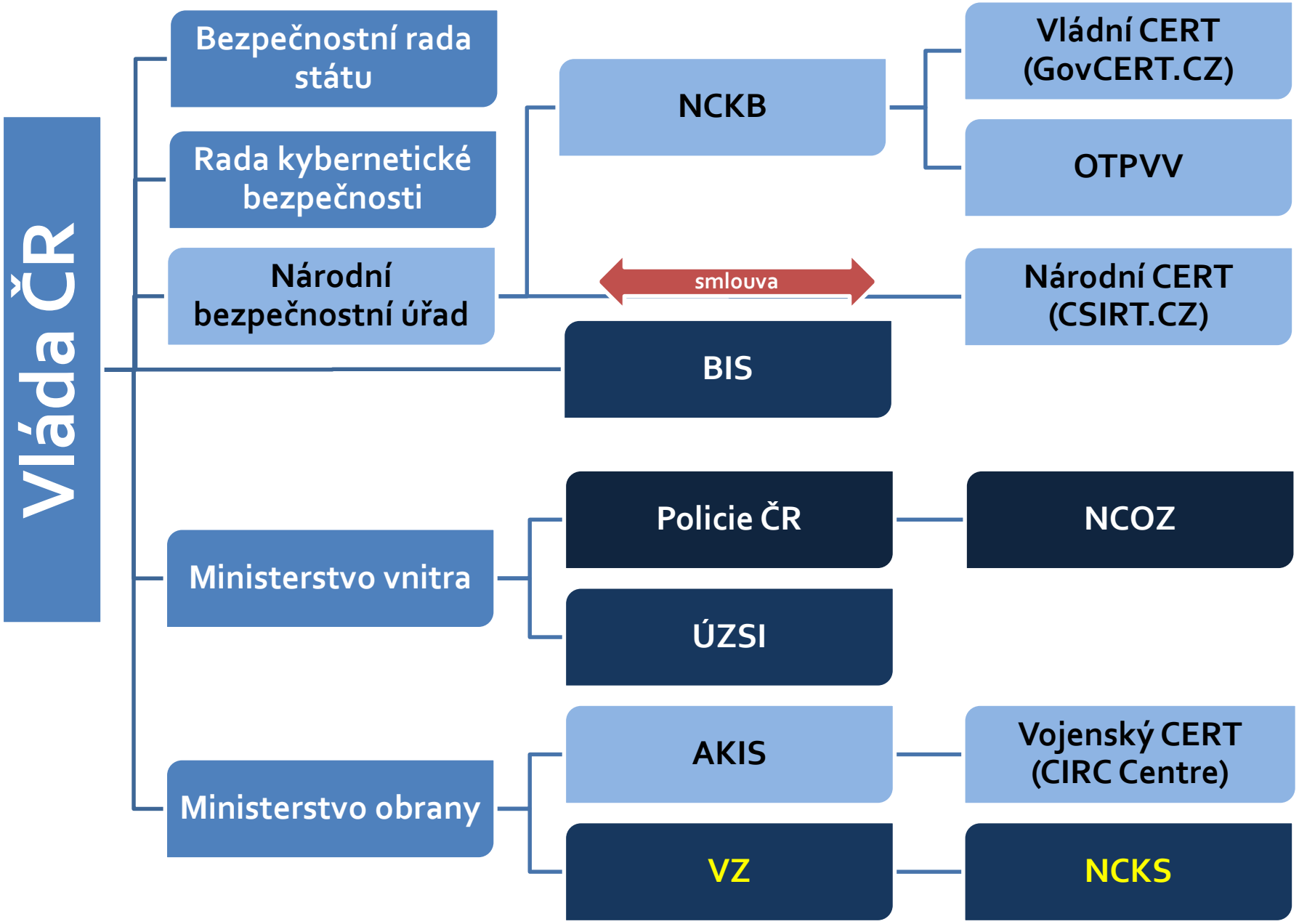
KYBERNETICKÁ BEZPEČNOST V ČESKÉ REPUBLICE

Aktuální situace

Jaroslav Šmíd
náměstek ředitele NBÚ

ORGANIZAČNÍ RÁMEC



Kybernetická bezpečnost/obrana/kriminalita – český přístup

- **BEZPEČNOST** – zastřešujícím termínem pro široké spektrum bezpečnostních oblastí, zahrnuje všechny preventivní a reaktivní aktivity státu v oblasti ochrany dat, informací, systémů, služeb a sítí ve smyslu neustálého navyšování integrity, odolnosti a robustnosti **státní** informační infrastruktury a infrastruktury pro **kritickou** informační infrastrukturu

- **OBRANA** – ochrana státu výhradně proti pokročilým, závažným, nepřátelským kybernetickým útokům (tj. proti jakýmkoliv aktivitám, které mohou narušit státní integritu a suverenitu nebo hrozbám působícím proti národním strategickým zájmům a ekonomické prosperitě země) Mezi kybernetickou bezpečností a obranou rozlišujeme v závislosti na:
  1. povaze hrozby
  2. a typu kybernetického útoku a jeho cíli

- **KRIMINALITA** – trestná činnost, pro kterou je určující vztah k software, k datům, respektive uloženým informacím, respektive veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat

NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI:

- Odbor vládní CERT

- Odbor kybernetických bezpečnostních politik

GOVCERT.CZ

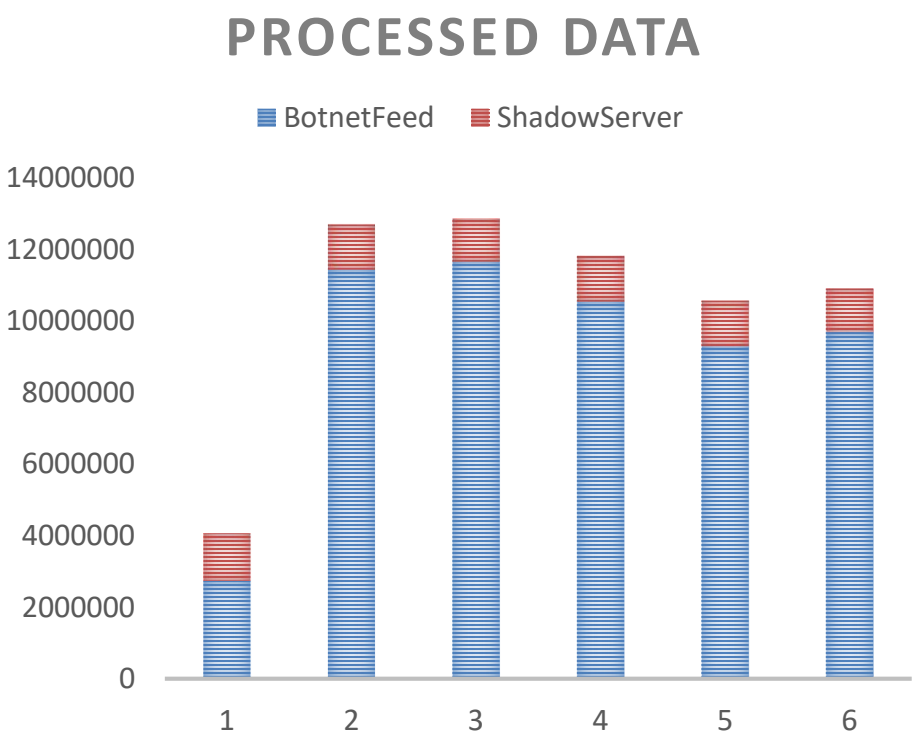
- Veřejný sektor a kritická informační infrastruktura
- Členění týmu
  - Reaktivní oddělení
  - Vývoj a bezpečnostní testování
  - Oddělení síťové analýzy
  - Analytické oddělení
- Základní služby
  - Proaktivní: koordinační činnost v rámci komunity a informační HUB
  - Detekční: schopnosti detekce anomálií
  - Reaktivní: reakce na incidenty, zpracování artefaktů
- Zaměření týmu
  - SCADA/ICS systémy
  - Penetrační testování
  - Forenzní činnost
  - Analýza malwaru a reverzní inženýrství
  - …

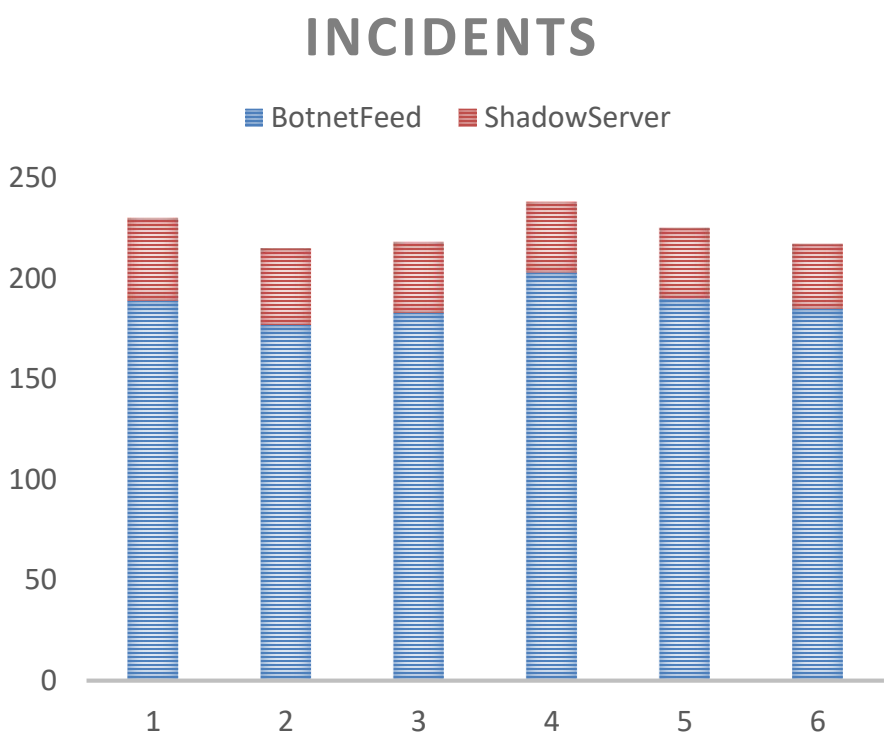
AKTUÁLNÍ TRENDY

- Rozsáhlé phishingové kampaně
- Locky Ransomware
- Ransomware ve formě výhružných emailů
  - Výhružky formou DDoS útoků, exfiltrace dat, atd.
- Velké množství škodlivého kódu
- Aktivity skupiny Anonymous

INCIDENTY ZA ROK 2016

- Hlášené incidenty cca 60 měsíčně
- Rostoucí trend





AKTUÁLNÍ PROJEKTY

- Koordinační centrum pro české bezpečnostní týmy
  - Videokonference se stálými i ad-hoc členy
  - Řešení rozsáhlých bezpečnostních útoků
- Nový webový portál
  - Veřejná a neveřejná část
  - Neveřejné fórum pro bezpečnostní týmy a další organizace
- Příprava technického cvičení Cyber Czech 2016
  - Red/blue tým cvičení s více než 60 účastníky
  - Unikátní cvičení v Evropě
- Forenzní laboratoř a penetrační testování

Odbor kybernetických bezpečnostních politik

Netechnické pracoviště

- plnění mezinárodních závazků
- mapování a určování KII a VIS
- vytváření a aktualizace strategických a dalších zásadních dokumentů

PLNĚNÍ MEZINÁRODNÍCH ZÁVAZKŮ

- **EU** – kybernetická diplomacie, NIS směrnice, atd.
- **ENISA** – členství v ENISA Management Board, zástupce v expertní skupině na národní strategie kybernetické bezpečnosti
- **OSCE** – opatření pro zvyšování důvěry mezi státy v kyberprostoru

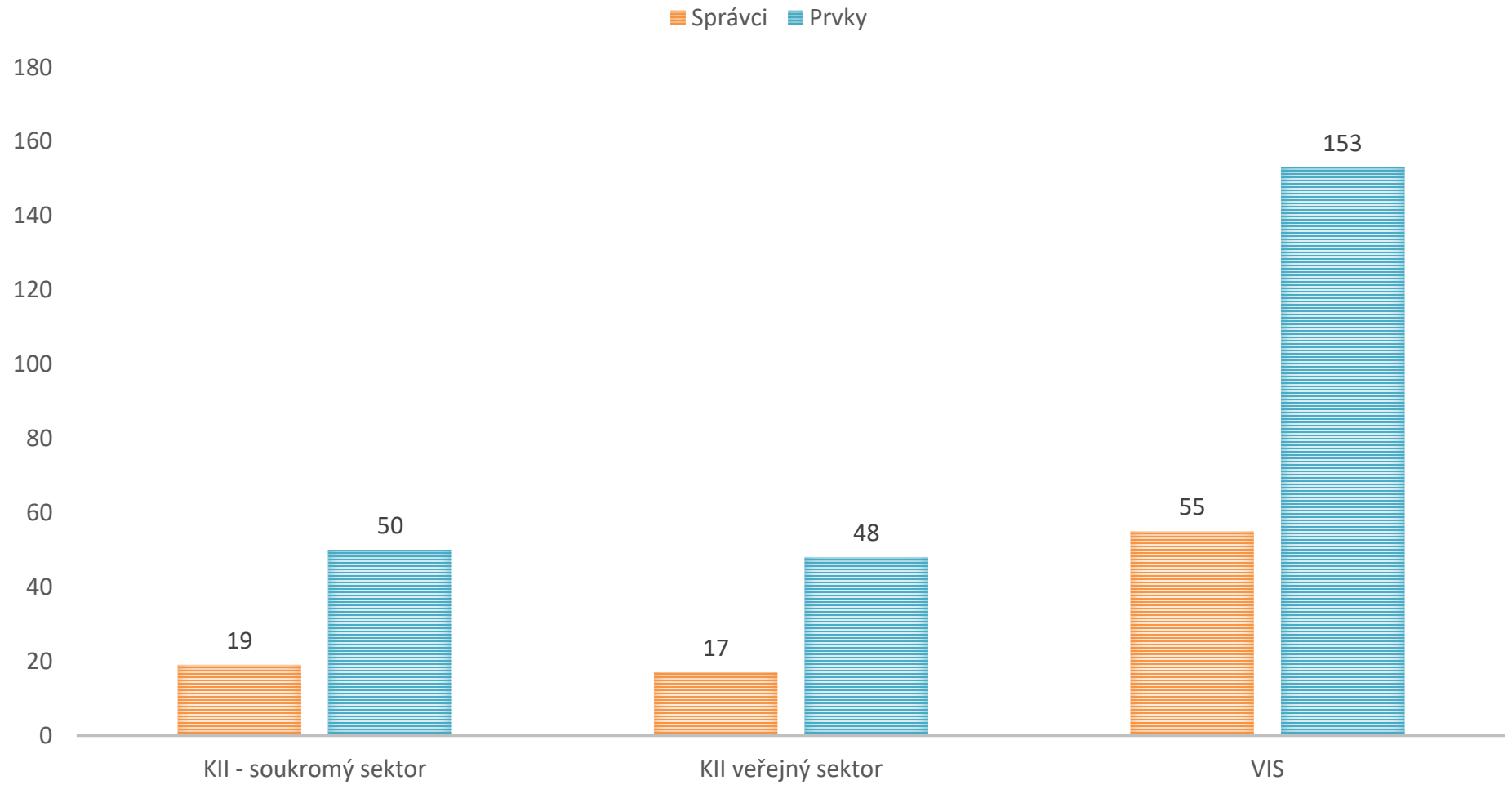
PLNĚNÍ MEZINÁRODNÍCH ZÁVAZKŮ (pokrač.)

- CECSP – Středoevropské platformy pro kybernetickou bezpečnost, založilo NBÚ
- NATO – kontaktní bod pro kybernetickou obranu
  - Memorandum ohledně spolupráce v kybernetické obraně
  - Zastupování ČR v Cyber Defence Committee
- CCDCOE – 1 stálý zástupce v Tallinnu, Estonsko

MAPOVÁNÍ A URČOVÁNÍ KII A VIS

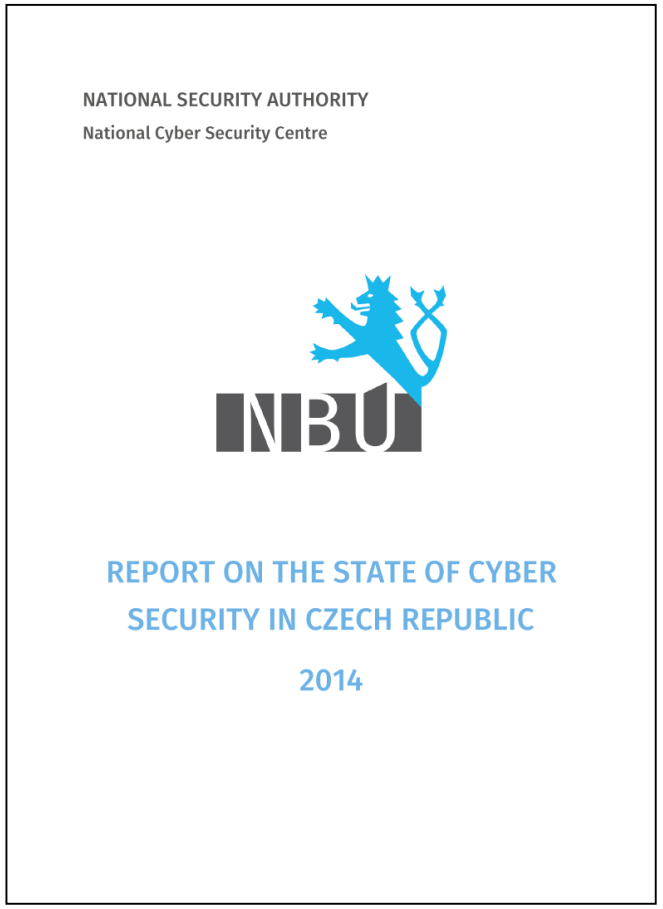
- Určování KII:
  - KII ve veřejném sektoru – NBÚ navrhne Ministerstvu vnitra zařadit IS nebo KS do seznamu, který bude následně předložen vládě ČR. Vláda ČR rozhodne usnesením a navrhovaný IS nebo KS určí.
  - KII v soukromém sektoru – vydávána opatření obecné povahy (OPP)
- Určování VIS:
  - Jedná se pouze o systémy orgánů veřejné moci
  - Naplnění kritérií posuzuje sám správce informačního systémů – Kritéria pro významné informační systémy jsou stanovena vyhláškou o významných informačních systémech, která zároveň uvádí jejich výčet

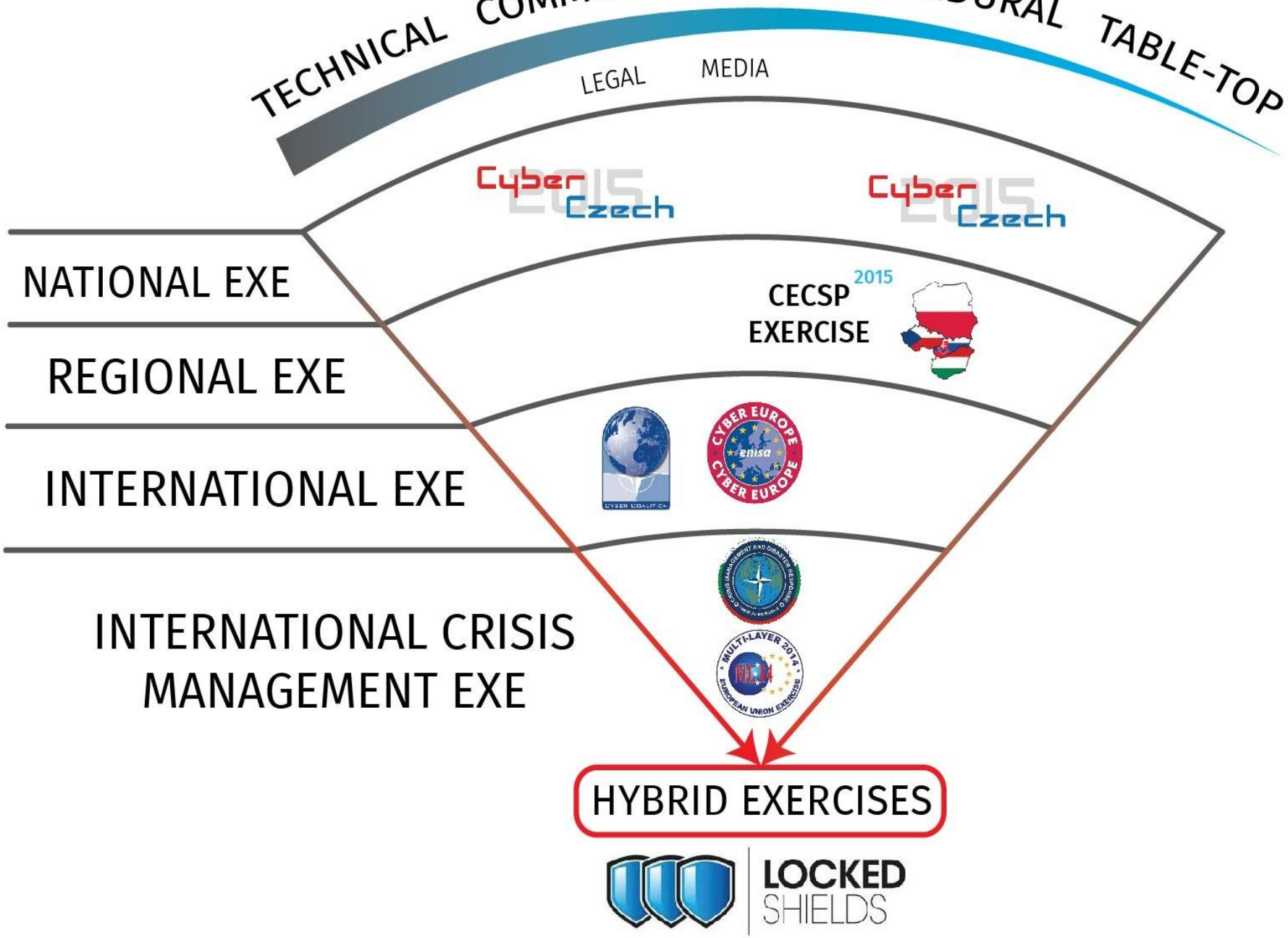
MAPOVÁNÍ A URČOVÁNÍ KII A VIS



VYTVÁŘENÍ A AKTUALIZACE STRATEGICKÝCH A DALŠÍCH ZÁSADNÍCH DOKUMENTŮ

- Národní strategie kybernetické bezpečnosti a Akční plán
- Každoroční zpracovávání Zprávy o stavu kybernetické bezpečnosti ČR
- Zpracovávání analýz / komentářů a podpora ostatním subjektům v otázkách kybernetické bezpečnosti




TECHNICAL
COMMUNICATION
PROCEDURAL
TABLE-TOP
LEGAL
MEDIA
Cyber Czech 2015
Cyber Czech 2015
NATIONAL EXE
CECSP 2015
EXERCISE
REGIONAL EXE
INTERNATIONAL EXE
CYBER EUROPE
enisa
CYBER EUROPE
INTERNATIONAL CRISIS
MANAGEMENT EXE
MULTI-LAYER 2014
EUROPEAN UNION EXERCISE
HYBRID EXERCISES
LOCKED
SHIELDS

ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

Zákon o kybernetické bezpečnosti č. 181/2014 Sb.:

- Novela ZKB současná situace:
  - Vytvoření Národního centra pro kybernetickou a informační bezpečnost
  - Transpozici směrnice NIS v ČR
    - Provozovatelé základních služeb
    - Poskytovatelé digitálních služeb (on line tržiště, internetové vyhledávače, cloud computing)
  - Praktické zkušenosti, které vyplynuly ze zkušeností s implementací ZKB

Zákon o kybernetické bezpečnosti č. 181/2014 Sb.:

- Novela ZKB současná situace:
  - Projednávání v PSP ČR
    - 12. dubna 2017 – schváleno ve třetím čtení
      - Projednáno ve výborech
    - Senát (workshop 3. května 2017), prezident republiky
    - Práce na vyhláškách
    - Účinnost

Provozovatel základní služby (PZS) – definice

- **§ 2 písm. i) 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:

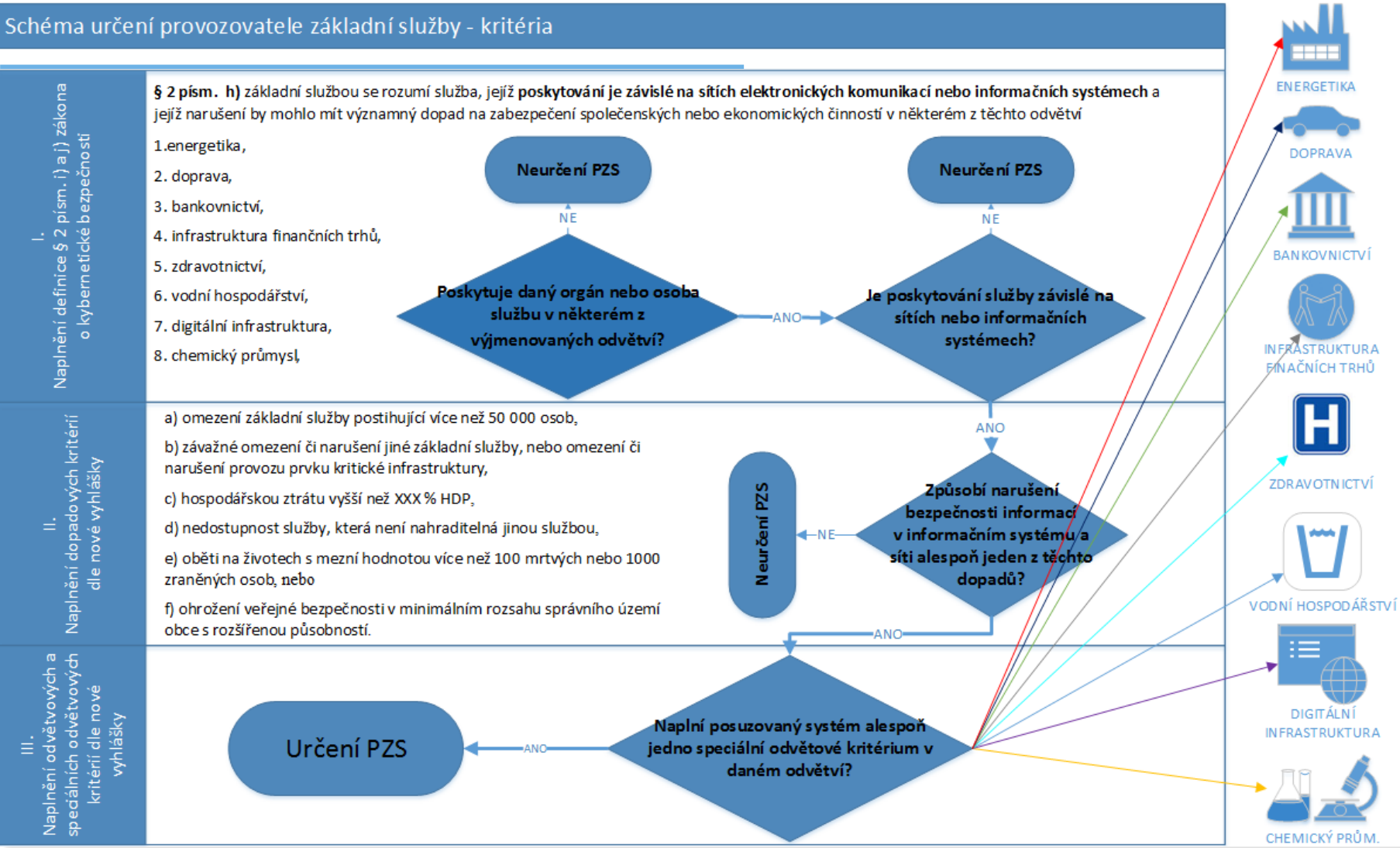
  1. Energetika
  2. Doprava
  3. Bankovnictví
  4. Infrastruktura finančních trhů
  5. Zdravotnictví
  6. Vodní hospodářství
  7. Digitální infrastruktura
  8. Chemický průmysl

- **§ 2 písm. j) NZKB: Informační systém základní služby** = systém, na jehož fungování je závislé poskytování základní služby
- **§ 2 písm. k) NZKB: Provozovatel základní služby** = orgán nebo osoba odpovědná za poskytování základní služby a určená NBÚ

Provozovatel základních služeb (PZS) - určování

- § 22a NZKB: Úřad rozhodnutím určí PZS a informační systém základní služby, pokud naplní odvětvová a dopadová kritéria
- Pro určení je nutné naplnit:
  - Definici: § 2 písm. i) a j) NZKB
  - Kritéria:
    - Kritérium **dopadové**
    - Kritérium **odvětvové**
    - **Speciální odvětvové** kritérium
- Konkrétní nastavení kritérií společně s odborníky – pracovní skupina
  - Cílem je nastavit kritéria tak, aby regulace pokryla pouze systémy nezbytné pro zajištění služeb (ne fakturační, marketingové systémy ani např. bankomaty)

Schéma určení PZS - kritéria



PZS – předpokládaný počet

Odvětví PZS	Je v odvětví určená KII?	Odhad počtu PZS (subjektů)
1. Energetika,	ANO	Nad rámec KII max. 5
2. Doprava	ANO	Nad rámec KII max. 10
3. Bankovnictví	ANO	Cca 10 (spíše ale budou KII)
4. Infrastruktura finančních trhů	NE	3
5. Zdravotnictví	NE	20
6. Vodní hospodářství	ANO (v procesu určení)	Cca 20 (některé ale budou spíše KII)
7. Digitální infrastruktura	NE	Max. 10
8. Chemický průmysl	NE	Max. 10 (spíše méně)
CELKEM	-	Cca 80 PZS

Pozn.: Jde o odhady založené na dosavadních zkušenostech z určování a statistických informacích (banky v ČR podle velikosti, počet měst nad 50 tis. obyvatel, apod.).

PZS – příklady společností, které mohou naplnit kritéria

Odvětví PZS	Druh subjektu/obor podnikání	Příklady společností (předpoklad)
1. Energetika	Rafinérie, teplárny	Česká rafinérská, a.s. - rafinérie Kralupy, Litvínov,
2. Doprava	Letiště, Železnice, Dopravní informační systémy	Letiště Praha, České dráhy, apod.
3. Bankovnictví	Banky	Některé tzv. jiné systémově významné finanční instituce nezařazené do KII – Raifeisen Bank, UniCredit apod.
4. Infrastruktura finančních trhů	Burzy (komoditní, finanční)	Burza cenných papírů Praha
5. Zdravotnictví	Fakultní nemocnice a některé významné krajské nemocnice	FN Motol, FN Brno, apod.
6. Vodní hospodářství	Provozovatelé vodáren a kanalizací ve velkých městech (nad 50 tis. obyvatel)	Pražské vodárny a kanalizace, Brněnské vodárny a kanalizace, apod.
7. Digitální infrastruktura	Nejvýznamnější provozovatelé sítí (páteřní sítě) a nejvýznamnější poskytovatelé internetových služeb	CESNET, ČD - telematika, NIX, apod.
8. Chemický průmysl	Klíčové chemické podniky	Spolana, Explosia, Sanofi, Precheza, apod.

PZS – dopadová kritéria z NIS

- Podle NIS by kritéria pro PZS měly zohledňovat alespoň následující hlediska (čl. 6/1 NIS):
  1. počet uživatelů, kteří jsou závislí na službě poskytované daným subjektem;
  2. závislost dalších odvětví na službě poskytované daným subjektem;
  3. možný dopad incidentů, pokud jde o intenzitu a trvání, na činnosti hospodářství a společnosti nebo na veřejnou bezpečnost;
  4. podíl daného subjektu na trhu;
  5. zeměpisný rozsah oblasti, která by mohla být incidentem dotčena;
  6. důležitost subjektu, pokud jde o udržování dostatečné úrovně dané služby, s přihlédnutím k dostupnosti alternativních způsobů zajištění této služby.

+ Možnost zvážit i další specifické okolnosti pro jednotlivá odvětví (čl. 6/2 NIS)

PZS – Návrh dopadových kritérií – návrh NBÚ

- Dopadové kritérium je naplněno v případě, že narušení bezpečnosti informací a dat v informačním systému může způsobit:

a) omezení základní služby postihující více než 50 000 osob	e) oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob
b) závažné omezení či narušení jiné základní služby, nebo omezení či narušení provozu prvku kritické infrastruktury	f) ohrožení veřejné bezpečnosti v minimálním rozsahu správního území ORP
c) hospodářskou ztrátu vyšší než 0, 25 % HDP	g) kompromitaci citlivých údajů o 200 000 osobách
d) nedostupnost služby, která není nahraditelná jinou službou	

- K nastavení kritérií je zřízena pracovní skupina při NBÚ
- V případě, že systém naplní kritéria pro PZS i KII – určí se jako KII
- Kritéria pro PZS by neměla být vyšší jak u KII

PZS – kritéria z NIS vs. návrh NBÚ - srovnání

1. **NIS:** počet uživatelů, kteří jsou závislí na službě poskytované daným subjektem;
   - ***NBÚ:*** *a) omezení základní služby postihující více než 50 000 osob*
2. **NIS:** závislost dalších odvětví na službě poskytované daným subjektem;
   - ***NBŮ:*** *b) závažné omezení či narušení jiné základní služby, nebo omezení či narušení provozu prvku kritické infrastruktury*
3. **NIS:** možný dopad incidentů, pokud jde o intenzitu a trvání, na činnosti hospodářství a společnosti nebo na veřejnou bezpečnost;
   - ***NBÚ:*** *f) ohrožení veřejné bezpečnosti v minimálním rozsahu správního území obce s rozšířenou působností + e) oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných*
4. **NIS:** podíl daného subjektu na trhu;
   - ***NBÚ:*** *c) hospodářská ztráta vyšší než 0, 25 % HDP*
5. **NIS:** zeměpisný rozsah oblasti, která by mohla být incidentem dotčena;
   - ***NBÚ:*** *b) ohrožení veřejné bezpečnosti v minimálním rozsahu správního území ORP*
6. **NIS:** důležitost subjektu, pokud jde o udržování dostatečné úrovně dané služby, s přihlédnutím k dostupnosti alternativních způsobů zajištění této služby.
   - ***NBÚ:*** *d) nedostupnost služby, která není nahraditelná jinou službou*

Odvětví PZS podle NIS: I. Energetika

- Pododvětví Elektřina
  - elektroenergetický podnik
  - provozovatel distribuční a 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
  - řídící orgány přístavů
- Pododvětví Silniční doprava
  - silniční orgány a provozovatelé inteligentních dopravních systémů

*Zde **KII** prozatím **neurčena***

*Zde **KII** prozatím **neurčena***

Odvětví PZS podle NIS:
III. Bankovnictví, IV. Infrastruktura finančních trhu

- Bankovnictví
  - úvěrové instituce (podnik, jehož činnost spočívá v přijímání vkladů nebo jiných splatných peněžních prostředků od veřejnosti a poskytování úvěrů na vlastní účet)
- Infrastruktura finančních trhů
  - provozovatelé obchodních systémů (regulovaný trh, mnohostranný obchodní systém nebo organizovaný obchodní systém)
  - ústřední protistrana (právnická 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)

*Zde **KII** prozatím **neurčena***

Odvětví PZS podle NIS:
V. Zdravotnictví, VI. Vodní hospodářství

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

*Zde **KII** prozatím **neurčena***

- Vodní hospodářství
  - Dodavatel vody určené k lidské spotřebě,
  - Provozovatel zařízení odvodu odpadních vod a jejich odvodu

Odvětví PZS podle NIS:
VII. Digitální infrastruktura, VIII. Chemický průmysl

- Digitální infrastruktura
  - Výměnné uzly internetu
  - Poskytovatelé služeb systému doménových jmen
  - Rejstříky internetových domén nejvyšší úrovně
- Chemický průmysl
  - Na konkrétních omezujících kritériích se pracuje

KII** prozatím **neurčena úplně

Speciální odvětvová kritéria - příklad

- Odvětví jsou směrnicí nastavena široce – omezení a „zpřísnění“ kritérií – tzv. speciální odvětvová kritéria
  - Zohledňují specifika jednotlivých odvětví a významnost subjektu
- Příklad speciálních odvětvových kritérií – Energetika:
  - Pododvětví elektřina

Výroba elektřiny	Výrobce elektřiny ve smyslu zákona č. 458/2000 Sb., energetický zákon	Řídicí systémy nezbytné pro provoz a řízení provozu výroben elektrické energie, jedná-li se o: a. výrobnu s celkovým instalovaným elektrickým výkonem nejméně 500 MW, b. výrobnu poskytující podpůrné služby s celkovým instalovaným elektrickým výkonem nejméně 100 MW, c. dispečink výrobce elektřiny.

  - Pododvětví ropa

Provoz ropovodu	Provozovatel ropovodu	a. Vnitrostátní ropovod s průměrným ročním objemem přepravy ropy více než 500 tisíc tun/rok b. Koncové zařízení pro předání ropy

Pracovní skupina k PZS – organizace jednání

- Konkrétní nastavení kritérií provádí NBÚ ve spolupráci s odborníky, zástupci subjektů a zástupci regulátorů jednotlivých odvětví – Pracovní skupina Sem napište text.
- Jednání pracovní skupiny
  - 20. 10. 2016 – společná prac. skup. pro všechna odvětví
  - 21. 11. 2016 – společná prac. skup. pro všechna odvětví

Pracovní skupina rozdělena na podskupiny dle odvětví

  - 8. 12. 2016 – Energetika – 3 podskupiny (elektřina, ropa, plyn)
  - 24. 1. 2017 – Doprava – 4 podskupiny (letecká, silniční, vodní, železniční)
  - 25. 1. 2017 – Bankovnictví, Finanční trhy, Zdravotnictví, Vodní hospodářství
  - 26. 1. 2017 – Digitální infrastruktura, Chemický průmysl

Navazující - finální jednání předpokládáme v první polovině roku 2017

Pracovní skupina k PZS – přizvané subjekty

Odvětví PZS	Subjekty oslovené do pracovní skupiny (příklady)
1. Energetika	MPO, ERÚ, ČEZ, ČEPS, Plynárenský svaz, EON, Net4Gas, Innogy, PRE, ČEPRO, PARAMO
2. Doprava	MD, Úřad pro civilní letectví, ŘLP, ŘSD, Svaz dopravy, SŽDC, Státní plavební správa, Ředitelství vodních cest ČR, Letiště VH, ČSA, ČD, RegioJet, Středočeský kraj, Drážní úřad, Centrum služeb pro silniční dopravu, CENDIS, SFDI, Travel service
3. Bankovnictví + 4. Infrastruktura finančních trhů	MF, ČNB, ČBA, ČS, ČSOB, KB, Pražská burza, UniCredit, J&T, Raiffeisen, PPF
5. Zdravotnictví	MZd, FN Brno, FN Motol, Kraje - Jihomoravský, Středočeský, Vysočina, Moravskoslezský, IKEM, Thomayerova nemocnice
6. Vodní hospodářství	MZe, MŽP, Veolia, Pražské vodárny a kanalizace, Brněské vodárny a kanalizace
7. Digitální infrastruktura	MV, MPO, ČTÚ, NIX, CZ.NIC, ČD telematika, Peering.cz, CETIN, CESNET
8. Chemický průmysl	Svaz chemického průmyslu ČR a jím doporučené organizace

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 regulační autoritě součinnost posouzení bezpečnosti
  - Provádět nápravu zjištěných nedostatků
- Povinnosti založené na normách ISO 27k
  - Podle dosavadních zkušeností plní většina potencionálních PZS množství opatření již nyní (někdy i na vyšší úrovni - banky, energetika, apod.)

Poskytovatelé digitálních služeb

- on line tržiště
- internetové vyhledávače
- cloud computing
- maximální regulace
- kompetence národního CERTu

Děkuji za pozornost!

Jaroslav Šmíd
náměstek ředitele NBÚ
www.nbu.cz
www.govcert.cz
j.smid@nbu.cz