IS/KS (§ 2 písm. g), smluvní vztahy s cloudem (§4/5) vzájemná informační povinnost (§ 4a), ustanovení o vlastnictví dat (§ 6a), hlášení incidentů provozovatelem (§ 8/4), pravomoc nařízení předání dat (§ 15a), změny správních deliktů (§ 25),

Struktura povinných podle ZKB – stav od 1. 8. 2017

- §3 NZKB

○ poskytovatelé služeb elektronických komunikací, subjekt zajišťující sít elektronických komunikací ○ orgán nebo osoba zajišťující významnou síť ○ **Poskytovatel digitálních služeb**	NÁRODNÍ CERT *CZ.NIC*
○ správce ***a provozovatel*** IS KII ○ správce ***a provozovatel*** KS KII ○ správce ***a provozovatel*** VIS ○ **správce a provozovatel IS základní služby** ○ **provozovatel základní služby**	VLÁDNÍ CERT *NÚKIB*

Nové povinné osoby

- **Provozovatel základní služby (PZS), informační systém základní služby (ISZS)**
  - Systémy klíčové pro zajišťování některých hospodářských a ekonomických činností
  - Podobné KII (jsou zde ale rozdíly)
- **Poskytovatel digitální služby (DSP)**
  - Zajišťuje služby cloudu, internetového vyhledávače, e-commerce
- **Provozovatel informačního/komunikačního systému KII/VIS/PZS**
  - *„zajišťuje funkčnost technických a programových prostředků tvořících informační nebo komunikační systém“ = klíčový dodavatel*
  - *Zařazen do povinných osob* – zavádí bezpečnostní opatření tam, kde je nemůže zavést správce
  - Důvod úpravy: problémy se zabezpečením dodavatelů…

Poskytovatel digitálních služeb (DSP)

Poskytovatel digitálních služeb (DSP) - definice

- Poskytovatel digitální služby = digital service provider = DSP

- 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 <u>netýká malých a mikro podniků</u>
  - <50 zaměstnanců a roční bilanční suma nebo obrat <10 mil. €
- Funguje zde <u>princip samourčení</u> – naplnění definice = povinná osoba

Poskytovatel digitálních služeb (DSP) – povinnosti dle ZKB

- Uplatňuje se princip **maximální harmonizace** – povinnosti nad rámec NIS se neukládají, kontrola pouze při podezření neplnění požadavků
- **§ 4 odst. 3 NZKB:** zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě a IS, využívané k poskytování služby
- **§ 8 odst. 2 NZKB:** hlásit kybernetický bezpečnostní incident s významným dopadem na poskytování jeho služeb NCERTu
- **§ 16 odst. 2 písm. h) NZKB:** oznamovat kontaktní údaje NCERTu
- Opatření musejí odpovídat „míře existujícího rizika“

- Bezpečnostní opatření - viz prováděcí nařízení komise 2018/151

Jak budou vypadat povinnosti u DSP?

- U PZS strukturu a rozsah povinností známe, můžeme si je upravit jako stát poměrně svobodně sami
- U DSP nemůžeme regulovat nad rámec NIS a prováděcí aktů EK
- Jak tedy budou vypadat jejich povinnosti?
  - Vodítka (povinná) vydává EK – tzv. „implentation acts“
    - Dne 31. 1. 2018 zveřejněno prováděcí nařízení komise (EU) 2018/151, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148 (Směrnice NIS) => **ÚČINNOST OD 10. května 2018**

http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv:OJ.L_.2018.026.01.0048.01.CES&toc=OJ:L:2018:026:TOC

  - ENISA by k tomu dále měla dávat doporučení – zatím pouze jedno:
    - **Minimální bezp. opatření pro DSP:** *Technical Guidelines for the implementation of minimum security measures for Digital Service Providers* (ENISA, prosinec 2016)

https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

Prováděcí nařízení komise 2018/151 ze dne 30. ledna 2018

- Plný název: Prováděcí nařízení komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný
- Dostupné i v ČJ zde: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32018R0151&from=CS

- Celkem 5 článků (důležitý je i recitál)
- Účinnost od 10. května 2018
- Přímo účinné – žádná transpozice
- Žádná přechodná lhůta pro povinnosti – 10. květen je závazný
- Připravovaná novela vyhlášky o kybernetické bezpečnosti na nařízení odkazuje

Provozovatel základní služby (PZS) a informační systém základní služby (ISZS)

Určování provozovatelů základních služeb (PZS) - obecně

- PZS budou na základě určujících kritérií určováni rozhodnutím (dle SŘ)
- Určující kritéria definuje vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby (účinnost od 1. února 2018)
  - Na nastavování kritérií se podílela pracovní skupina z řad soukromé i státní sféry (14 podskupin dle odvětví a pododvětví)
- Pro určení bude nutné naplnit jak dopadová tak odvětvová kritéria
  - Odvětví kopírují NIS (+ chemický průmysl a teplárenství)
  - Dopadová kritéria respektují požadavky směrnice a zohledňují národní podmínky
- Kritéria a definice nastavena tak, aby regulace pokryla pouze systémy nezbytné pro zajištění služeb (ne fakturační, marketingové systémy ani např. bankomaty)
- Mnoho vitálních systémů již určeno jako KII
- V případě, že systém naplní kritéria pro PZS i KII – určí se jako KII

Určování provozovatelů základních služeb (PZS) - kritéria

Aby byl subjekt a jeho informační systém určen musí naplnit všechny tři podmínky

1. **Definice ZKB**
   - Závislost na IS/KS
   - Narušení služby by mělo dopad ve vymezených odvětvích
2. **Odvětvová kritéria** (3 úrovně)
   - Druh služby
   - Druh subjektu
   - Speciální kritéria druhu subjektu
3. **Dopadová kritéria**
   - Dopad kybernetického bezpečnostní incidentu v IS/KS, na jehož fungování je závislé poskytování služby

1. Provozovatel základní služby (PZS) – definice dle NZKB

- **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. bankovnictví
4. infrastruktura finančních trhů
5. zdravotnictví
6. vodní hospodářství
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 NÚKIB

2. Provozovatel základní služby (PZS) – odvětvová kritéria

- Směrnice NIS uvádí odvětví, ve kterých budou PZS určováni:
  1. energetika
  2. doprava
  3. bankovnictví
  4. infrastruktura finančních trhů
  5. zdravotnictví
  6. vodní hospodářství
  7. digitální infrastruktura

  + nad rámec směrnice přidán 8. chemický průmysl
- Některá odvětví se dále dělí na pododvětví:
  - Energetika na: elektřina, plyn, ropa, teplárenství
  - Doprava na: leteckou, železniční, vodní a silniční
- Směrnice nastavuje rozsah povinných subjektů poměrně široce
- Ve vyhlášce jsou v relevantních odvětvích přidána ještě tzv. **speciální kritéria druhu subjektu**,
  - Naplní je pouze nejvýznamnější organizace v daném odvětví či pododvětví
  - ➢ Ne všechny organizace v daném odvětví budou posuzovány z hlediska dopadu incidentu v jejich IS/KS

3. Provozovatel základní služby (PZS) – dopadová kritéria (ČR)

Dopad kybernetického bezpečnostního incidentu v informačním systému nebo sítí el. komunikací, na jehož fungování je závislé poskytování služby, může způsobit:	
a) závažné omezení či narušení druhu služby postihující více než 25 000* nebo 50 000* nebo 500 000* osob,	e) oběti na životech s mezní hodnotou více než 100* nebo 200* mrtvých nebo 1 000 zraněných osob vyžadujících lékařské ošetření,
b) závažné omezení či narušení jiné základní služby, nebo omezení či narušení provozu prvku kritické infrastruktury,	f) narušení veřejné bezpečnosti na významné části správního území obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací základními a ostatními složkami integrovaného záchranného systému, nebo
c) hospodářskou ztrátu vyšší než 0,25 % HDP,	g) kompromitaci citlivých údajů o více než 200 000 osobách.
d) nedostupnost druhu služby pro více než 1 600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,*	

Pozn.: Jedná se o výčet všech použitých dopadů – v jednotlivých odvětvích se jejich uplatnění liší

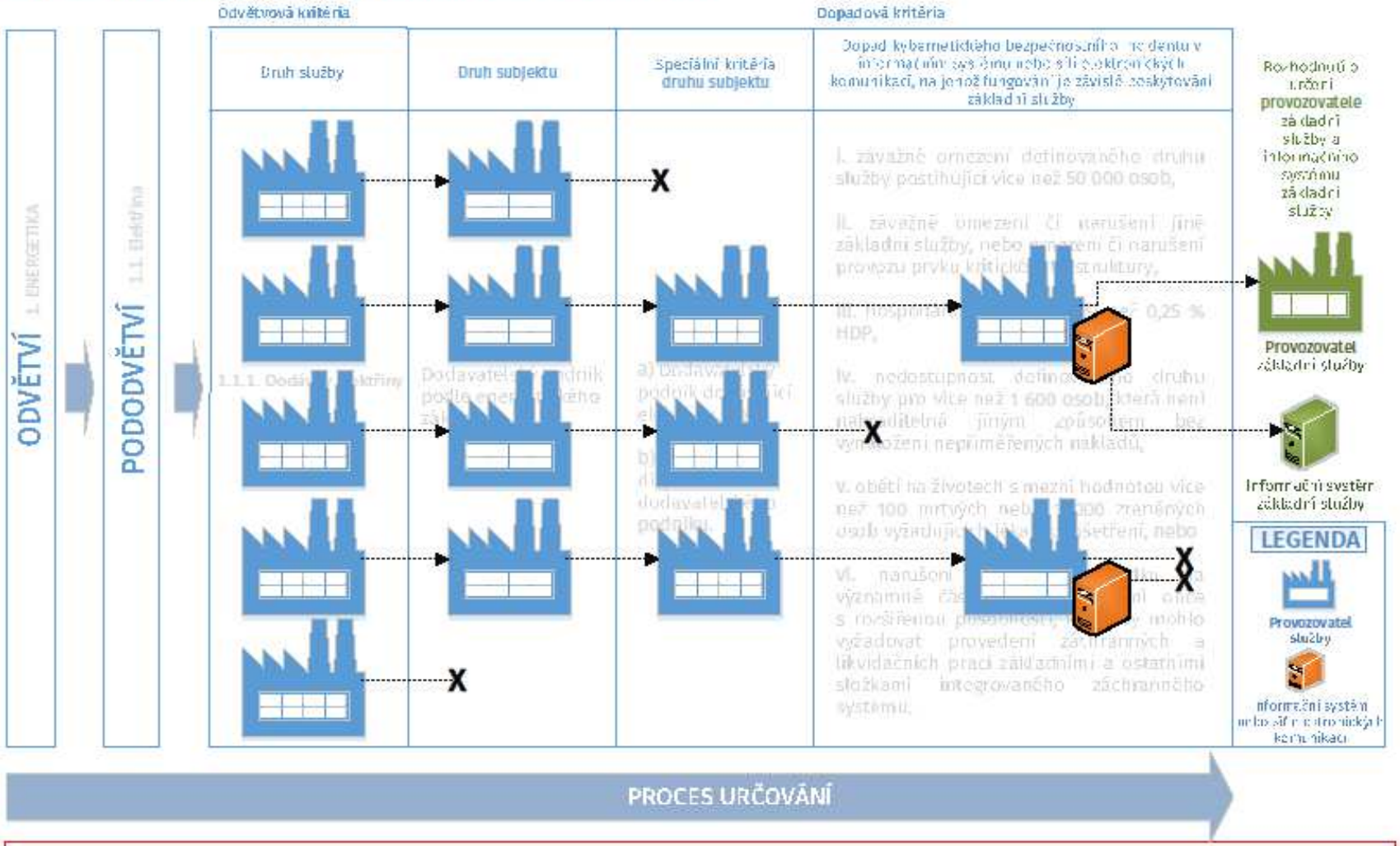
* V závislosti na specifících jednotlivých odvětví se tyto hodnoty liší

Základní služba

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

Proces určení provozovatele základní služby a informačního systému základní služby dle zákona o kybernetické bezpečnosti a vyhlášky o kritériích pro určení provozovatelů základních služeb



Upozornění:

Dokument slouží pouze jako podpůrné vodítko, nenahrazuje žádný ze zákonů a souvisejících prováděcích předpisů. Právo změny tohoto dokumentu vyhrazeno. Další šíření tohoto dokumentu je možné pouze s písemným souhlasem Národního úřadu pro kybernetickou a informační bezpečnost.

Více informací o procesech určování a posuzování, včetně povinností orgánů a osob, naleznete na www.GovCERT.cz

Zdroj: https://www.govcert.cz/cs/zkb/podpurne-materialy/

Příloha vyhlášky č. 437/2017 Sb. – příklad - 3. Bankovnictví

3. Bankovnictví

Odvětvová kritéria			Dopadová kritéria
Druh služby	**Druh subjektu**	**Speciální kritéria druhu subjektu**	
3.1. Výkon činnosti úvěrové instituce	Úvěrová instituce podle přímo použitelného předpisu Evropské unie[9])	a) Počet klientů nad 500000 nebo b) tržní podíl přesahující 1 % z bilanční sumy bankovního sektoru.	Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit I. závažné omezení druhu služby postihující více než 500000 osob, II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury, III. hospodářskou ztrátu vyšší než 0,25 % HDP nebo IV. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému.

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 je regulována jako samostatná kategorie - není zahrnuta pod krizový zákon

Provozovatel informačního/komunikačního systému

Provozovatel = *„zajišťuje funkčnost technických a programových prostředků tvořících informační nebo komunikační systém“ (§ 2 písm. g) ZKB)*
= klíčový dodavatel

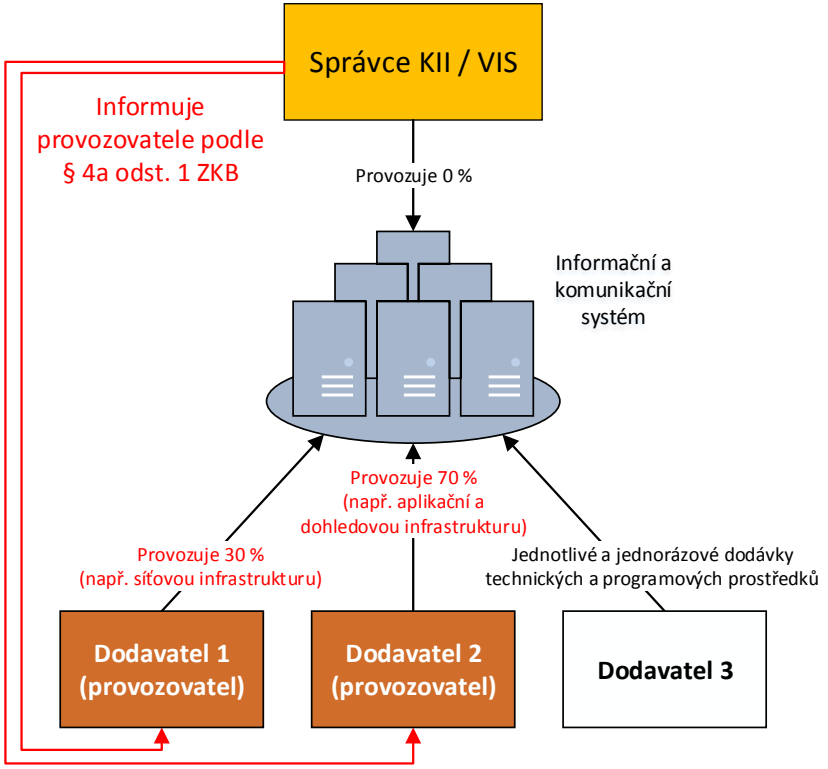
Provozovatel informačního/komunikačního systému

- Provozovatel IS/KS je „malou novelou“ od 1. 7. 2017 přidán do § 3 ZKB mezi povinné osoby = tam kde je to vhodné a možné zavadí bezp. opatření.
- Týká se KII, VIS a PZS
- Je možné u něj provést kontrolu plnění ZKB a při porušení vůči němu zahájit správní řízení
- Důvod zavedení: často velmi problematické smlouvy v oblasti IT zejména ve státní správě
- Provozovatel ≠ každý dodavatel
- Ostatní dodavatelské vztahy musí být také z pohledu bezpečnosti řízeny - § 7 VKB
- Definice provozovatele v § 2 je dosti široká
  - Podpůrný materiál NÚKIB: https://www.nukib.cz/cs/zkb/podpurne-materialy/

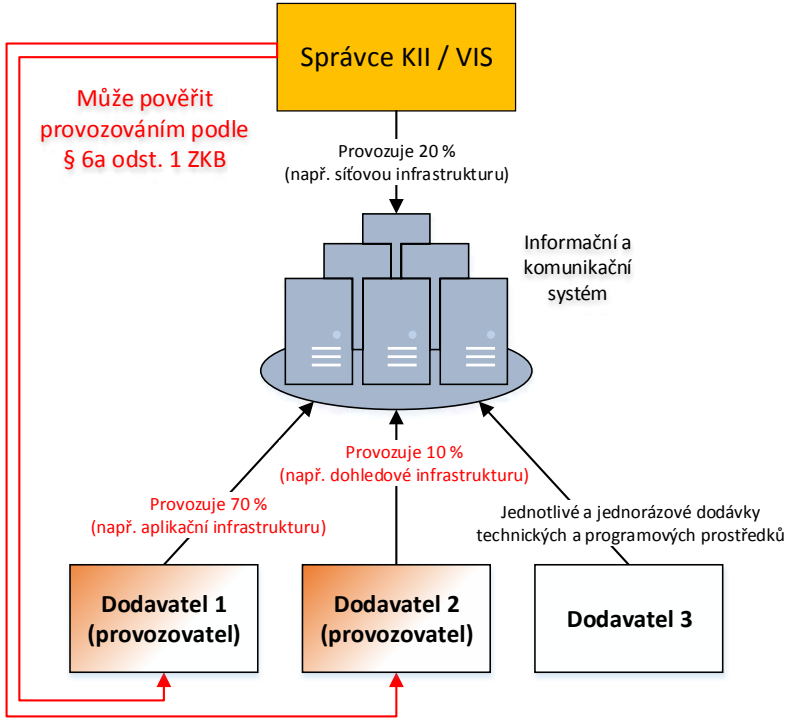
Provozovatel informačního/komunikačního systému

- Definice v ZKB (§ 2 písm. g)): *„zajišťuje funkčnost technických a programových prostředků tvořících informační nebo komunikační systém“* = klíčový dodavatel
- Identifikace provozovatele (2 způsoby):
  - § 4a odst. 1: Správce, který neprovozuje svůj systém informuje provozovatelé, že je tento povinnou osobou (100 % outsorcing, možno i více provozovatelů jednoho systému)
  - § 6a odst. 1: Správce může pověřit jiného provozem KII/VIS, pokud to nevylučuje jiný zákon (částečný outsorcing, možno i více provozovatelů jednoho systému))
  - ➢ Správce informuje dodavatele, že se stává provozovatelem
- Povinnosti provozovatele
  - § 4 odst. 2 ZKB: Provozovatel zavádí bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti – na systém KII/VIS/IS ZS
  - ➢ Opatření zavadí tam, kde je nemůže zavést správce a tam, kde to po něm správce vyžaduje (za to může být požadována úhrada nákladů)

Provozovatel informačního/komunikačního systému



Identifikace provozovatele dle § 4a odst. 1 zákona



Identifikace provozovatele dle § 6a odst. 1 zákona

Zdroj: https://www.govcert.cz/cs/zkb/podpurne-materialy/

Co dále přináší novela ZKB

Co přináší novela ZKB – nové definice

- **§ 2 písm. h) – m):** definice nových povinných osob
  - provozovatel základní služby (PZS), poskytovatel digitální služby (DSP), provozovatel IS/KS
- **§ 3:** do povinných osob zahrnut pojem provozovatel (KII, VIS, PZS)
- **§ 3a**: pokud DSP nemá zástupce v členském státu EU musí jej zřídit
  - DSP, který nemá zástupce v EU a chce v ní poskytovat služby si jej musí zřídit
  - Ustaví – li zástupce v ČR, platí že v ní má sídlo a vztahuje se na něj česká právní úprava
  - Zástupce: FO/PO výslovně pověřena jednat jménem DSP ve vztahu k ZKB

Co přináší novela ZKB – dodavatelské vztahy I.

- **§ 4 odst. 5**: **KII, VIS a PZS kteří jsou orgánem veřejné moci**, jsou povinni si **s poskytovatelem cloud computingu** smluvně ošetřit vlastnictví dat a možnost jejich kontroly v reálném čase
- Ustanovení dále uvádí povinné náležitosti smluv OVM (KII/VIS/PZS) s CC:
  - Například: SLA, specifikace podmínek ukončení smlouvy, dohoda o důvěrnosti, ochrana dat, informování o incidentech, BCM, subdodavatelé…
  - Budou nutné úpravy některých smluv – ustanovení o vlastnictví informací a dat + ustanovení ohledně kontroly informací a dat
    - Vlastnictví informací a dat – koho jsou které informace/data, dostupnost a způsoby předání, předávaný formát ,atd.
    - Možnost kontroly informací a dat – ustanovení o zákaznickém auditu ze strany správce, nebo pověřené třetí strany

Co přináší novela ZKB – dodavatelské vztahy II.

- **§ 4 odst. 6**:
- Nutno si ve spojitosti se zaváděním bezp. opatření poskytovatelem cloud computungu dohodnout způsob a výši vynaložených nákladů
- **§ 4 odst. 7:**
- Zohlednění požadavků vyplývajících z bezp. pravidel není nezákonným omezením hosp. soutěže, nebo nedůvodná překážka v této soutěži

- Obsah a rozsah bezp. pravidel pro využívání cloud computingu orgány veřejné moci dále stanoví prováděcí vyhláška - **§ 6 písm. e)**

Co přináší novela ZKB – informační povinnost

- **§ 4a odst. 1 a 3**: Pokud správce KII, VIS nebo PZS není provozovatelem svého systému, musí provozovatele neprodleně a prokazatelně informovat o tom, že IS/KS byl určen a že se provozovatel stává povinným ze ZKB
  - Důvod: provozovatel (dodavatel) IS/KS musí vědět, že je provozovatelem IS/KS pod ZKB – vyplývají mu z toho povinnosti
  - Způsob: zákon neupravuje, musí být prokazatelný – datová schránka, dopis…
- **§ 4a odst. 2**: KII musí informovat své ISP o tom, že se tito ISP stávají významnou sítí
  - Důvod: Významné sítě často neví, že jsou významné sítě
  - Způsob: zákon neupravuje, musí být prokazatelný – datová schránka, dopis…

Co přináší novela ZKB – exit strategie

- **§ 6a odst. 1:** možnost pověřit jiného provozem KII/VIS, pokud to nevylučuje jiný zákon => tím se z něj stane provozovatel KII/VIS
- **§ 6a odst. 2:** povinnost provozovatele KII/VIS předat správci bezodkladně data, provozní údaje a informace, které má v souvislosti s provozem KII/VIS
- **§ 6a odst. 3**: úprava předání a ničení dat v mezi správcem a provozovatelem KII/VIS v případě ukončení spolupráce
  - Povinnost provozovatele předat v dohodnutém formátu data, provozní údaje a informace související s provozem KII/VIS
  - Povinnost provozovatel tato dat a info. po předání zničit – prokazatelně a bezpečně
    - Povinnost umožnit správci dohled nad ničením
    - Způsob likvidace dat stanoví VKB
- **§ 6a odst. 4:** právo provozovatele požadovat úhradu nákladů spojených s výše uvedeným a povinnost správce je uhradit

Co přináší novela ZKB – incidenty I.

- **§ 8 odst. 1:** Všechny povinné osoby vyjma poskytovatelů služeb el. komunikací musí hlásit incidenty, čímž není dotčena povinnost z GDPR,
- **§ 8 odst. 2**: DSP musí hlásí incident s významným dopadem na poskytování svých činností
- **§ 8 odst. 5:** Možnost přenést povinnost hlásit incident ze správce na provozovatele KII/VIS
  - Pokud Úřadu hlásí incident provozovatel, musí zároveň informovat správce
- **§ 8 odst. 6:** Možnost dobrovolného hlášení incidentů V CERTu nebo N CERTu i pro jiné než povinné osoby
- **§ 8 odst. 8:** Pokud má incident u DSP významný dopad na poskytování základní služby, hlásí to DSP Úřadu

Co přináší novela ZKB – incidenty II.

- **§ 12 odst. 3:** Právo NÚKIB informovat veřejnost o incidentu
- V případě že existuje veřejný zájem na tom aby byly zveřejněny informace o incidentů má Úřad právo informovat nebo dotčené osobě uložit aby tak učila sama
  - Krajní možnost
  - Nutnost veřejného zájmu
  - Příklad: rozsáhlý přihlašovacích údajů k internetovému bankovnictví – existuje veřejný zájem na tom, aby se o tom vědělo a uživatelé si dali pozor a hesla změnili – již nyní dělají některé subjekty dobrovolně

Co přináší novela ZKB – poskytování informací

- Změna zákona č. 106/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 106 nezná bezpečnost, jako důvod k neposkytnutí informací
  - Otázka: transparentnost na úkor bezpečnosti?

- **Prolomení z. č. 106 nově přímo v ZKB (§ 10a):**

*„Informace, jejichž zpřístupnění by mohlo **ohrozit zajišťování kybernetické bezpečnosti** nebo **účinnost opatření** vydaného podle tohoto zákona, anebo **informace, které jsou vedené v evidenci incidentů**, ze kterých by bylo možné identifikovat orgán nebo osobu, jež kybernetický bezpečnostní incident ohlásila, **se** podle předpisů upravujících svobodný přístup k informacím **neposkytují**.“*

- Potřeba stanovit co je informací, jejíž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti **=> klasifikace informací (VKB)**

Co přináší novela ZKB – předávání dat

- **§ 15a:** Pravomoc Úřadu na návrh správce KII/VIS v případě hrozícího incidentu uložit provozovateli systému předat data, provozní údaje a informace spojené se systémem
  - Povinné náležitosti návrhu: odůvodnění, popis přechozích jednání mezi správcem a provozovatelem, možné následky nepředání dat, údajů a informací
  - Povinnost předání ukládána rozhodnutím (dle správního řádu), vykonatelné dnem doručení, rozklad nemá odkladného účinku
  - Úhrada nákladů obdobná jako v § 6a/4 – účelně a prokazatelně vynaložené náklady na předání uhradí správce (navrhovatel)

Co přináší novela ZKB – povinnosti/oprávnění NÚKIB

- § 20: Vládní CERT - práva a povinnosti v souvislosti s NIS (kontaktní místo v síti CSIRT, oprávnění ve vztahu k novým povinným osobám atd.)
- § 21a: zřízení NÚKIB
- § 22: činnosti a pravomoci NÚKIB
- § 22a: určení PZS a ISZS
- § 22b: přístup NÚKIB do základních registrů a k dalším informacím

Co přináší novela ZKB - Přestupky - § 25

- Změn poměrně dost – původní znění mělo 3 odstavce, po novele jich je 13
- Zavedení nových přestupků, doplnění nových povinných osob
- Změna výše sankcí za přestupky – zvyšují se pokuty
  - Z 100 000 Kč na 1 000 000/5 000 000 Kč
  - Spodní hranice pokut nestanovena

Povinnost	sankce	Povinná osoba
Neplnění povinnosti při SKB, nápravných opatření , rozhodnutí, nepředání dat	1000 K	Siť el. komunikací, významná síť
Nebude mít smluvně ošetřené vlastnictví, ničení a předání dat	1000 K	KII, VIS
Nehlásí incidenty, neplnění rozhodnutí, nezveřejnění informací	1000 K	Významná síť, KII, VIS, PZS
Nezavede bezp. opatření	5000 K	KII,VIS, PZS
Neustaví si zástupce, neprovádí bezp. opatření, nehlásí incidenty, neplní uložené povinnosti NÚKIB	1000 K	DSP
Hlášení kontaktních údajů	10 K	Všichni
Nepředá data, nezničí data/nespolupracuje při určování	200 K	Provozovatelé IS/KS/PZS

Novela vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti
–
změny ve vyhlášce a shrnutí povinností

Adam Kučínský
Vedoucí oddělení regulace
Sekce NCKB

Národní úřad pro kybernetickou a informační bezpečnost

Přehled povinností podle ZKB

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

Cíle změn vyhlášky

- Soulad s novým zněním ZKB a směrnicí NIS,
- soulad s „best practice“,
- odstranění chyb,
- úprava některých stávajících povinností.

Průběh prací

- **Nové znění ZKB**
  - účinné od 1. 7. a 1. 8. 2017.
- **Svolání expertního týmu**
  - celkem 11 schůzí ET, vždy na min. 4 hodiny,
  - souběžná spolupráce s vládním CERT,
  - 7. 6. – 3. 10. 2017.

Průběh prací

- **Nová VKB verze I. (neoficiální verze)**
  - 6. 10. 2017.
- **Zpřístupnění nové (neoficiální) verze VKB veřejnosti**
  - možnost vyjádřit se pro každého,
  - 6. 10. – 31. 10. 2017.
- **Zapracování nových návrhů a připomínek, finalizace věcného znění**
  - 1. 11 – 1. 12. 2018.

Průběh prací

- **Poslední jednání ET Nová VKB verze II. (neoficiální verze) + připomínky veřejnosti**
  - 20. 12. 2018
- **Předání VKB právnímu oddělení NÚKIB, finalizace za NÚKIB**
  - 15.01.2018
- **Nová VKB verze III.**
  - 01. 02. 2018
- **Legislativní proces**
  - 16. 02. 2018 – až nyní
- **Snaha o účinnost vyhlášky od 10. 05. 2018**

Co bude jinak

- Bezpečnostní opatření povinně **nově zavádí**:
  - správce **a provozovatel IS KII**,
  - správce **a provozovatel KS KII**,
  - správce **a provozovatel VIS**,
  - **správce a provozovatel IS ZS**,
  - *DSP*

Co bude jinak

- **Pořadí některých §**
- **Úprava formulací**
  - odstranění duplicit,
  - přeformulování názvů některých §, požadavků…
- **Logické úpravy některých povinností**
  - zjednodušení, odstranění, přidání…

Co bude jinak

- **Větší soulad s „best practice“**
  - požadavky i terminologie
- **Nové přílohy**
  - likvidace dat,
  - hrozby a zranitelnosti,
  - bezpečnostní role a jejich kompetence,
  - bezpečnostní opatření pro smluvní vztahy.

Co bude jinak

- 1/2 Organizační opatření:
  - § 3 Systém řízení bezpečnosti informací
  - § 4 Řízení aktiv
  - § 5 Řízení rizik
  - § 6 Organizační bezpečnost
  - § 7 Bezpečnostní role
  - § 8 Řízení dodavatelů
  - § 9 Bezpečnost lidských zdrojů
  - § 10 Řízení provozu a komunikací
  - § 11 Řízení změn

Co bude jinak

- 2/2 Organizační opatření:
  - § 12 Řízení přístupu
  - § 13 Akvizice, vývoj a údržba
  - § 14 Zvládání kybernetických bezpečnostních událostí a incidentů
  - § 15 Řízení kontinuity činností
  - § 16 Audit kybernetické bezpečnosti
  - § 30 Bezpečnostní politika a bezpečnostní dokumentace

Co bude jinak

- 1/2 Technická opatření:
  - § 17 Fyzická bezpečnost
  - § 18 Bezpečnost komunikačních sítí
  - § 19 Správa a ověřování identit
  - § 20 Řízení přístupových oprávnění
  - § 21 Ochrana před škodlivým kódem
  - § 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
  - § 23 Detekce kybernetických bezpečnostních událostí

Co bude jinak

- 2/2 Technická opatření:
  - § 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí
  - § 25 Aplikační bezpečnost
  - § 26 Kryptografické prostředky
  - § 27 Zajišťování úrovně dostupnosti informací
  - § 28 Průmyslové, řídící a obdobné specifické systémy

Děkuji za pozornost

Adam Kučínský

a.kucinsky@nukib.cz