Aktuální stav kybernetické bezpečnosti v České republice

Adam Kučínský
Oddělení regulace
Odbor regulace, auditu a podpory

Národní úřad
pro kybernetickou
a informační bezpečnost

Kybernetická bezpečnost v ČR

2011
- NBÚ ustanoven jako gestor KB
- vznik Národního centra kybernetické bezpečnosti

2012
- Národní strategie kybernetické bezpečnosti I.

2015
- Zákon o kybernetické bezpečnosti
- Národní strategie kybernetické bezpečnosti II.

2016
- Směrnice NIS

2017
- Novela zákona o kybernetické bezpečnosti
- Vznik NÚKIB

NBÚ

nckb

NÚKIB

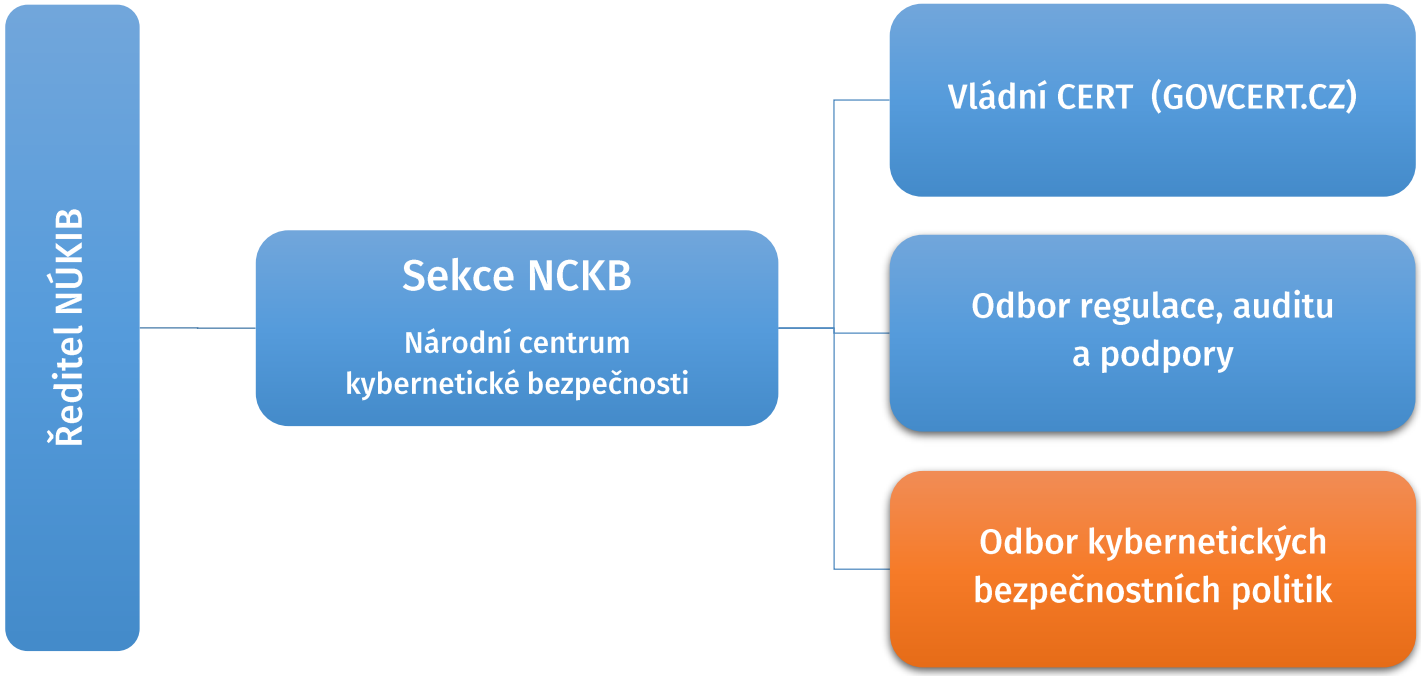
Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost

- Vznik 1. 8. 2017
- Ústřední správní orgán pro:
  - kybernetickou bezpečnost
  - ochranu utajovaných informací v oblasti informačních a komunikačních systémů
  - Kryptografickou ochranu
- Služby NÚKIB v oblasti kybernetické bezpečnosti
  - provoz Vládního CERTu České republiky (GovCERT.CZ)*
  - spolupráce s ostatními CERT A CSIRT
  - příprava bezpečnostních standardů
  - osvěta a podpora vzdělávání
  - výzkum a vývoj
  - ochrana utajovaných informací v oblasti IS/KS
  - kryptografická ochrana
  - Kontaktní místo GALILEO

*Computer Emergency Response Team

Organizační schéma – NÚKIB – NCKB – OKBP



I. Oddělení strategických informací a analýz (OSINA)

- Co děláme: Strategická analýza zaměřená na zasazení technických informací do kontextu

- Proč to děláme:
  - informační podpora decision-makerů
  - prevence rizik
  - informační podpora v případě krizových situací
  - zvyšování povědomí o kybernetických hrozbách
  - formulace opatření

- Pro koho to děláme:
  - vedení NÚKIB
  - předseda vlády a jednotlivá ministerstva
  - bezpečnostní komunita (zpravodajské služby, PČR)
  - KII a VIS
  - mezinárodní organizace (NATO, EU)
  - bilaterální partneři (USA, UK, KOR a další)

Vybrané kybernetické hrozby posledního roku

- E-health
  - Počet kybernetických útoků na zdravotnická zařízení narůstá
  - Kybernetické útoky proti zdravotním systémům mohou při nízkých nákladech a malém úsilí přinést útočníkům relativně velké zisky
- Nástup státních aktérů, kteří ještě před několika lety nebyli považováni za dostatečně vyspělé
  - narůstající ofenzivní kybernetické schopnosti, včetně schopností provádět kybernetické útoky způsobující fyzickou škodu
  - finančně motivované útoky na bankovní sektor, krádež kryptoměn, šíření malwaru pro těžbu kryptoměn
- APT (advanced persistent threat)
  - Začínají se více zaměřovat na slabiny v dodavatelském řetězci, které je dovedou k hlavnímu cíli
  - K trvajícímu zájmu o průmyslová tajemství evropských firem se přidává rostoucí zájem o strategické informace (utajované informace, interní komunikace vládních úřadů, vojenské informace)
- Kyberterorismus
  - Hrozba kyberterorismu v současné době pravděpodobně není vysoká. Teroristé, včetně Islámského státu, zatím nemají dostačené schopnosti k provedení sofistikovaného kybernetického útoku.

II. Oddělení národních strategií a politik

Implementace Národní strategie kybernetické bezpečnosti

- plnění, koordinace a kontrola Akčního plánu

Příprava dlouhodobých plánů a projektů

- „Spolek přátel kybernetické bezpečnosti“ - Kyberliga
- plánování rozvoje kapacit
- spolupráce se soukromým sektorem

Vyhodnocování nových hrozeb na strategické úrovni

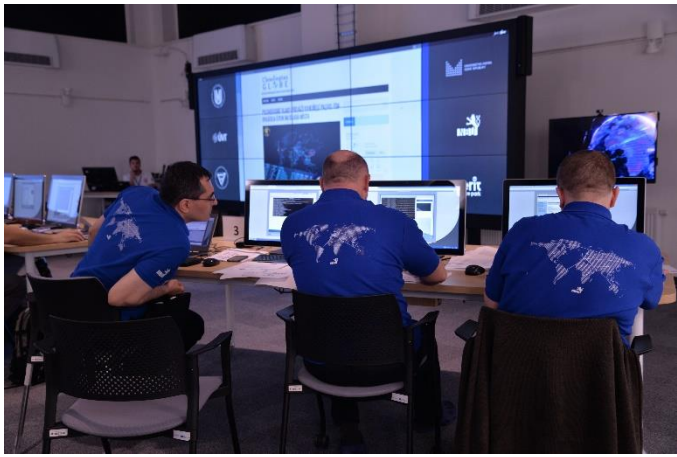
- koordinace činností souvisejících s plněním Národní strategie kybernetické bezpečnosti na národní úrovni

Koordinace konference CyberCon Brno a akce C2S2

III. Oddělení cvičení (EDEX)

Cvičení pořádaná pro **národní partnery**:

- Český statistický úřad: interaktivní školení pořádáno v rámci vytvrzování volebního procesu.
- Kurz Generálního štábu: netechnické table-top cvičení zařazeno jako součást pravidelného každoročního kurzu.
- Národní technické cvičení Cyber Czech:
  - Připravováno ve spolupráci s Masarykovou univerzitou.
  - Cvičení se aktivně účastní okolo 80 osob.
  - Založeno na modelu útočící červený tým versus obranný modrý tým.
  - Zaměřeno na procvičení technických schopností.



Oddělení cvičení (EDEX)

Cvičení pořádaná pro **zahraniční partnery**:

- Kongres USA: netechnické table-top cvičení pro asistenty kongresmanů.
- Africa Endeavor: netechnické table-top cvičení bylo součástí symposia, kterého se účastnili představitelé z více než 30 afrických států.

Účast na tvorbě **mezinárodních cvičení**:

- Locked Shields: organizováno centrem excelence v Tallinnu, ČR letos obsadila 3. místo v technické části.
- Cyber Coalition: technické a procedurální cvičení NATO.
- EU HEX 2018 (PACE): procedurální cvičení krizového řízení Evropské unie.

IV. Oddělení Mezinárodních organizací a práva

Základní informace:

- **zastoupení ČR v** mezinárodních organizacích řešících kyber problematiku – primárně **NATO, EU, OBSE**
  - příprava instrukcí, podkladů, účast na pracovních jednáních
  - EU – implementace směrnice NIS, digitální agenda, Horizont 2020 a cPPP pro kybernetickou bezpečnost, horizontální spolupráce
  - NATO – Cyber Defence Committee, právní podpora cvičení
  - OBSE – opatření pro budování důvěry
  - OECD – kybernetická bezpečnost jako předpoklad ekonomického rozvoje

Činnost Oddělení mezinárodních organizací a práva

EU:

- Cyber Security Act
- Závěry Rady EU o nepřátelské činnosti v kyberprostoru
- Závěry Rady EU ke koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize

NATO

- NATO Summit v Bruselu

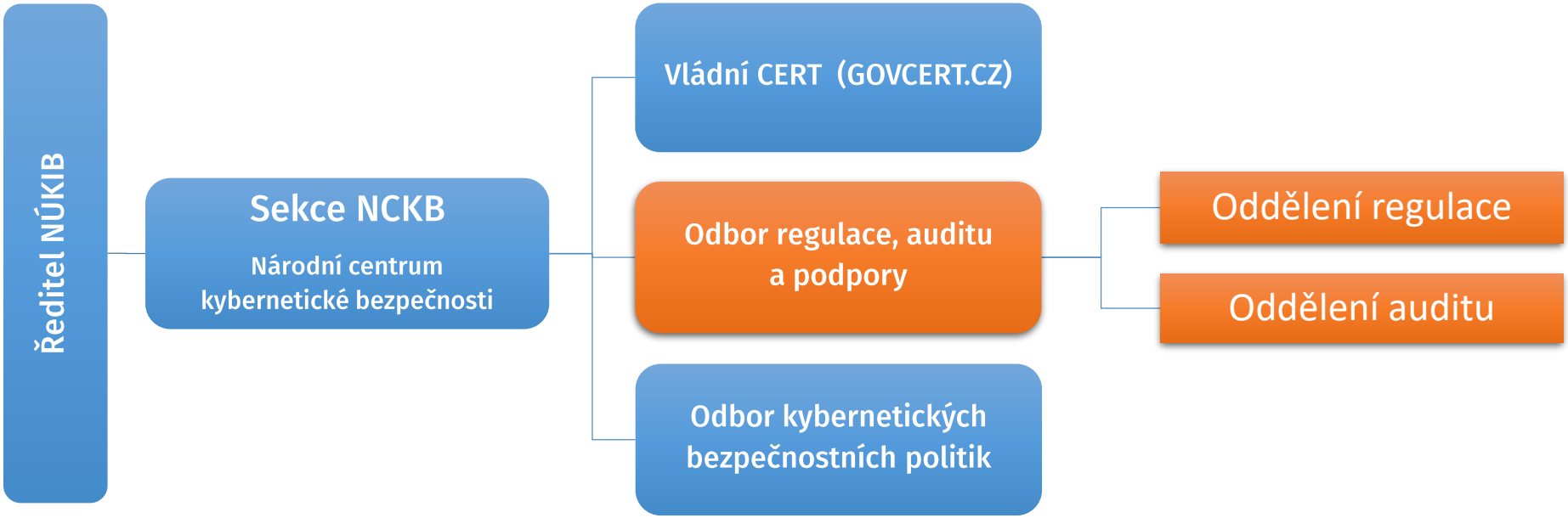
OBSE

- Iniciativa pro osvojení realizace opatření pro budování důvěry (CBM)

GFCE

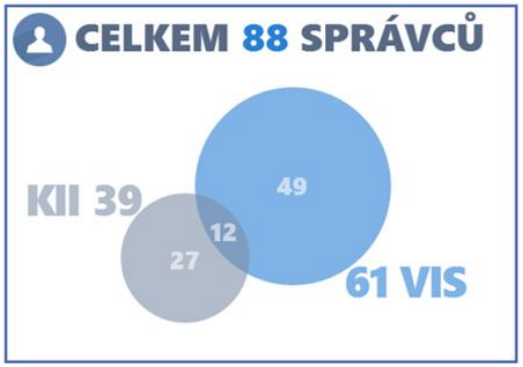
- Přistoupení k fóru v tomto roce

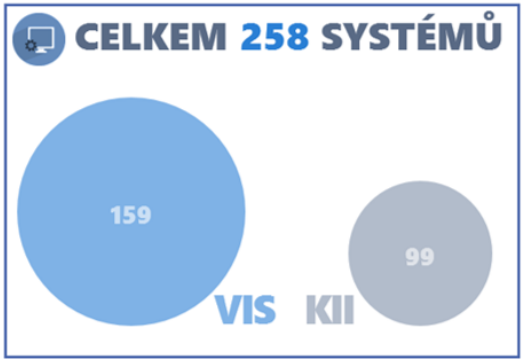
Organizační schéma – NÚKIB – NCKB - RAP



Oddělení Regulace

- Stanovení, které subjekty a ICT dle kritérií ZKB spadají pod regulaci a které nikoliv
  - Určovací schůzky se subjekty
  - Vydávání opatření obecné povahy, návrhy na usnesení vlády (určení KII), vydávání rozhodnutí (PZS)
- Správa databáze kontaktů (vlastní NCKB systém)
  - Min. 15 změn v 1 měsíci
- Příprava legislativy
- Výklad zákona, konzultace se subjekty





Oddělení Auditu (kontrola ZKB)

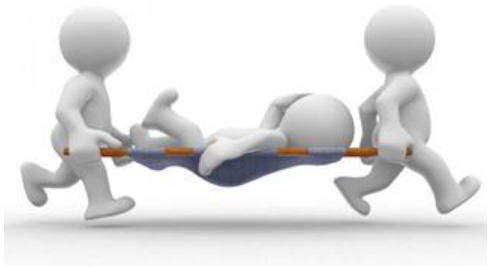
- Kontrola dodržování ZKB
  - přistupujeme k ní podobně jako k auditu systému řízení bezpečnosti informací podle ISO 27 001, což přináší přidanou hodnotu i pro regulované subjekty
- Metodická podpora subjektů z pohledu zavádění ISMS
- Prozatím neprovádíme kontrolu dodržování ZKB u jiných, než KII/VIS subjektů.

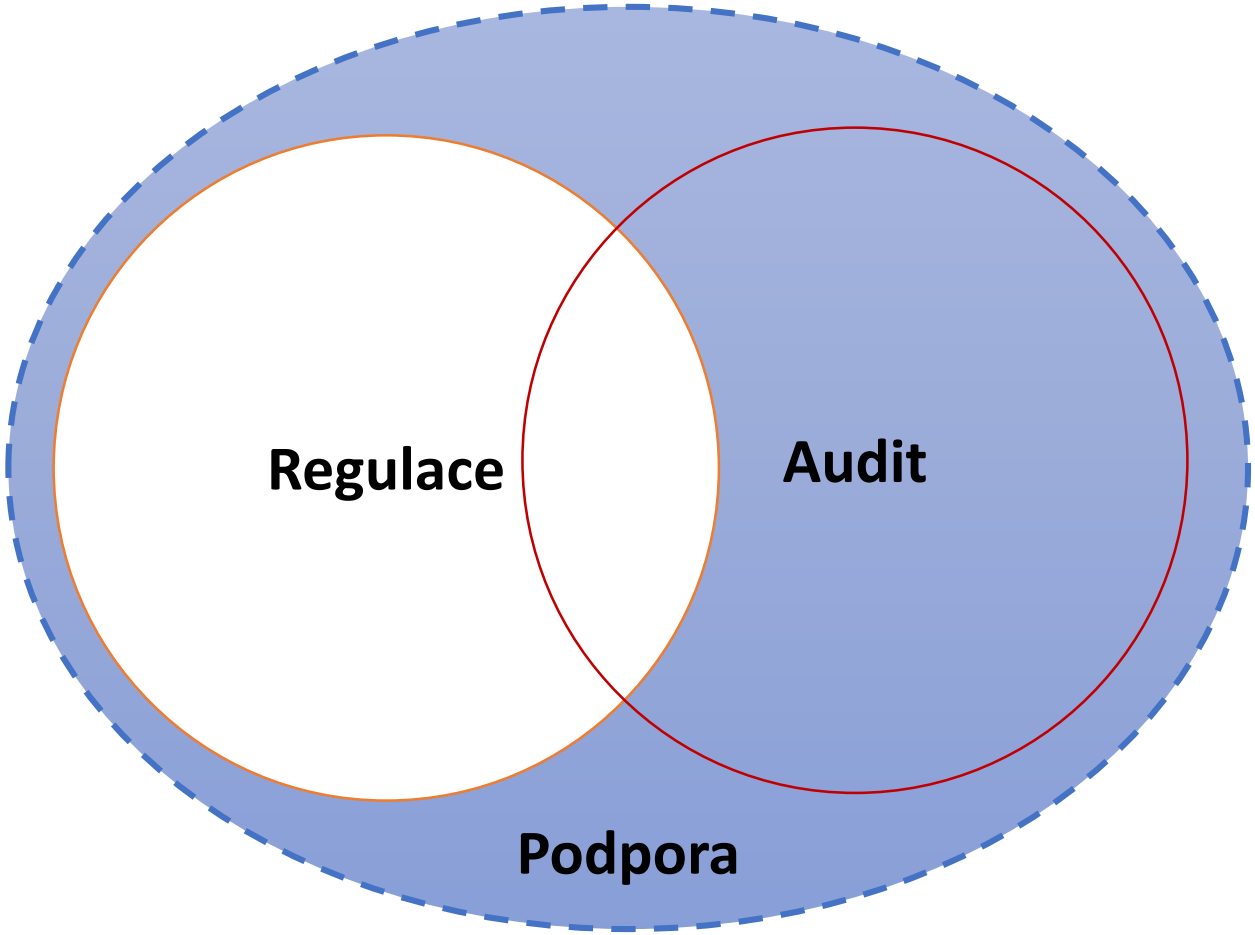
Novelizace ZKB a tvorba souvisejících předpisů

- ~~Novela ZKB~~
- ~~Vyhláška o PZS~~
- ~~Novela VKB~~
- *Vyhláška o likvidaci dat*
- *Vyhláška o bezpečnosti Cloud Computingu*
- *Novela vyhlášky o VIS*

„Měkká“ podpora

- jsme v 1. linii při kontaktu s regulovanými subjekty
- výklad ZKB
- výklad vyhlášek
- metodická podpora při implementaci ZKB (implementaci organizačních a technických opatření)
- „konzultační a poradenská činnost“ v oblasti kybernetické bezpečnosti pro regulované subjekty





Další činnosti

- Vzdělávání a osvěta v oblasti ZKB
- Účast na různých pracovních skupinách
- Pořádání workshopů, seminářů apod.
- …

Spolupráce s jinými odděleními (1/2)

- Školení a výuka (např. výuka na VŠ nebo školení pro Úřad vlády, MMR aj.)
  - spolupráce s Oddělením cvičení, vzdělávání a výzkumu
    - např. výuka na VŠ nebo školení pro Úřad vlády, MMR aj.
    - E-learning – Modul B
- Incident Handling
  - Spolupráce s týmem GovCERT.CZ – konzultace ohledně ZKB
- Vývoj vlastní DB kontaktních údajů

Spolupráce s jinými odděleními (2/2)

- Kontroly ZKB
  - Spolupráce s relevantními odděleními koordinovaná Oddborem regulace, auditu a podpory
  - Postupně se snažíme brát své kolegy na audity
- Mezinárodní organizace a právo
  - Spolupráce při tvorbě práv. předpisů
  - Spolupráce při reportování směrem k EU apod.
- Kybernetická cvičení
  - Spolupráce s CERT a Oddělením cvičení

Spolupráce napříč odděleními

- Usnesení vlády ze dne 8. 2. 2017 č. 104 a z něj vyplývající poskytnutí analýzy a metodické podpory 18 institucím státní správy
  - Spolupráce napříč týmem GovCERT.CZ a odborem regulace, auditu a podpory
  - „Pohotovostní“ výjezd 3 analytických týmů
  - **Šlo o koordinaci cca 22 zaměstnanců NCKB, ti v rámci práce na projektu vykonali skvělou práci. Projekt byl splněn v plánovaném termínu.**

Další zajímavé projekty, které máme za sebou

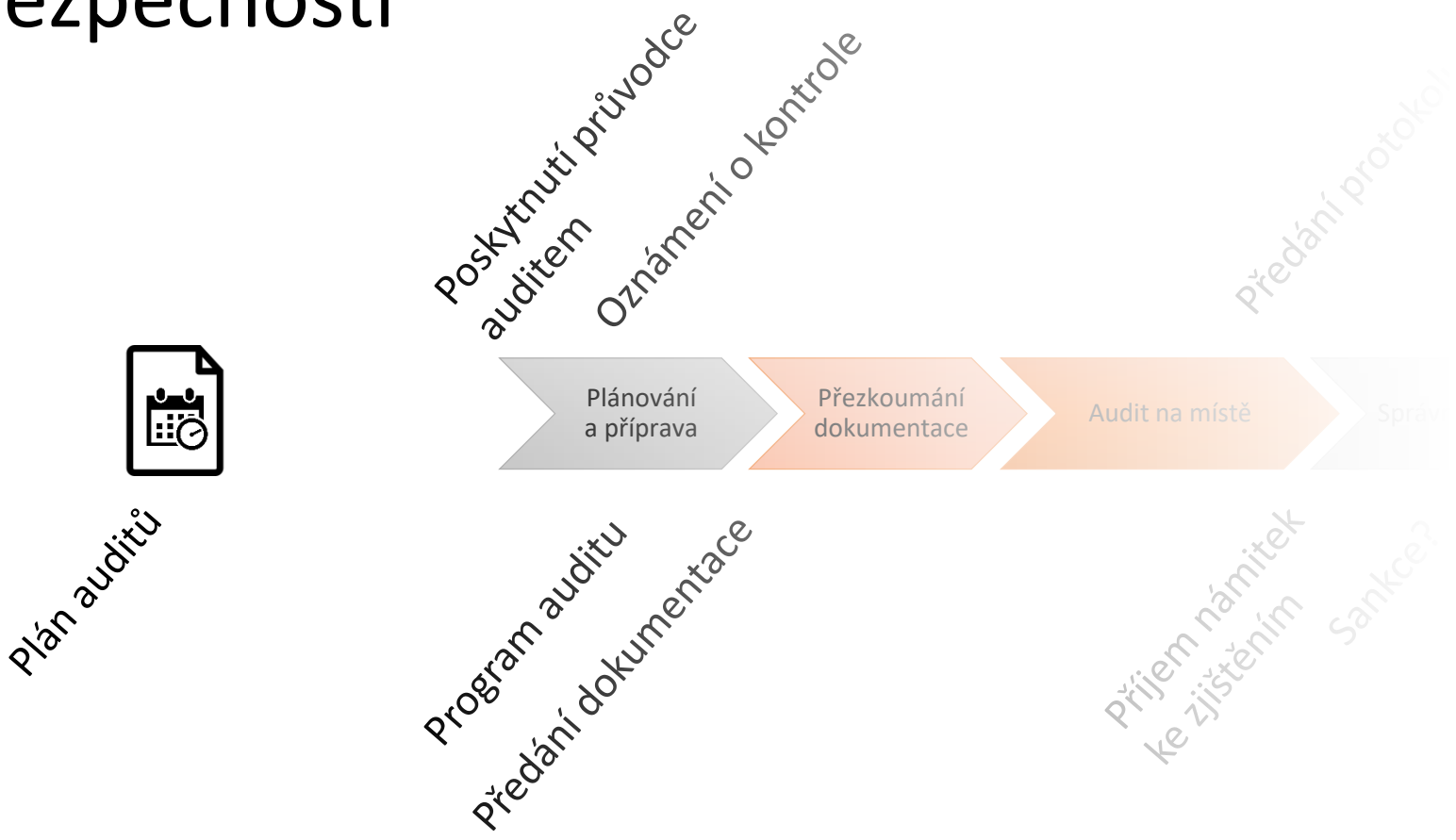
- Procesy a podpůrné materiály:
  - Určování
  - Audit
  - Výklad různých problematických oblastí
- Konzultace a audit na Úřadu vlády
- Projekt vzdělávání pro státní správu v oblasti KB – pod IVS
- Školení a tvorba podkladů na auditorský atestační kurz (ČIIA)
- Audit 15 subjektů v r. 2016, metodická podpora 18 ÚSÚ v roce 2017 a 2018
- Podílení se na přípravě legislativy – novela ZKB, PZS vyhlášky
- Netradiční přístup k VKB vyhlášce
- …

Zkušenosti z auditů (kontrol) ZKB

Charakteristika auditu shody se zákonem o kybernetické bezpečnosti

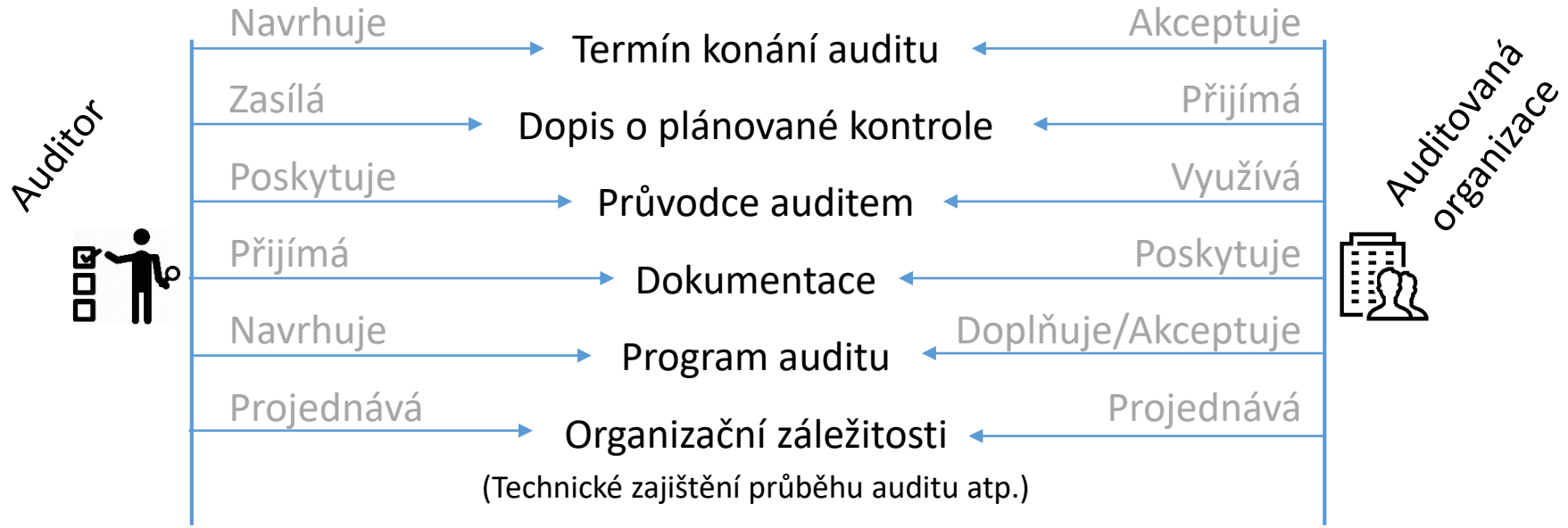
- V souladu s:
  - Kontrolním řádem,
  - Správním řádem.
- Auditované organizace: **správci KII a VIS.**
- Předmět auditu: **systémy KII a VIS.**
- Kritéria auditu: **zákon a vyhláška.**
- Obsah auditu: **cca 100 - 150 kontrolních bodů z oblastí:**
  - Organizačních opatření,
  - Technických opatření,
  - Zvládání incidentů.

Proces auditu zákona o kybernetické bezpečnosti



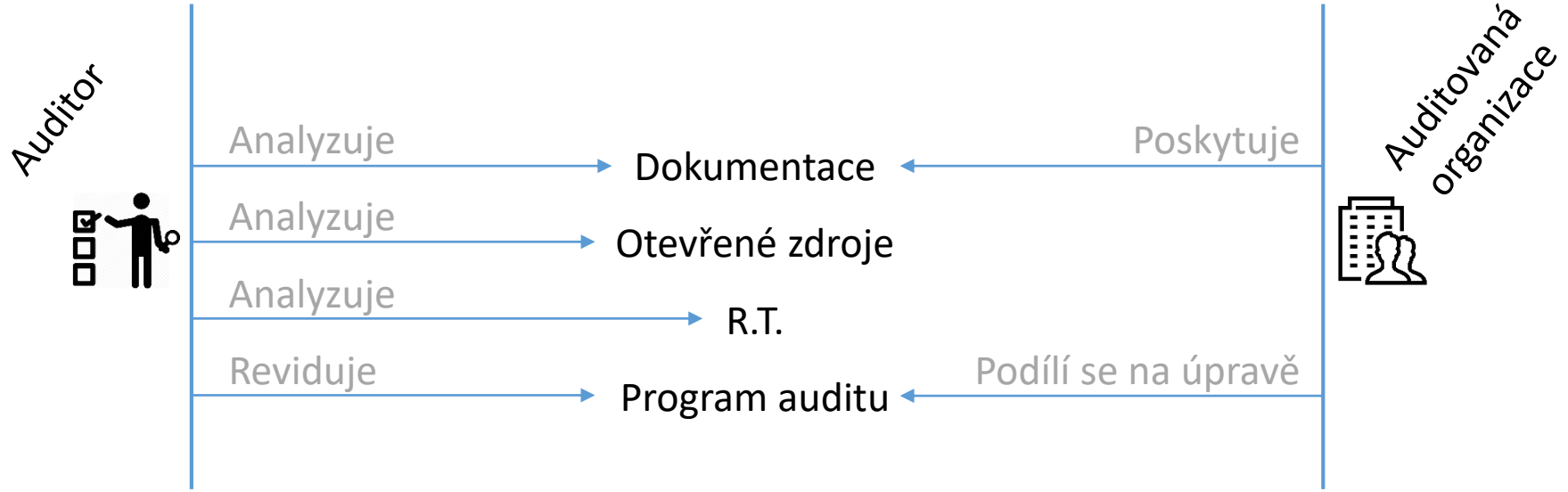
Plánování a příprava → Přezkoumání dokumentace → Audit na místě → Správní řízení → Kontrola nápravných opatření → Následný audit

14 – 30 dní před auditem



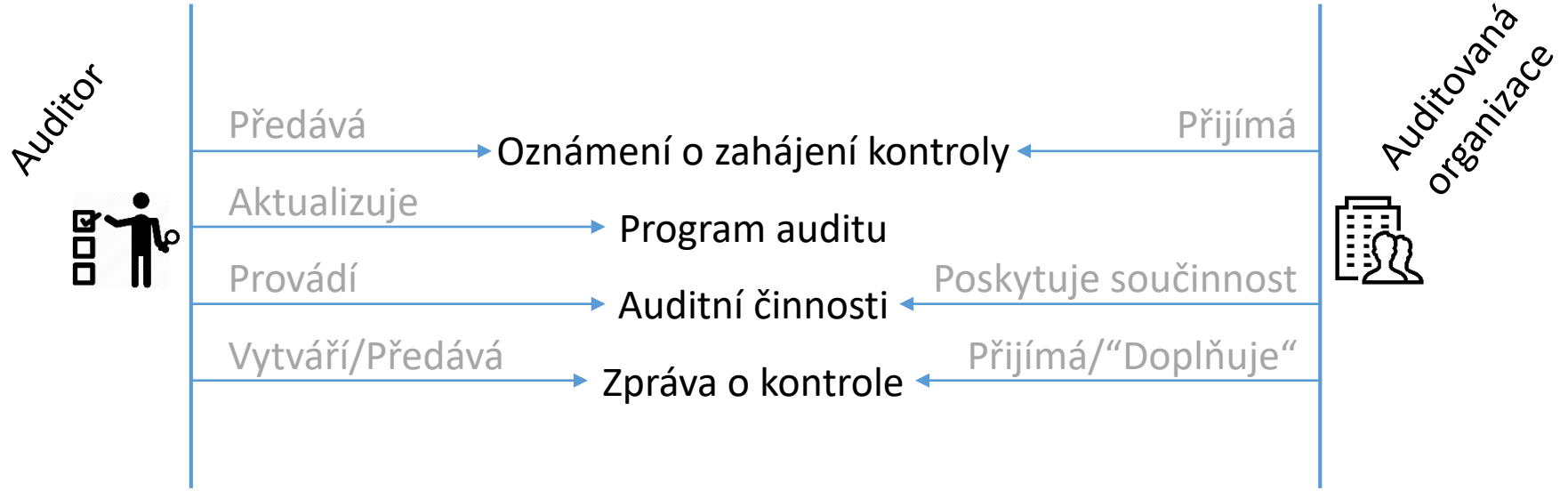
Plánování a příprava | **Přezkoumání dokumentace** | Audit na místě | Správní řízení | Kontrola nápravných opatření | Následný audit

Cca týden před auditem



Plánování a příprava → Přezkoumání dokumentace → **Audit na místě** → Správní řízení → Kontrola nápravných opatření → Následný audit

VIS cca 2 - 3 dny
KII cca 2 - 8 dní



KLASIFIKACE (TYPY) AUDITNÍCH ZJIŠTĚNÍ

Neshoda (důvod k zahájení správního řízení (udělení sankce))

Neshodou se rozumí nesplnění požadavku podle stanovených kritérií nebo odchýlení praxe od dokumentovaných postupů.

Příležitost ke zlepšení

Příležitost ke zlepšení je typ zjištění, které má charakter doporučení a vychází ze zkušeností kontrolujícího.

Potenciální riziko

Touto formou kontrolující upozorňuje na možné riziko.

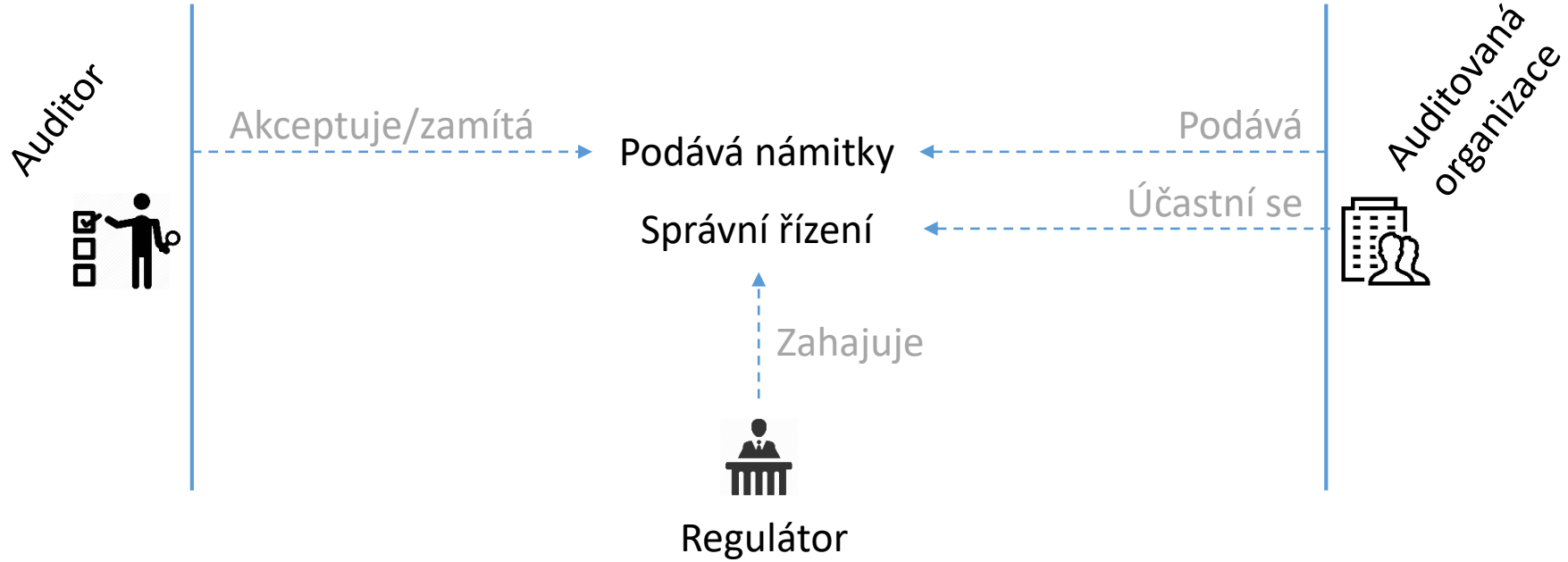
Pozoruhodné úsilí

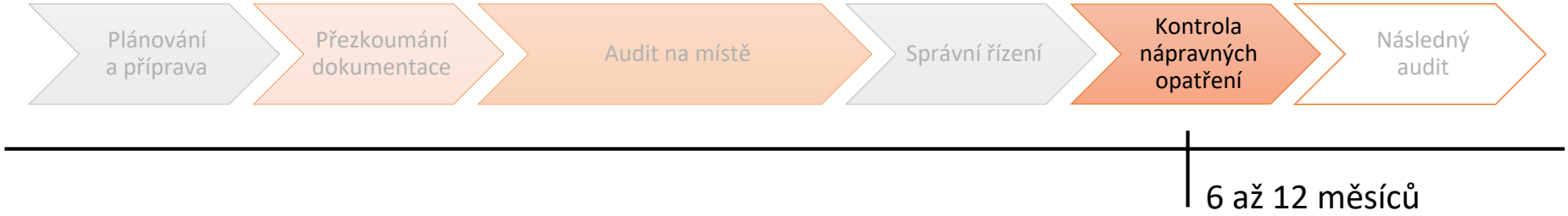
Vyjadřuje ocenění nadstandartní snahy plnění požadavků v dané oblasti.

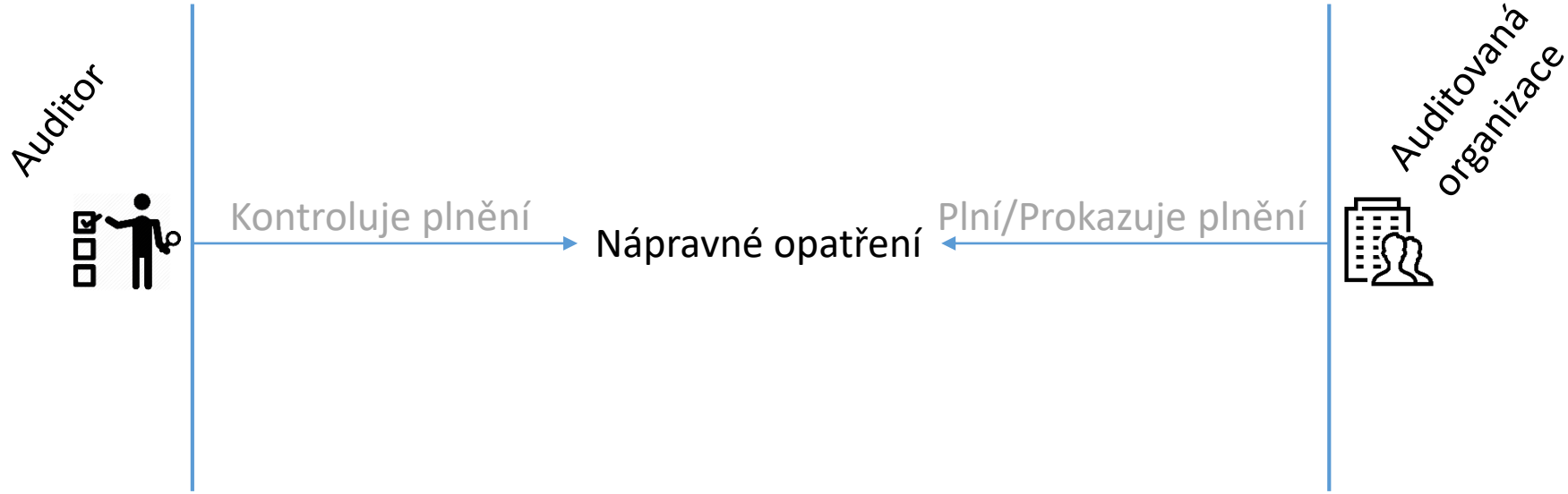
Shoda

Přidaná hodnota auditu?

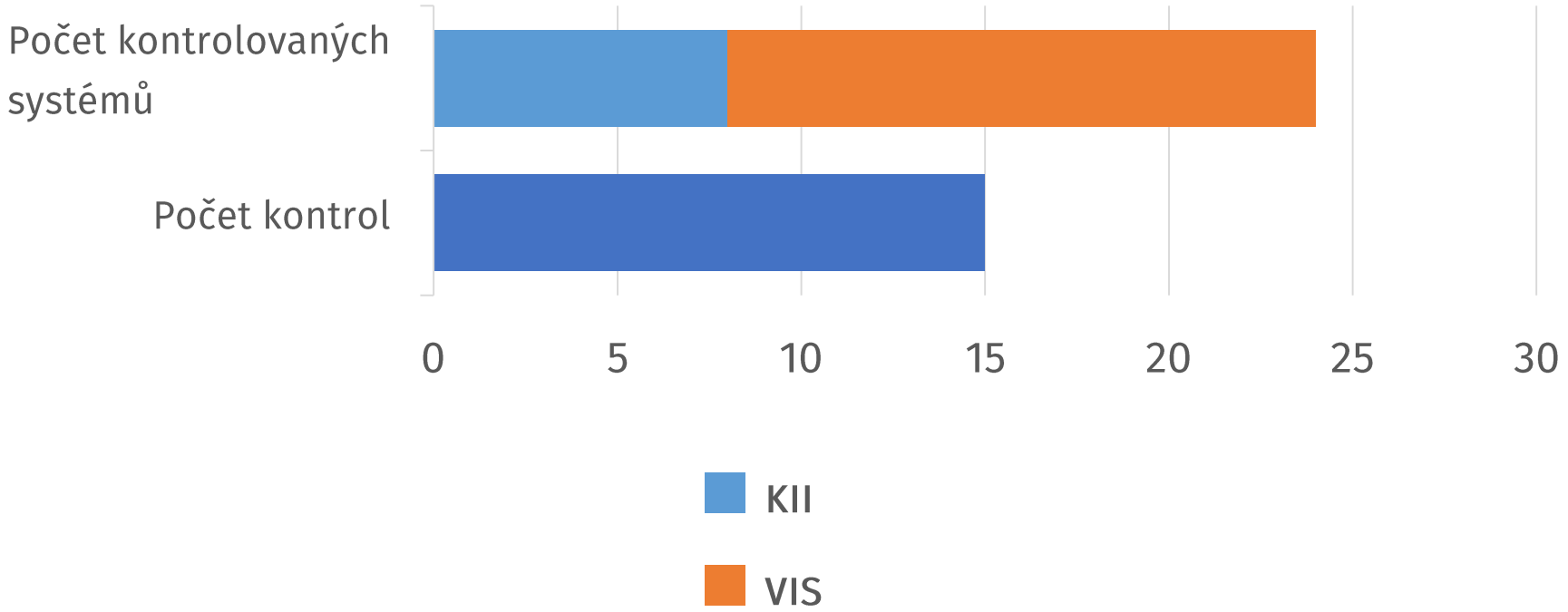
lhůta 15 dní na podání námitek
→ případné správní řízení (45+ dní)







Počet kontrol a kontrolovaných systémů dle kategorie



Analýzy ministerstev

- Usnesení Vlády ČR ze dne 8. 2. 2017 č. 104
  - Subjekty: všechna ministerstva, Poslanecká sněmovna, Senát a Kancelář prezidenta republiky
  - CÍL: zjištění aktuální situace v oblasti kybernetické bezpečnosti

- Na to navázalo **Usnesení Vlády ČR ze dne 21. srpna 2017 č. 607**
  - Provést obdobné analýzy dotčených subjektů do 31. prosince 2018

Analýzy ministerstev

- Zaměření analýz: systémy a služby splňující
  - Dostupnost systému z veřejného Internetu
  - Vzdálené připojení nebo přihlášení uživatelů organizace
  - Např. e-mail, služby pro vzdálený přístup (VPN, RDP, …)
- Související síťová infrastruktura a ICT procesy

Nejčastější auditní zjištění I.

- Nedostatečná **podpora kybernetické bezpečnosti** vedením organizace.
- Nedostatek lidských zdrojů v oblasti kybernetické bezpečnosti.
- (Ne)řízení dodavatelů.
- Nevhodný rozsah systému řízení bezpečnosti.

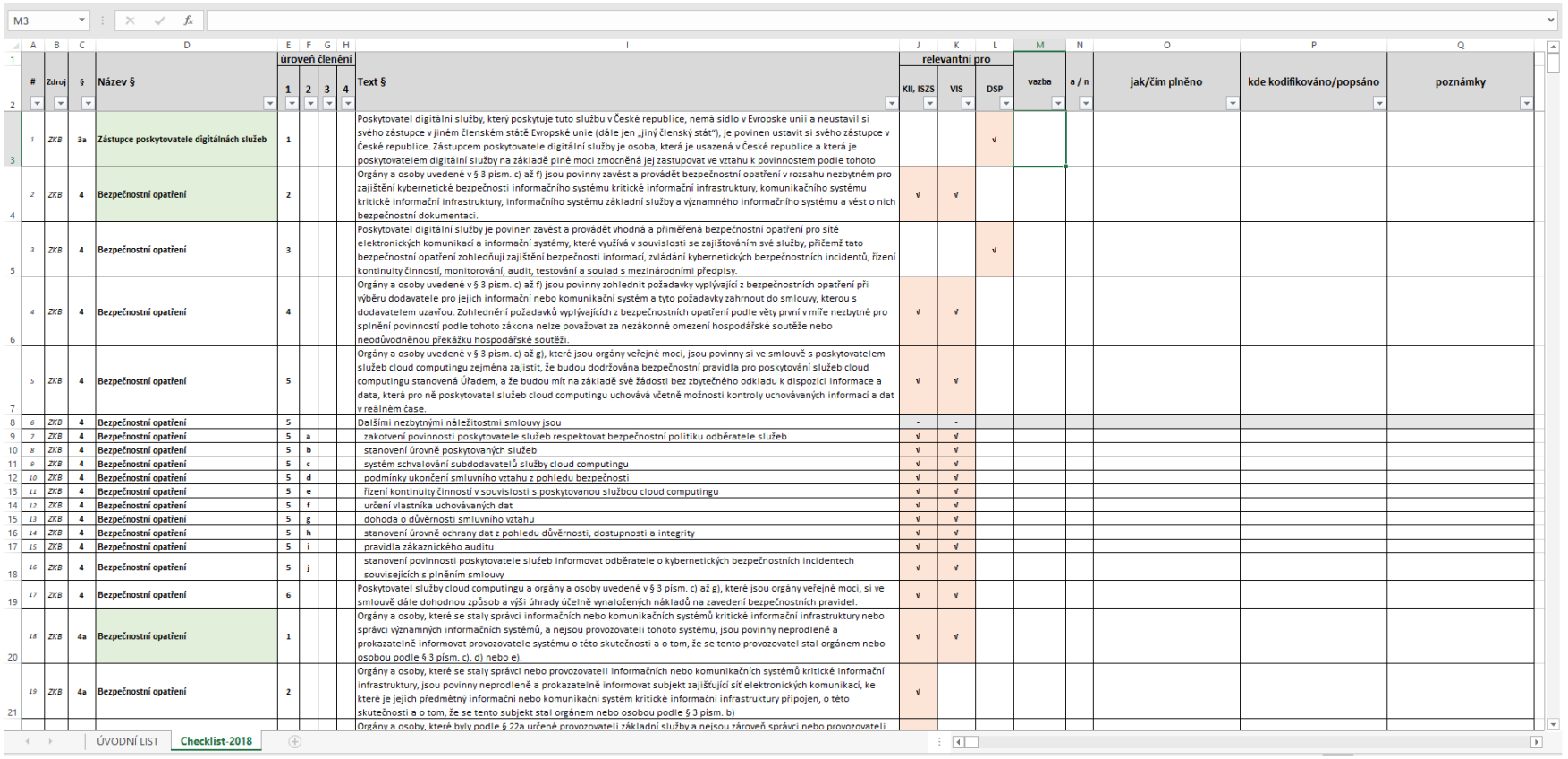
Nejčastější auditní zjištění II.

- Neúplná, nevhodná, neschválená, … **bezpečnostní politika a** dokumentace.
- Nevhodné organizační zařazení kybernetické bezpečnosti.
- Chyby v procesu řízení aktiv a rizik.
- Nedostatečné řízení zranitelností.
- Výjimky z pravidel pro top management.

Nejčastější auditní zjištění III.

- **Občas jsou věci dělány mnohem složitěji, než je nutné.**
- **Nízké bezpečnostní povědomí** uživatelů v oblasti kybernetické bezpečnosti.
- Neexistující centrální bezpečnostní monitoring.

Pomůcka k auditu kybernetické bezpečnosti



#	Zdroj	§	Název §	úroveň členění 1	2	3	4	Text §	relevantní pro KII, ISZS	VIS	DSP	vazba	a / n	jak/čím plněno	kde kodifikováno/popsáno	poznámky
1	ZKB	3a	Zástupce poskytovatele digitálnách služeb	1				Poskytovatel digitální služby, který poskytuje tuto službu v České republice, nemá sídlo v Evropské unii a neustavil si svého zástupce v jiném členském státě Evropské unie (dále jen „jiný členský stát"), je povinen ustavit si svého zástupce v České republice. Zástupcem poskytovatele digitální služby je osoba, která je usazená v České republice a která je poskytovatelem digitální služby na základě plné moci zmocněná jej zastupovat ve vztahu k povinnostem podle tohoto			v					
2	ZKB	4	Bezpečnostní opatření	2				Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému a vést o nich bezpečnostní dokumentaci.	v	v						
3	ZKB	4	Bezpečnostní opatření	3				Poskytovatel digitální služby je povinen zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby, přičemž tato bezpečnostní opatření zohledňují zajištění bezpečnosti informací, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, monitorování, audit, testování a soulad s mezinárodními předpisy.			v					
4	ZKB	4	Bezpečnostní opatření	4				Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.	v	v						
5	ZKB	4	Bezpečnostní opatření	5				Orgány a osoby uvedené v § 3 písm. c) až g), které jsou orgány veřejné moci, jsou povinny si ve smlouvě s poskytovatelem služeb cloud computingu zejména zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu stanovená Úřadem, a že budou mít na základě své žádosti bez zbytečného odkladu k dispozici informace a data, která pro ně poskytovatel služeb cloud computingu uchovává včetně možnosti kontroly uchovávaných informací a dat v reálném čase.	v	v						
6	ZKB	4	Bezpečnostní opatření	5				Dalšími nezbytnými náležitostmi smlouvy jsou	-	-						
7	ZKB	4	Bezpečnostní opatření	5	a			zakotvení povinnosti poskytovatele služeb respektovat bezpečnostní politiku odběratele služeb	v	v						
8	ZKB	4	Bezpečnostní opatření	5	b			stanovení úrovně poskytovaných služeb	v	v						
9	ZKB	4	Bezpečnostní opatření	5	c			systém schvalování subdodavatelů služby cloud computingu	v	v						
10	ZKB	4	Bezpečnostní opatření	5	d			podmínky ukončení smluvního vztahu z pohledu bezpečnosti	v	v						
11	ZKB	4	Bezpečnostní opatření	5	e			řízení kontinuity činností v souvislosti s poskytovanou službou cloud computingu	v	v						
12	ZKB	4	Bezpečnostní opatření	5	f			určení vlastníka uchovávaných dat	v	v						
13	ZKB	4	Bezpečnostní opatření	5	g			dohoda o důvěrnosti smluvního vztahu	v	v						
14	ZKB	4	Bezpečnostní opatření	5	h			stanovení úrovně ochrany dat z pohledu důvěrnosti, dostupnosti a integrity	v	v						
15	ZKB	4	Bezpečnostní opatření	5	i			pravidla zákaznického auditu	v	v						
16	ZKB	4	Bezpečnostní opatření	5	j			stanovení povinnosti poskytovatele služeb informovat odběratele o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy	v	v						
17	ZKB	4	Bezpečnostní opatření	6				Poskytovatel služby cloud computingu a orgány a osoby uvedené v § 3 písm. c) až g), které jsou orgány veřejné moci, si ve smlouvě dále dohodnou způsob a výši úhrady účelně vynaložených nákladů na zavedení bezpečnostních pravidel.	v	v						
18	ZKB	4a	Bezpečnostní opatření	1				Orgány a osoby, které se staly správci informačních nebo komunikačních systémů kritické informační infrastruktury nebo správci významných informačních systémů, a nejsou provozovateli tohoto systému, jsou povinny neprodleně a prokazatelně informovat provozovatele systému o této skutečnosti a o tom, že se tento provozovatel stal orgánem nebo osobou podle § 3 písm. c), d) nebo e).	v	v						
19	ZKB	4a	Bezpečnostní opatření	2				Orgány a osoby, které se staly správci nebo provozovateli informačních nebo komunikačních systémů kritické informační infrastruktury, jsou povinny neprodleně a prokazatelně informovat subjekt zajišťující síť elektronických komunikací, ke které je jejich předmětný informační nebo komunikační systém kritické informační infrastruktury připojen, o této skutečnosti a o tom, že se tento subjekt stal orgánem nebo osobou podle § 3 písm. b)	v							
								Orgány a osoby, které byly podle § 22a určené provozovateli základní služby a nejsou zároveň správci nebo provozovateli								

Zdroj: govcert.cz

Plnění ZKB

- Kybernetické bezpečnostní incidenty
  - Měsíčně hlášeno cca 30 incidentů, dalších cca 50 identifikuje GovCERT sám
- Počet KII – cca 110 systémů u 39 subjektů
  - z toho 50 systémů v soukromém sektoru a 49 ve veřejném
- Počet VIS – 169 systémů u 62 subjektů
  - Celkem pod ZKB spadá cca 268 systémů
- Určování PZS – v srpnu 2018 proces určování spuštěn
- 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 2017
  https://nukib.cz/cs/informacni-servis/publikace/2612-zprava-o-stavu-kyberneticke-bezpecnosti-ceske-republiky-2017/

Stav implementace směrnice NIS v ČR

NIS Directive 2017	ZKB 2015 – 2017	Novela ZKB 1. 8. 2017 ->
Národní strategie kybernetické bezpečnosti	✓	✓
Stanovení bezpečnostních požadavků na IS/KS	✓	✓
Zřídit Cyber Incident Response Teams (CSIRT)	✓	✓
Ustavit národní autoritu v oblasti KB	✓	✓
Stanovit jednotné kontaktní místi pro oblast KB	✓	✓
Určit PZS	⚠ *	
Definovat DSP	✗ **	✓

* Částečně zavedeno – kritická informační infrastruktura

** Nezavedeno

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) - definice

- 1. podmínka:
  - Poskytovatel digitální služby poskytuje službu digitální společnosti (podle zákona o některých službách digitální společnosti):

    „služba poskytovaná zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb“
- 2. podmínka:
  - 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) – Online tržiště

A. **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

- **Definice je složitá – ale je převzatá z NIS**

DSP – co je tedy tím „On-line tržištěm“

- **Za on-line tržiště se považují**
  - platformy, které vystupují jako prostředník mezi prodávajícími podnikateli (prodávající) a spotřebiteli a podnikateli (zde v pozici kupujících) a umožňuje prodej zboží či služeb.
  - Jedná se o službu, která umožňuje spotřebitelům a podnikatelům (kupujícím) uzavírat s prodávajícími podnikateli (prodávající) smlouvy přímo prostřednictvím on-line tržiště, a to s konečnou platností.

- **Za on-line tržiště se <u>nepovažují</u> webové stránky, které**
  - přesměrovávají uživatele na další webové stránky, aby až tam uzavřeli smlouvu (např. srovnávače cen)
  - slouží pouze k propojení prodávajících podnikatelů (prodávajících) se spotřebiteli a prodávajícími (kupující) (např. inzertní webové stránky)
  - slouží prodávajícímu podnikateli (prodávající) přímo k prodeji zboží spotřebitelům a prodávajícím (kupující)(např. online maloobchod).

DSP - „Internetový vyhledávač“ a „Cloud“

B. Internetový vyhledávač

- umožňuje provádět vyhledávání v zásadě na všech internetových stránkách,
- na základě dotazu uživatele na jakékoliv téma v podobě klíčového slova, sousloví nebo jiného zadání,
- služba poskytuje odkazy, na nichž lze nalézt informace související s požadovaným obsahem

C. Cloud computing

- digitální služba umožňující přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů, které je možno sdílet.
- **Nepatří sem firemní cloudy sloužící pro uzavřenou skupinu**
- Tento pojem tak zahrnuje různé typy cloud computingu:
  - IaaS (Infrastructure asa Service),
  - PaaS (Platform as a Service) nebo
  - SaaS (Software as a Service).

- Více k DSP a jejich identifikaci:

https://nukib.cz/download/kii-vis/Definice_DSP_v1.pdf

Určování provozovatelů základních služeb (PZS) - obecně

- PZS jsou 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 – nepředpokládáme výrazné množství PZS (výjimky - např. zdravotnictví)

Určování provozovatelů základních služeb (PZS) - kritéria

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

1. **Definice ZKB**
   - Závislost služby 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 (NIS)

- Směrnice v čl. 6 stanoví okolnosti (dopady kybernetického bezpečnostního incidentu), které mají státy při určení zvážit:

a) počet uživatelů, kteří jsou závislí na službě	d) podíl daného subjektu na trhu
b) závislost dalších odvětví na službě poskytované daným subjektem	e) zeměpisný rozsah oblasti, která by mohla být incidentem dotčena
c) možný dopad incidentů pokud jde o jejich intenzitu a délku trvání, na ekonomické a společenské činnosti nebo veřejnou bezpečnost	f) důležitost subjektu, pokud jde o udržování dostatečné úrovně dané služby, s přihlédnutím k dostupnosti alternativ

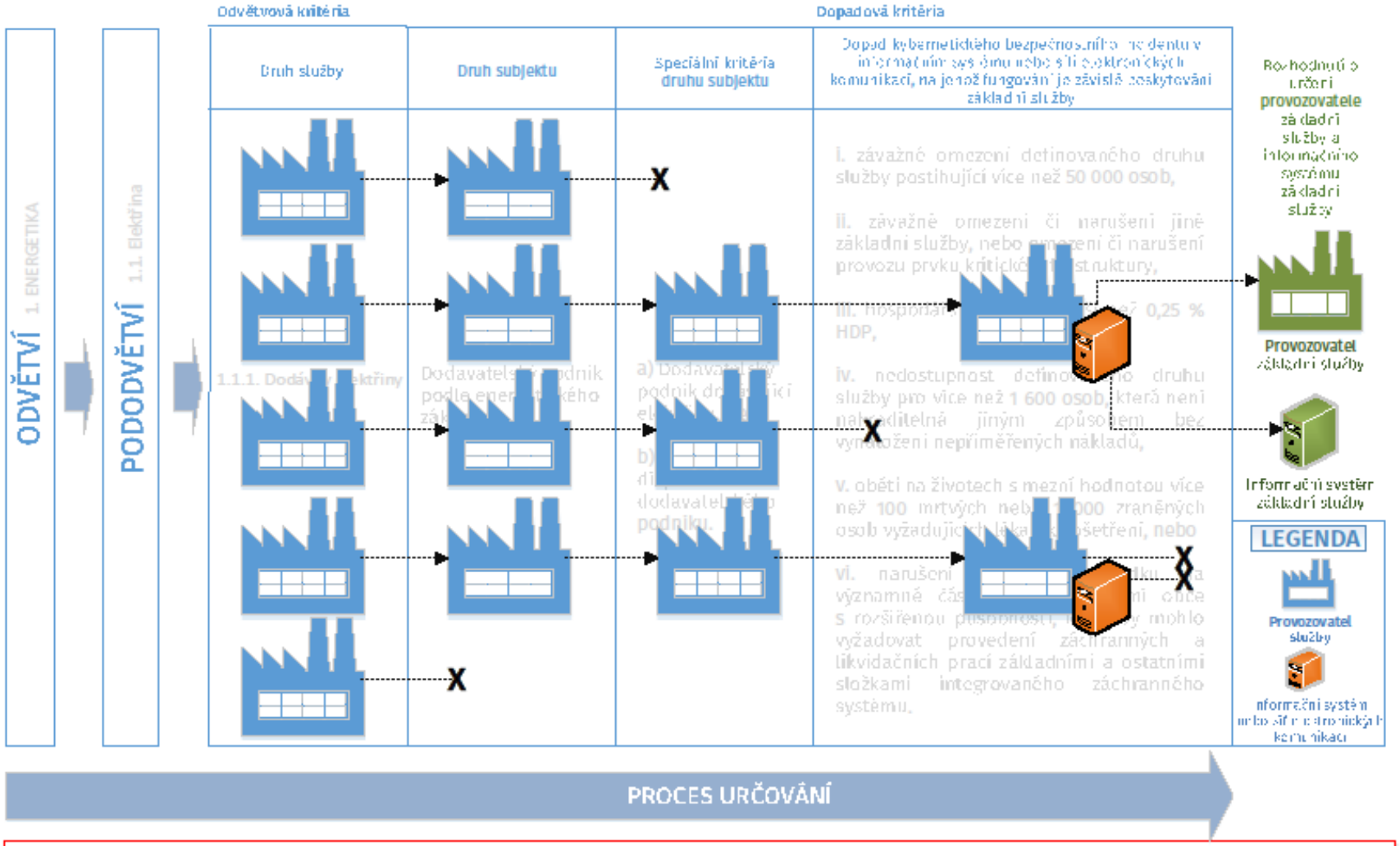
- Na základě těchto požadavků byla konstruována dopadová kritéria, která musí být incidentem v posuzovaném informačním systému nebo síti elektronických komunikací (komunikačním systému) naplněna

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:

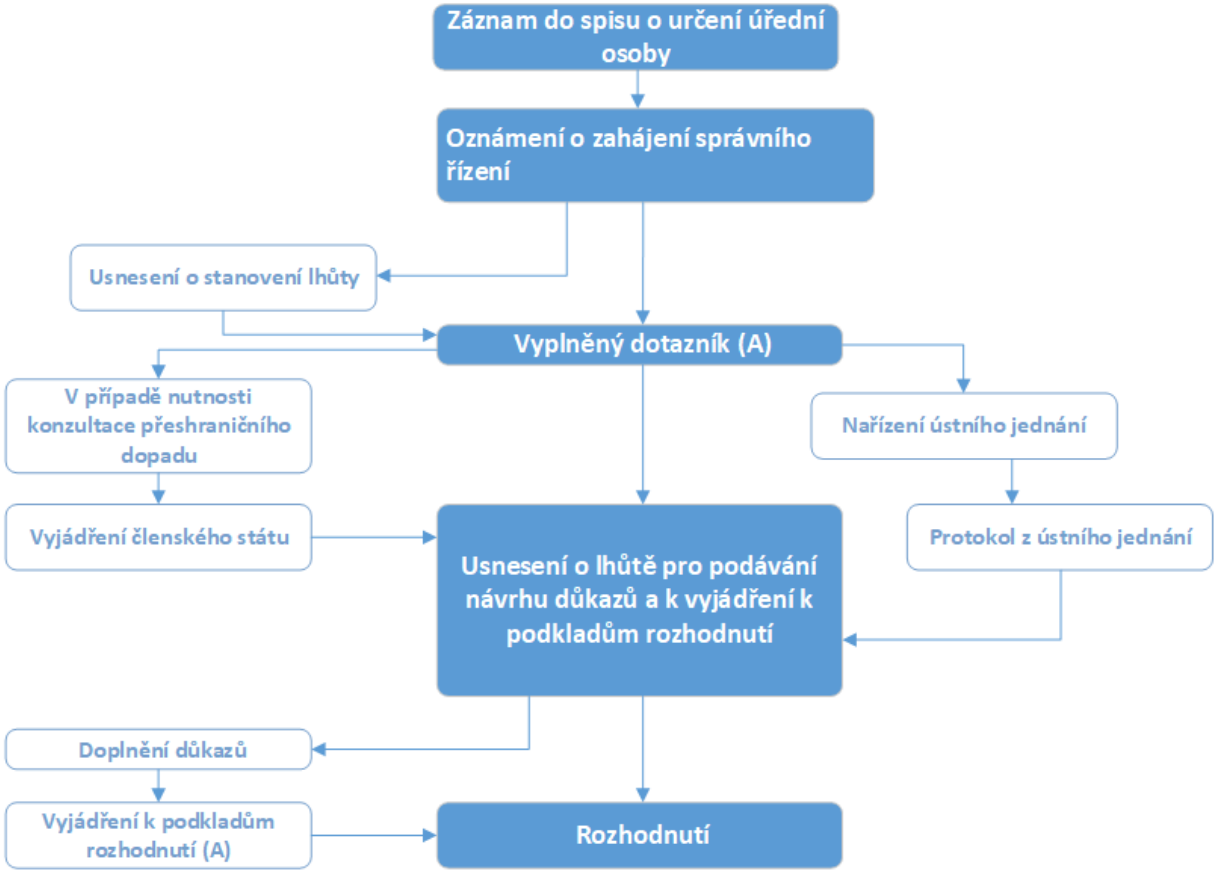
Dokument slouží pouze jako podpůrné vodítko, nenahrazuje žádný ze zákonů a souvisejících prováděcích předpisů. Právo změny tohoto dokumentu vyhrazeno. Další šíření tohoto dokumentu je možné pouze s písemným souhlasem Národního úřadu pro kybernetickou a informační bezpečnost.

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/

Provozovatel základní služby (PZS) – proces určení

- Určení/neurčení probíhá ve správním řízení a je zakončeno rozhodnutím
- Proces správního řízení je následující



Dotazy?

Děkuji za pozornost.

Více informací zde: https://nukib.cz/cs/kyberneticky-zakon/podpurne-materialy/