Zákon o kybernetické bezpečnosti a jeho dopad na provozovatele telekomunikačních sítí

Adam Kučínský
Odbor regulace

Národní úřad
pro kybernetickou
a informační bezpečnost

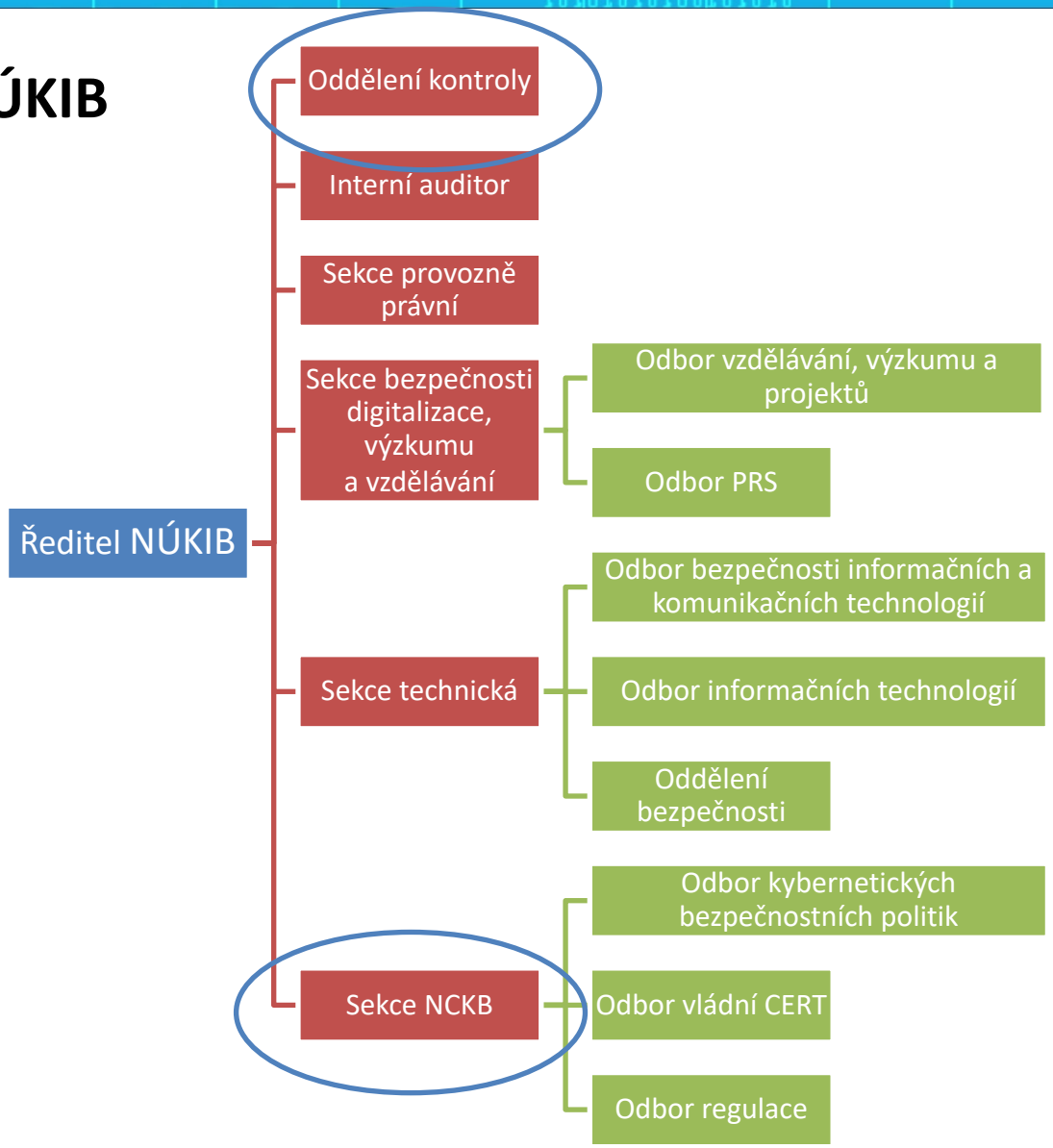
Disclaimer

- Prezentace obsahuje informace platné ke dni její realizace, tedy k 17. 4. 2019.
- Informace, fakta a údaje obsažené v prezentaci mají informační a osvětový charakter.
- Pro zajištění souladu se zákonem o kybernetické bezpečnosti je nutno vycházet z aktuálně účinné legislativy. Aplikaci takových informací či opatření je nutné vždy vztahovat ke konkrétním systémům a institucím.

Národní úřad pro kybernetickou a informační bezpečnost

- Ústřední správní orgán pro:
  - kybernetickou bezpečnost
  - ochranu utajovaných informací v oblasti informačních a komunikačních systémů
  - kryptografickou ochranu
  - problematiku neveřejné služby v rámci družicového systému Galileo
- Služby NÚKIB v oblasti kybernetické bezpečnosti:
  - provoz Vládního CERT České republiky
  - spolupráce s ostatními CERT A CSIRT
  - osvěta a podpora vzdělávání
  - ochrana utajovaných informací v oblasti IS/KS
  - kryptografická ochrana

Struktura NÚKIB



Odbor kybernetických bezpečnostních politik

- Připravuje dlouhodobou strategii a poskytuje analýzu, a potřebnou expertízu, aby ČR plnila všechny stanovené cíle v oblasti zajišťování kybernetické bezpečnosti, a to co nejefektivnějším způsobem
- Kybernetická cvičení (technická i netechnická - Table Top)
- Příprava strategických analýz
- Zastupování ČR v EU, NATO, OBSE
- Tvorba (**netechnických**) analytických materiálů a strategických briefingů k hrozbám a trendům v oblasti KB

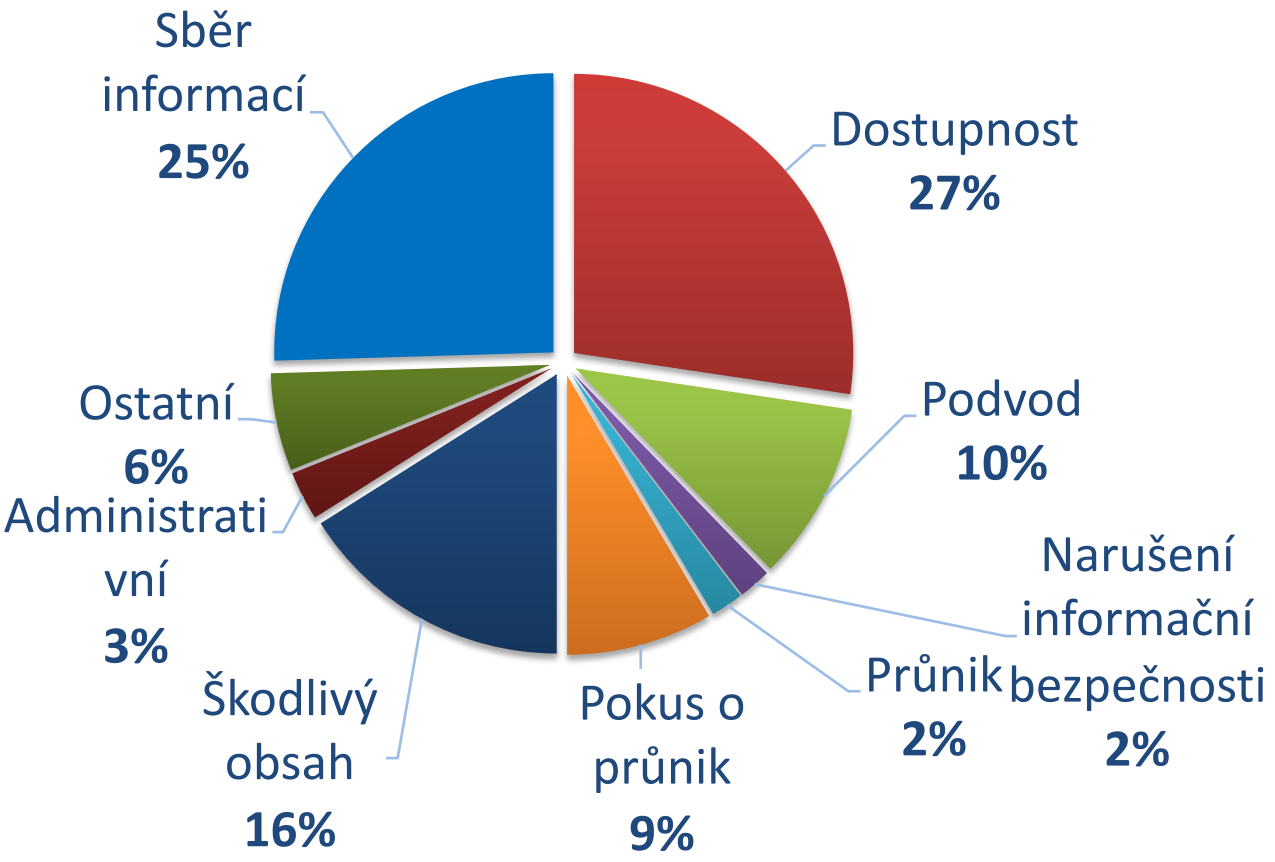
Vládní CERT

- Primární zaměření: veřejný sektor, kritická informační infrastruktura, provozovatelé základních služeb
- Koordinační tým (nejedná se o interní typ)
- Struktura týmu:
  - Zpracování incidentů
  - Vývoj a bezpečnostní testování
  - Síťová bezpečnost
  - Analytická skupina
- Základní služby:
  - Reaktivní: zpracování a řešení incidentů, zpracování artefaktů a analýza dat
  - Detekční: detekce anomálií, zpracování indikátorů kompromitace
  - Proaktivní: koordinace v rámci české bezpečnostní komunity a sdílení informací, penetrační testování, kybernetická cvičení a další

Vládní CERT

- Hlášené incidenty - přibližně 30 měsíčně
- Stabilní trend

Klasifikace incidentů



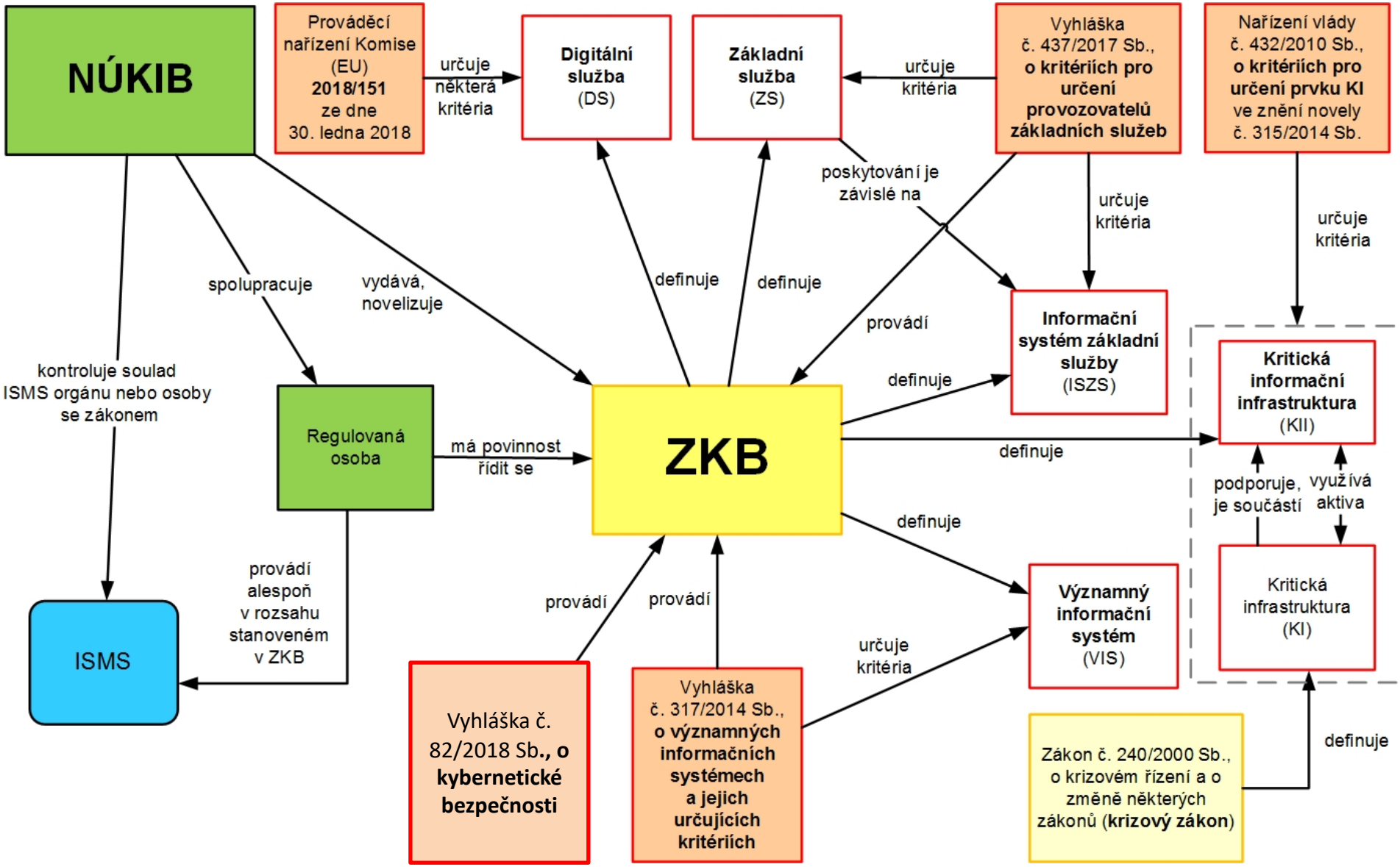
Oddělení kontroly

- Kontrola povinností povinných subjektů dle ZKB
- Metodická pomoc

- Kontrola dodržování ZKB
  - přistupujeme k ní podobně jako k auditu systému řízení bezpečnosti informací podle ISO 27 001, což přináší přidanou hodnotu i pro regulované subjekty
  - **v roce 2016 bylo 80 % kontrolovaných v nesouladu, od té doby jsou patrná významná zlepšení**
- Prozatím neprovádíme kontrolu dodržování ZKB u jiných, než KII/VIS subjektů.

Odbor regulace

- Určování povinných osob
  - KII, PZS, podpora identifikace poskytovatelů digitálních služeb a VIS
- Výklad zákona o kybernetické bezpečnosti a souvisejících právních předpisů
  - Zodpovídání dotazů k problematice aplikace ZKB
  - Spolupráce s OK v zodpovídání dotazů na požadavky ZKB a VKB
- Poskytování metodické podpory
  - Tvorba podpůrných materiálů dostupných na webu


NÚKIB
Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018
určuje některá kritéria
Digitální služba (DS)
Základní služba (ZS)
určuje kritéria
Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb
Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku KI ve znění novely č. 315/2014 Sb.
poskytování je závislé na
určuje kritéria
určuje kritéria
spolupracuje
vydává, novelizuje
definuje
definuje
provádí
Informační systém základní služby (ISZS)
definuje
kontroluje soulad ISMS orgánu nebo osoby se zákonem
Regulovaná osoba
má povinnost řídit se
ZKB
definuje
Kritická informační infrastruktura (KII)
podporuje, je součástí
využívá aktiva
Kritická infrastruktura (KI)
definuje
provádí alespoň v rozsahu stanoveném v ZKB
ISMS
provádí
provádí
Významný informační systém (VIS)
určuje kritéria
Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti
Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)
definuje

Zákon o kybernetické bezpečnosti

- Upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti
- Obsahuje základní nezbytné definice
- Transponuje směrnici NIS
- Cílem je stanovit:
  - základní úroveň bezpečnostních opatření,
  - zlepšit detekci a zavést hlášení kybernetických bezpečnostních incidentů,
  - zavést systém opatření k reakci na kybernetické bezpečnostní incidenty
  - upravit činnost dohledových pracovišť
- Zavádí stav kybernetického nebezpečí
- Zřizuje Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Dohledová pracoviště v ČR podle ZKB

- Vládní CERT a Národní CERT
  - Hlavní úkol:
    - vyhodnocování kybernetické bezpečnostní situace v informačních a komunikačních systémech
    - ochrana těchto systémů před kybernetickými bezpečnostními incidenty
  - Základním smyslem fungování dohledových pracovišť je vyhodnocování informací o výskytu kybernetických bezpečnostních incidentů z pokud možno co největšího množství informačních a komunikačních systémů
  - Rozdělení gesce v kyberprostoru
    - Soukromoprávní X Veřejnoprávní podstata
  - Spolupráce
- Vedle těchto existují i další CERT

Národní CERT

- Osoba soukromého práva
- Bez nařizovacích nebo sankčních pravomocí
- Kontaktní místo pro některé povinné osoby ZKB zejména pro osoby soukromého práva (ne nutně - viz dále)
- K vyhodnocování a metodické podpoře subjektů, které aktivně projeví zájem o výhody kolektivní ochrany před kybernetickými bezpečnostními incidenty

- K výkonu své činnosti oprávněn na základě veřejnoprávní smlouvy uzavírané s Úřadem
  - vybrán Úřadem v řízení o výběru žádosti podle správního řádu
- V současné době jej provozuje sdružení CZ.NIC

Struktura povinných podle ZKB

- §3 ZKB

a)	poskytovatelé služeb elektronických komunikací, subjekt zajišťující sít elektronických komunikací	NÁRODNÍ CERT *CZ.NIC*
b)	orgán nebo osoba zajišťující významnou síť	
h)	Poskytovatel digitálních služeb	
c)	správce *a provozovatel* IS KII	VLÁDNÍ CERT *NÚKIB*
d)	správce *a provozovatel* KS KII	
e)	správce *a provozovatel* VIS	
f)	správce a provozovatel IS základní služby	
g)	provozovatel základní služby	

Pozn.: Písmena odpovídají písmenům v ZKB

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
  - **Pouze povinnost hlásit kontaktní údaje**

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 definicí v ZKB
- Sféra Národního CERTu
  - Povinnost hlásit kontaktní údaje
  - Povinnost detekovat kybernetické bezpečností události
  - Povinnost hlásit incidenty
- Změny v souvislosti s novelami ZKB neprobíhaly

Provozovatel základní služby

- **Základní službou je:**
  - služba, jejíž **poskytování je závislé na informačních systémech nebo sítích elektronických komunikací** a
  - jejíž **narušení by mohlo mít významný dopad** na zabezpečení společenských nebo ekonomických činností
  - **v některém z odvětví:** energetiky, dopravy, bankovnictví, infrastruktury finančních trhů, zdravotnictví, vodního hospodářství, digitální infrastruktury nebo chemického průmyslu**.**
- **Postup určení**
  - NÚKIB **vytipuje s pomocí kritérií** ve vyhlášce č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby relevantní subjekty, které osloví a zahájí správní řízení o jejich určení.
  - Proběhnou **jednání** mezi NÚKIB a určovaným subjektem.
  - Určování je správním řízením

Příloha vyhlášky č. 437/2017 Sb. – 5. Zdravotnictví

5. Zdravotnictví

Odvětvová kritéria			Dopadová kritéria
Druh služby	**Druh subjektu**	**Speciální kritéria druhu subjektu**	
5.1. Poskytování zdravotních služeb	Poskytovatel zdravotních služeb podle zákona o zdravotních službách	a) Celkový počet akutních lůžek v posledních třech kalendářních letech nejméně 800 nebo b) statut centra vysoce specializované traumatologické péče podle zákona o zdravotních službách.	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 50000 osob, II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury, III. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů, IV. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření, V. 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, nebo VI. kompromitaci citlivých osobních údajů o více než 200000 osobách.

Kritická informační infrastruktura (KII)

- KII = Prvek nebo systém prvků **kritické infrastruktury (KI)** v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti (§ 2 písm. b) ZKB)
- Komplex informačních a komunikačních systémů, jejichž narušení by mohlo způsobit **závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu** (§ 2 písm. g, krizového zákona)
- Určena podle stanovených **průřezových** a **odvětvových kritérií v oblasti kybernetické bezpečnosti** (§ 2 písm. i), krizového zákona, NV 432/2010 Sb.,)
- Stejně jako KI se týká veřejnoprávních i soukromoprávních subjektů

Kritická informační infrastruktura (KII)

- Systémy důležité pro chod státu a ekonomiky
- Sféra Vládního CERTu
- Určuje/navrhuje NÚKIB
- Nejpřísnější regulace – povinnost plnit celý ZKB:
  - Hlásí kontaktní údaje
  - Detekuje a hlásí incidenty
  - Povinnost zavést bezpečností opatření podle vyhlášky č. 82/2018 Sb.
  - Provádí ochranná a reaktivní opatření vydaná NÚKIB

Poskytovatel digitální služby (DSP)

- **Poskytovatel digitální služby** (§ 3 písm. h) ZKB).

- digitální službou služba informační společnosti podle zákona upravujícího některé služby informační společnosti, která spočívá v provozování
- 1. on-line tržiště,
- 2. internetového vyhledávače,
- 3. cloud computingu.
- Určení:
  - **orgán nebo osoba** posoudí naplnění kritérií a **nahlásí se jako povinná osoba Národnímu CERT**
- Regulace se netýká malých a mikro podniků
  - <50 zaměstnanců a roční bilanční suma nebo obrat <10 mil. €
- Funguje zde princip samourčení – naplnění definice = povinná osoba
- Prováděcí nařízení Komise č. 2018/151 – stanovuje povinnosti subjektů
- Maximální harmonizace

Významný informační systém

- **Významným informačním systémem** se rozumí informační systém **spravovaný orgánem veřejné moci**, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého **narušení bezpečnosti informací může omezit** nebo **výrazně ohrozit výkon působnosti orgánu veřejné moci**.
- Pouze státní sektor
- Postup určení:
  - **orgán nebo osoba** posoudí naplnění kritérií dle vyhlášky č. 317/2014 Sb. a **nahlásí se jako povinná osoba NÚKIB**

    nebo
  - **informační systém je zahrnut do přílohy vyhlášky č. 317/2014 Sb.**

Správce a provozovatel

- **Správcem informačního systému základní služby** (§ 3 písm. f)) je ten, kdo určuje účel zpracování informací a podmínky jeho provozování.
  - tj. ten, kdo systém „vlastní“
  - vždy jen jeden subjekt
- **Provozovatelem informačního systému základní služby** (§ 3 písm. f)) je ten, kdo **zajišťuje funkčnost technických** (hardware) **a programových** (software) **prostředků** jej tvořících.
  - tj. „důležití“ nebo „hlavní“ dodavatelé
  - jeden nebo více subjektů
  - Pouze u KII, VIS, PZS

Přehled povinností podle ZKB

- Nahlášení kontaktních údajů (§16 ZKB)
  - Všechny povinné osoby
  - KII, VIS, PZS – vládní CERT,
  - Sítě elektronických komunikací a významné sítě, DSP – Národní CERT
- Hlášení kybernetických bezpečnostních incidentů (§8 ZKB)
  - KII, VIS, významné sítě, PZS
  - významné sítě, DSP – Národní CERT
- Zavedení bezpečnostních opatření (standardizace) (§4 ZKB)
  - KII, VIS, PZS, DSP pouze některá opatření
- Opatření vydané NÚKIB (§11 ZKB)
  - Varování, reaktivní opatření, ochranné opatření
  - KII, VIS, PZS
  - Významné sítě a poskytovatelé služby el. komunikací pouze za stavu kybernetického nebezpečí, pouze reaktivní opatření

Varování podle § 12 ZKB
-
použití a dopady

Institut Varování

§ 12 ZKB – Varování

(1) **Úřad vydá varování**, **dozví-li se** zejména 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**.

(2) Varování **Úřad zveřejní na svých internetových stránkách a oznámí je orgánům a osobám uvedeným v § 3**, jejichž kontaktní údaje jsou vedeny v evidenci podle § 16 odst. 4.

Co varování znamená

- Prostřednictvím varování NÚKIB **upozorňuje na existenci hrozby** v oblasti kybernetické bezpečnosti, na kterou je nutné bezprostředně reagovat.
- **Subjekty,** které spadají pod zákon ZKB, **jsou povinny se touto hrozbou dále zabývat a zohlednit ji v analýze rizik**, kterou v souladu s požadavky ZKB a příslušné vyhlášky již pravidelně provádí.
- Varování neznamená bezpodmínečný zákaz používání daných technických a programových prostředků, ale nutnost zvážit případné bezpečnostní riziko související s jejich užíváním.
- Dovolí-li to výsledky analýzy rizik, uvedené technické nebo programové prostředky je možné i nadále používat.
- **Orgánům a osobám, kterým ZKB neukládá povinnost zavést a provádět bezpečnostní opatření, stejně tak jako široké veřejnosti, nezakládá varování NÚKIB povinnosti**. Tyto subjekty tedy nejsou podle ZKB povinny varování NÚKIB zohlednit. Další kroky s tím spojené jsou pouze na nich.

Implementace varování

- KII, VIS a PZS jsou povinni podle § 5 VKB pro určené IS a KS provádět pravidelnou analýzu rizik, identifikovat rizika a identifikovaná rizika řídit.
- Na základě vyhodnocení rizik potom výše uvedené subjekty zavádějí a provádějí bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti v souladu s § 4 odst. 2 ZKB.
- Bezpečnostní opatření jsou blíže specifikována ve VKB.
- V souvislosti s řízením rizik musejí podle § 5 odst. 1 písm. h) bod 3 VKB tyto subjekty zohlednit mimo jiné i opatření podle § 11 ZKB, tedy i varování vydané podle § 12 ZKB.
- **Na základě vydaného varování tedy musejí výše zmíněné povinné osoby v rámci zavedeného řízení rizik provést analýzu rizik, ve které zohlední hrozbu, a následně na riziko reagovat přijetím bezpečnostních opatření, která musí být v souladu s nastavenými metrikami pro akceptovatelnost rizika a hodnotou daného rizika.**

Děkuji Vám za pozornost

regulace@nukib.cz