



MUNI
LAW



KYBERNETICKÁ BEZPEČNOST V ČR

VÁCLAV STUPKA

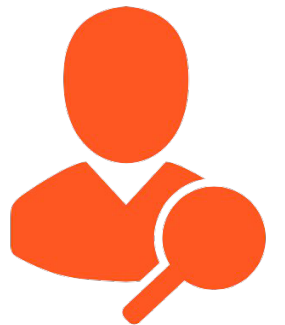
2 REGULATORNÍ MODELY

Identifikační model

- USA, některé jihoamerické státy
- Efektivní, univerzální
- Vysoká míra zásahu do informačního soukromí – politická citlivost
- Problém výpadků
- Nedostatek mezinárodní podpory

Model ochrany prostředí

- EU, ČR
- Méně efektivní, institucionální oddělení
- Performativní pravidla, chytrá regulace
- Menší zásah do informačního soukromí



RELEVANTNÍ LEGISLATIVA

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
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb

Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku KI

Zákonč. 365/2000 Sb. o IS veřejné správy (orgány veřejné moci) (ISVS)

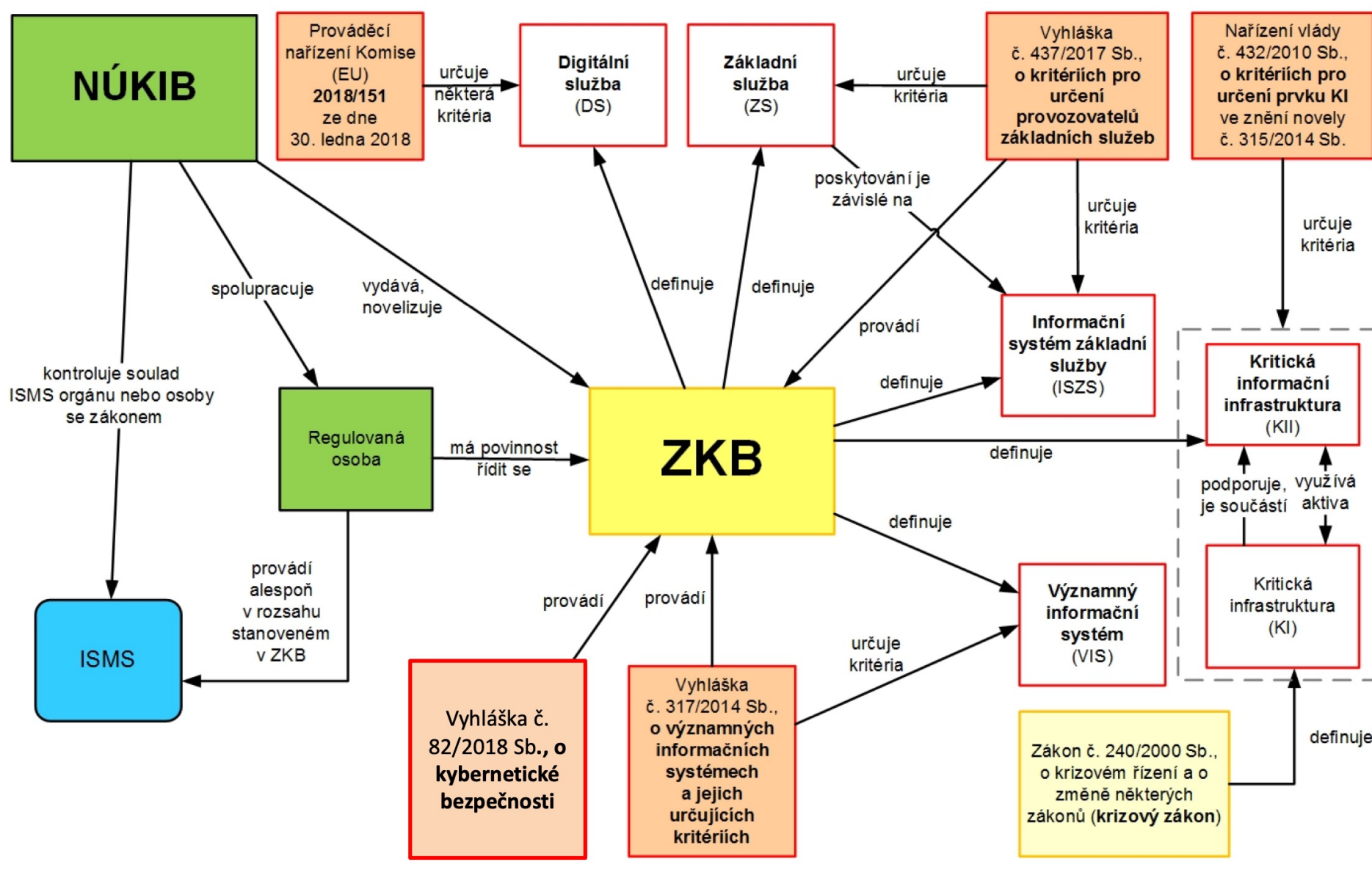
Směrnice (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS)

- Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018

Nařízení (EU) 2019/881 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti“)

Sektorová regulace (energetika, zdravotnická dokumentace, bankovní a finanční služby), obecná regulace (osobní údaje, utajované informace)







INSTITUCIONÁLNÍ ZAJIŠTĚNÍ

INSTITUCIONÁLNÍ ZAJIŠTĚNÍ

NÚKIB – Národní úřad pro
kybernetickou a informační
bezpečnost

- NCKB – Národní centrum pro kybernetickou bezpečnost
- GovCERT – Vládní CERT

CSIRT.CZ

- Csirt.cz – Národní CERT



Ústřední správní orgán pro:

- Kybernetickou bezpečnost
- Ochranu utajovaných informací v oblasti informačních a komunikačních technologií
- Kryptografickou ochranu
- Problematiku neveřejné služby v rámci družicového systému Galileo

Služby NÚKIB v oblasti kybernetické bezpečnosti

- Provoz Vládního CERT ČR
- Spolupráce s ostatními CERT a CSIRT
- Osvěta a podpora vzdělávání
- Ochrana utajovaných informací v IS/KS
- Kryptografická ochrana

NÚKIB



CSIRT.CZ



- Osoba soukromého práva
- Bez nařizovacích a sankčních pravomocí
- Kontaktní místo pro některé povinné osoby podle ZoKB
- Poskytuje služby vyhodnocování a metodické podpory pro subjekty, které aktivně projeví zájem o výhody kolektivní ochrany před KBI
- K výkonu své činnosti oprávněn prostřednictvím veřejnoprávní smlouvy uzavřené s NÚKIB
- V současné době jej provozuje CZ.NIC





INSTITUTY ZOKB

INSTITUTY



Obecné povinnosti:

Kontaktní údaje
Bezpečnostní opatření
(organizační a technická)



Operativní povinnosti

Hlášení incidentů
Varování
Protiopatření (reaktivní a
ochranná)



Stav kybernetického nebezpečí



Požadavky na dodavatele



Certifikace



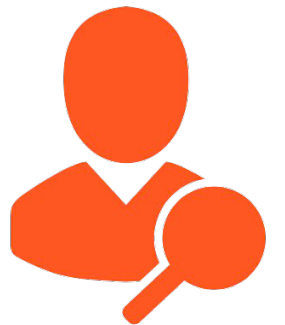
BEZPEČNOSTNÍ OPATŘENÍ

- Organizačními opatřeními jsou
 - 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, zvládnání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, řízení kontinuity činností a kontrola a audit kritické informační infrastruktury a významných informačních systémů.
- Technickými opatřeními jsou
 - 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 bezpečnostních událostí, nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí, aplikační bezpečnost, kryptografické prostředky, nástroj pro zajišťování úrovně dostupnosti informací a bezpečnost průmyslových a řídicích systémů.



VAROVÁNÍ

- §12
 - (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.
- Upozornění na existence hrozeb
- Povinnost hrozby zohledňovat -> analýza rizik
- Není vyžadována konkrétní akce



- **Kybernetickým bezpečnostním incidentem** je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací
- Povinná detekce a bezodkladného hlášení KBI (možná kombinace s dalšími oznamovacími povinnostmi)
- Klasifikace incidentů a formální požadavky na hlášení

HLÁŠENÍ KBI

Formulář hlášení kybernetického bezpečnostního incidentu	
HLÁŠENÍ KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU	
MÍRA OCHRANY INFORMACE	
Úroveň ochrany	
	Osobní – seznam příjemců Omezená distribuce Neomezeno
KONTAKTNÍ ÚDAJE	
Orgán a osoba uvedená v § 3 písm. c) až e) zákona	
Email	
Telefon	
DETAILY INCIDENTU	
Datum a čas zjištění	
Časová zóna	
Kategorie incidentu	Kategorie III – velmi závažný kybernetický bezpečnostní incident Kategorie II – závažný kybernetický bezpečnostní incident Kategorie I – méně závažný kybernetický bezpečnostní incident
Typ incidentu	Kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb. Kybernetický bezpečnostní incident způsobený škodlivým kódem. Kybernetický bezpečnostní incident způsobený překonáním technických opatření. Kybernetický bezpečnostní incident způsobený porušením organizačních opatření. Kybernetický bezpečnostní incident spojený s projevem trvale působících hrozeb. Ostatní kybernetické bezpečnostní incidenty způsobené kybernetickým útokem. Kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv. Kybernetický bezpečnostní incident způsobující narušení integrity primárních aktiv.

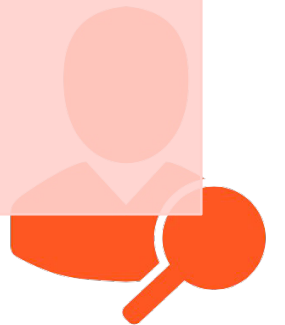
REAKTIVNÍ A OCHRANNÁ OPATŘENÍ

Reaktivní

- v reakci na KBI
- Rozhodnutí, nebo opatření obecné povahy
- Oznámení o provedení opatření

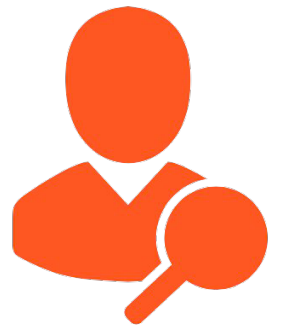
Ochranná

- V reakci na výsledek analýzy KBI
- Opatření obecné povahy



STAV KYBERNETICKÉHO NEBEZPEČÍ

- = stav, ve kterém je **ve velkém rozsahu ohrožena bezpečnost informací** v informačních systémech **nebo bezpečnost služeb elektronických komunikací** anebo **bezpečnost a integrita sítí elektronických komunikací**, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací.
- Rozhoduje ředitel NÚKIB
- Povinnost zveřejnění
- Max 7/30 dnů
- Rozšíření působnosti reaktivních protiopatření
- Možnost navazujícího nouzového stavu

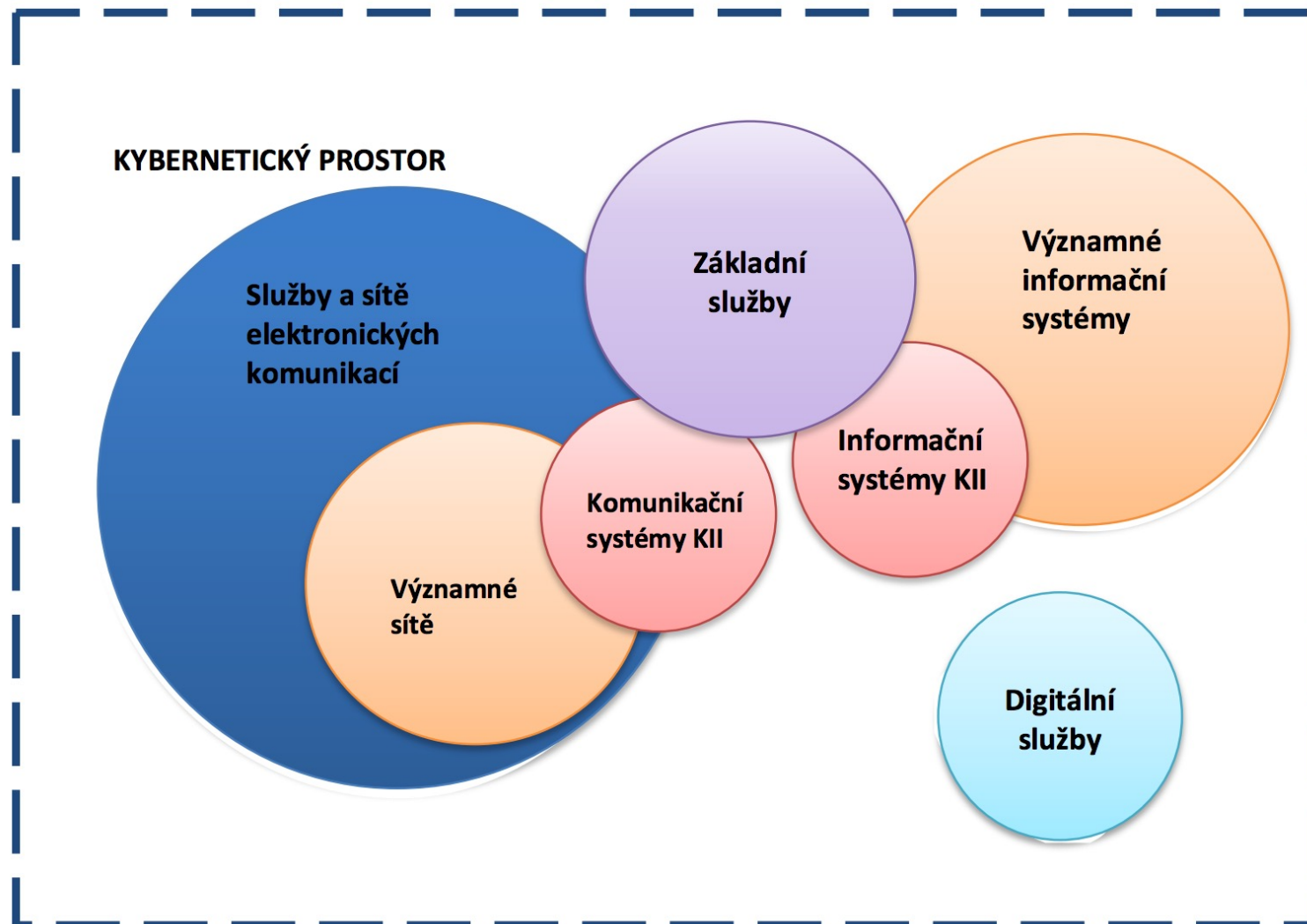




POVINNÉ OSOBY

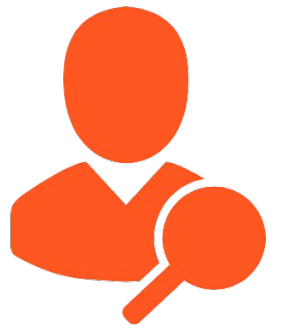
ZOKB

POVINNÉ OSOBY



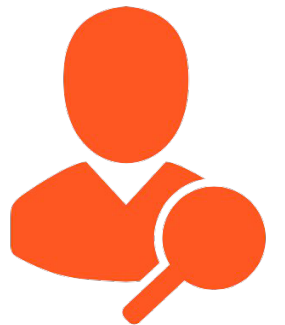
SLUŽBY A SÍTĚ ELEKTRONICKÝCH KOMUNIKACÍ

- Zákon č. 127/2005 Sb., o elektronických komunikacích
 - §2 písm. f) ZEK – „zajišťování sítě elektronických komunikací zřízení
 - §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



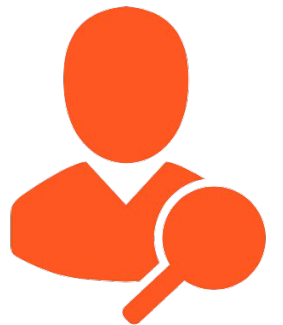
VÝZNAMNÉ SÍTĚ

- §2 písm. g ZKB
- „sít' 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
- Povinnosti:
 - Povinnost hlásit kontaktní údaje
 - Povinnost detekovat kybernetické bezpečností události
 - Povinnost hlásit incidenty



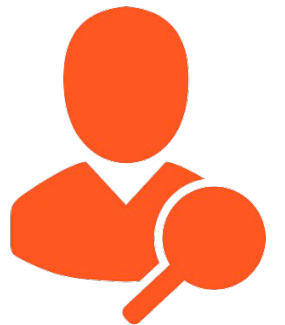
KRITICKÁ INFORMAČNÍ INFRASTRUKTURA

- 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



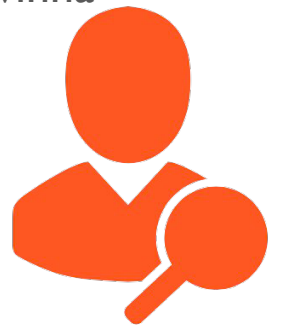
KRITICKÁ INFORMAČNÍ INFRASTRUKTURA

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



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.

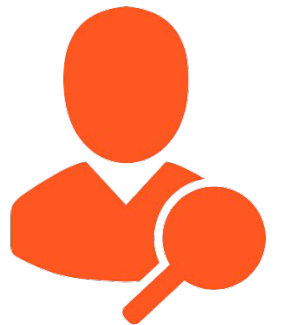


ZÁKLADNÍ SLUŽBY

- “služba, jejíž poskytování je závislé na informačních systémech nebo sítích elektronických komunikací a o jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností o v některém z odvětví”:
 - energetiky, dopravy, bankovníctví, infrastruktury finančních trhů, zdravotnictví, vodního hospodářství, digitální infrastruktury nebo chemického průmyslu
- Postup určení:
 - NÚKIB vtipuje 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

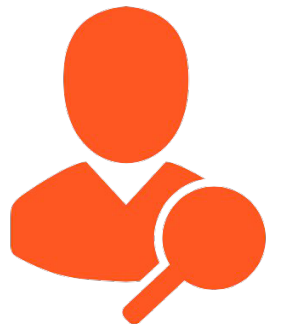
5. Zdravotnictví

Odvětová 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 nepřímých 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.



DIGITÁLNÍ SLUŽBY

- 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 $\emptyset < 50$ 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



POVINNOSTI

<i>Povinné osoby</i>	<i>Bezpečnostní opatření</i>	<i>Detekce a hlášení KBI</i>	<i>Reaktivní opatření</i>	<i>Ochranné opatření</i>	<i>Kontaktní údaje</i>
<i>Poskytovatel/zajišťující služby a sítě el. komunikací</i>	NE	NE	NE/ANO*	NE	ANO – národní CERT
<i>Orgán/osoba zajišťující významné sítě</i>	NE	ANO – národní CERT	NE/ANO*	NE	ANO – národní CERT
<i>Správce informačního systému KII</i>	ANO	ANO – NÚKIB	ANO	ANO	ANO - NÚKIB
<i>Správce komunikačního systému KII</i>	ANO	ANO – NÚKIB	ANO	ANO	ANO – NÚKIB
<i>Správce významného informačního systému</i>	ANO	ANO – NÚKIB	ANO	ANO	ANO – NÚKIB
<i>Správce informačního systému základní služby</i>	ANO	ANO – NÚKIB	NE	NE	ANO - NÚKIB
<i>Poskytovatel digitální služby</i>	ANO	ANO- národní CERT	NE	NE	ANO – národní CERT





**DÍKY ZA
POZORNOST**

STUPKA@NC3.CZ