Budoucí regulace kybernetické bezpečnosti v oblasti vědy a výzkumu a vysokého školství

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

říjen 2022

TLP: AMBER

Odbor regulace
NÚKIB

NÚKIB a předmět dnešní schůzky

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost (a další činnosti).

Vznikl 1. srpna 2017 na základě novelizace zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

Tento zákon spolu s prováděcími právními předpisy spadá do jeho gesce, stejně tak jako veškeré otázky spojené s agendou kybernetické bezpečnosti.

Jedním z úkolů úřadu je předkládat novou legislativu nebo legislativní úpravy týkající se kybernetické bezpečnosti.

Nová směrnice NIS2

- Směrnice NIS2 navazuje na obsah směrnice NIS1 přijaté v roce 2016 a prohlubuje regulaci kybernetické bezpečnosti v Evropské unii.
  - přináší zejména velké rozšíření povinných osob
  - nové požadavky na bezpečnostní opatření i hlášení incidentů
  - razantní navýšení pokut za neplnění povinností
  - a mnohé další
- Obsah **evropských směrnic je potřeba převést do národního práva členských států** (nelze pouze odkázat na evropský předpis).
- Stav: Aktuálně politická shoda na úrovni Evropské unie nalezena, finalizován text, **publikace plánována v 4Q 2022** (transpoziční lhůta 21 měsíců).

- **Návrh zákona a prováděcích právních předpisů bude dán do legislativního procesu v první polovině roku 2023.** Mezirezortní připomínkové řízení v polovině roku.

- Implementace do národního práva se předpokládá v polovině roku 2024.

Disclaimer

Ačkoli již byla v rámci unijního legislativního procesu nalezena předběžná shoda ohledně budoucí podoby směrnice NIS2, finální text směrnice dosud nebyl schválen a publikován v Úředním věstníku Evropské unie.

Výsledná podoba směrnice se tedy ještě může měnit.

Informace publikované v této prezentaci vycházejí z posledních veřejně dostupných verzí směrnice a mohou být do budoucna upraveny v závislosti na finální podobě textu.

V rámci legislativního procesu mohou prezentované závěry projít změnami.

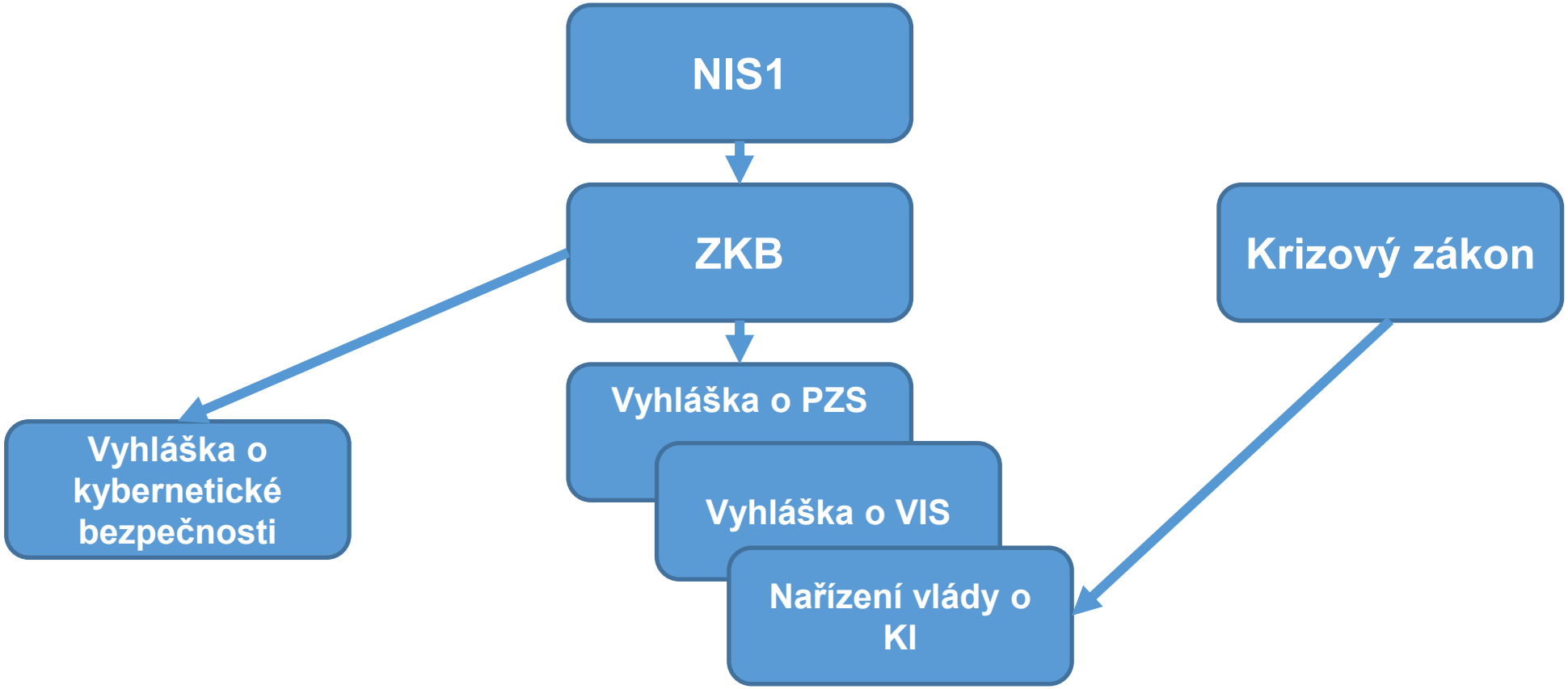
Nová směrnice NIS2

Doposud nezveřejněna (na konci roku 2022).

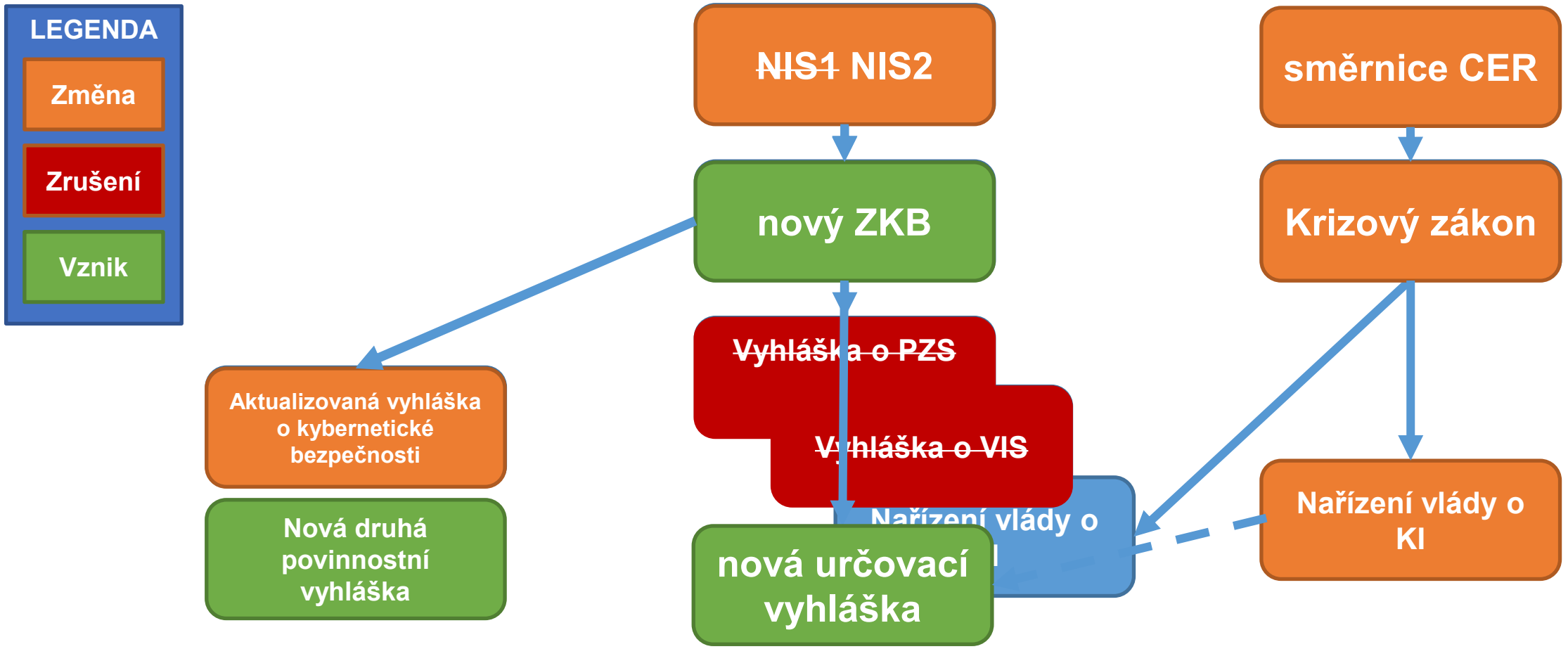
Nejaktuálnější verze zde: NIS2_aktuální_znění.pdf (nukib.cz)

1. **General provisions** (čl. 1 – čl. 4)
   obecná ustanovení, rozsah, stanovení povinných osob, definice
2. **Coordinated cybersecurity regulatory frameworks** (čl. 5 – čl. 11)
   policy na národní úrovni
3. **EU cooperation** (čl. 12 – čl. 16)
   policy na evropské úrovni
4. **Cybersecurity risk management and reporting obligations** (čl. 17 – čl. 25)
   regulace
5. **Information sharing** (čl. 26 a čl. 27)
   zlepšení prostředí kybernetické bezpečnosti
6. **Supervisory and enforcement** (čl. 28 – čl. 34)
   dohled a ukládání pokut
7. **Transitional and final provisions** (čl. 35 – čl. 43)
   závěrečná ustanovení

Návrh změny – současný stav



Návrh změny – budoucí chtěný stav



Konkrétní změny – povinné osoby

Aktuálně regulováno cca **400** povinných osob

Nově regulováno minimálně **6 000** povinných osob
(tzn. min 15x tolik)

Proč?

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential".

ENERGETIKA

Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu

Subjekty poskytující službu dálkového vytápění nebo chlazení.

Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení.

Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.

DOPRAVA

Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.

Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.

Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.

Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ

Sektor bankovnictví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ

Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ

Poskytovatelé zdravotní péče (nemocnice a další), subjekty

PITNÁ VODA

Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA

Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA

Poskytovatelé: výměnných uzlů internetu (IXP), cloud

systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

VEŘEJNÁ SPRÁVA

Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik" a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik" a „střední podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important" (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

CHEMICKÝ PRŮMYSL

Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POSKYTOVATELÉ DIGI SLUŽEB

Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

Koho se budou nové povinnosti týkat I.

- Okruh odvětví regulovaných NIS2 je uveden v přílohách I a II.
  - Směrnicí je regulováno cca 60 služeb v 18 odvětvích
- **Regulace se netýká každého v daném odvětví** – musí splnit kritéria:
  - organizace poskytuje **alespoň jednu službu uvedenou v přílohách směrnice, a zároveň**
  - **je středním nebo velkým podnikem**, tedy zaměstnává 50 a více zaměstnanců, nebo dosahuje ročního obratu nebo bilanční sumy roční rozvahy alespoň 10 milionů EUR (zhruba 250 milionů CZK).
- ! Počítání podniku – nutno zohlednit i majetkově propojené společnosti

Doporučení Komise 2003/361/ES z 6. května 2003

Kategorie podniku	Počet zaměst-nanců: roční pracovní jednotka (RPJ)	Roční obrat	nebo	Bilanční suma roční rozvahy
Střední podnik	< 250	≤ 50 milionů EUR	nebo	≤ 43 milionů EUR
Malý podnik	< 50	≤ 10 milionů EUR	nebo	≤ 10 milionů EUR
Mikropodnik	< 10	≤ 2 miliony EUR	nebo	≤ 2 miliony EUR

Evropská Komise, Uživatelská příručka k definici malých a středních podniků, PDF ISBN 978-92-79-69931-3 doi:10.2873/117802 ET-01-17-660-CS-

Koho se budou nové povinnosti týkat II.

- **Velikost organizace ve spojení se službou je sice primárním způsobem určení, ale také není jediným.**
- U některých vyjmenovaných služeb je stanoveno, že pod regulaci směrnice NIS2 budou **spadat všechny organizace**, nehledě na jejich velikost.
- Členské státy mají také k zařazení do regulace využit dodatečných kritérií a vztáhnout regulaci i na takové organizace, které **poskytují služby uvedené v přílohách, a zároveň bez ohledu na velikost**
  - jsou **jedinými poskytovateli** služby, která je nezbytná v členském státě ze sociálního nebo ekonomického hlediska,
  - by narušení jejich služby mohlo mít **významný dopad** na veřejnou bezpečnost nebo zdraví osob,
  - by narušení jejich služby mohlo vyvolat **významné riziko, zejména s přeshraničním dopadem**.
- Posledním specifickým způsobem určení je **propojení směrnice NIS2 s tzv. směrnicí CER (směrnice týkající se budoucí kritické infrastruktury)** – kdo bude povinnou osobou podle CER (neznámá množina) – bude povinou osobou podle NIS2

Současné znění zákona o kybernetické bezpečnosti

§ 3 Orgány a osobami, kterým ládají povinnosti v oblasti kybernetické bezpečnosti, jsou

a) **poskytovat elektronických unikací** a **subjekt zajišťující síť elekt komunikací**,
b) orgán nebo osoba zajišť **významnou síť,**
c) správce a provozovatel informačního systému **kri é informační infrastruktury,**
d) správce a provozovatel komunikačn mu **kritické inf ní infrastruktury,**
e) správce a provozovatel **význam informač stému,**
f) správce a provozovatel i ního syst u základní služby,
g) **provozovatel základ žby,** a
h) **poskytovatel digitální služby**

směrnice NIS2
směrnice NIS2
směrnice NIS2
národní úprava
směrnice NIS2
směrnice NIS2

Současné znění zákona o kybernetické bezpečnosti

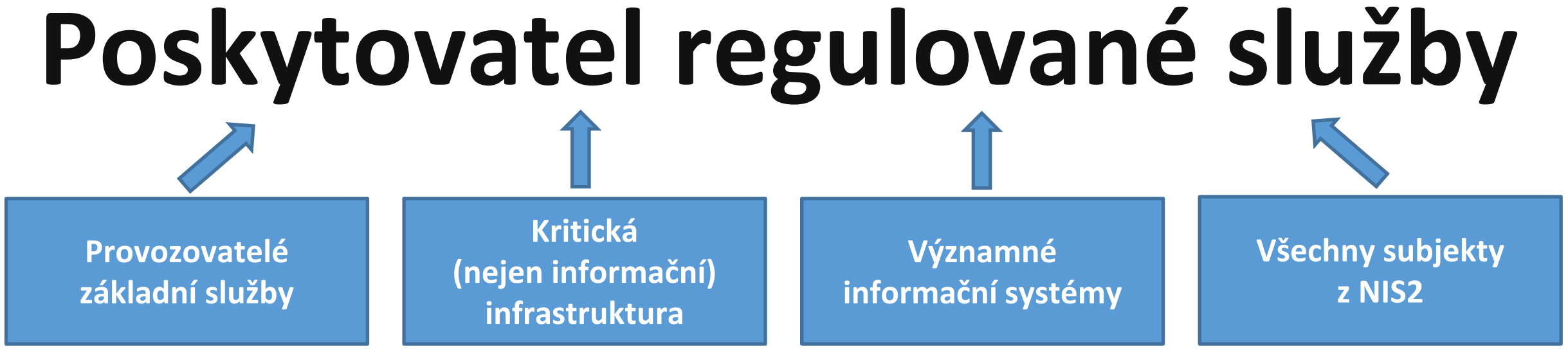
§ 3 Orgány a osobami, kterým [illegible]ádají povinnosti v oblasti kybernetické bezpečnosti, jsou

a) **poskytovat[illegible] elektronických [illegible]unikací** a **subjekt zajišťující síť elekt[illegible]í komunikací**,
b) orgán nebo osoba zajišťu[illegible] **významnou síť,**
c) správce a provozovatel informačního systému **kriti[illegible]é informační infrastruktury,**
d) správce a provozovatel komunikačn[illegible]ího **kritické inf[illegible]ní infrastruktury,**
e) správce a provozovatel **význam[illegible] informač[illegible]stému,**
f) správce a provozovatel i[illegible]ního systém[illegible]u **základní služby,**
g) **provozovatel základ[illegible]žby,** a
h) **poskytovatel digitální služby**.

směrnice NIS2
směrnice NIS2
směrnice NIS2
národní úprava
směrnice NIS2
směrnice NIS2

Nové znění zákona o kybernetické bezpečnosti

Jedna jediná povinná osoba*:



*Pro primární sadu některých povinností spojených s prevencí – zavádění bezpečnostních opatření, hlášení incidentů, apod.

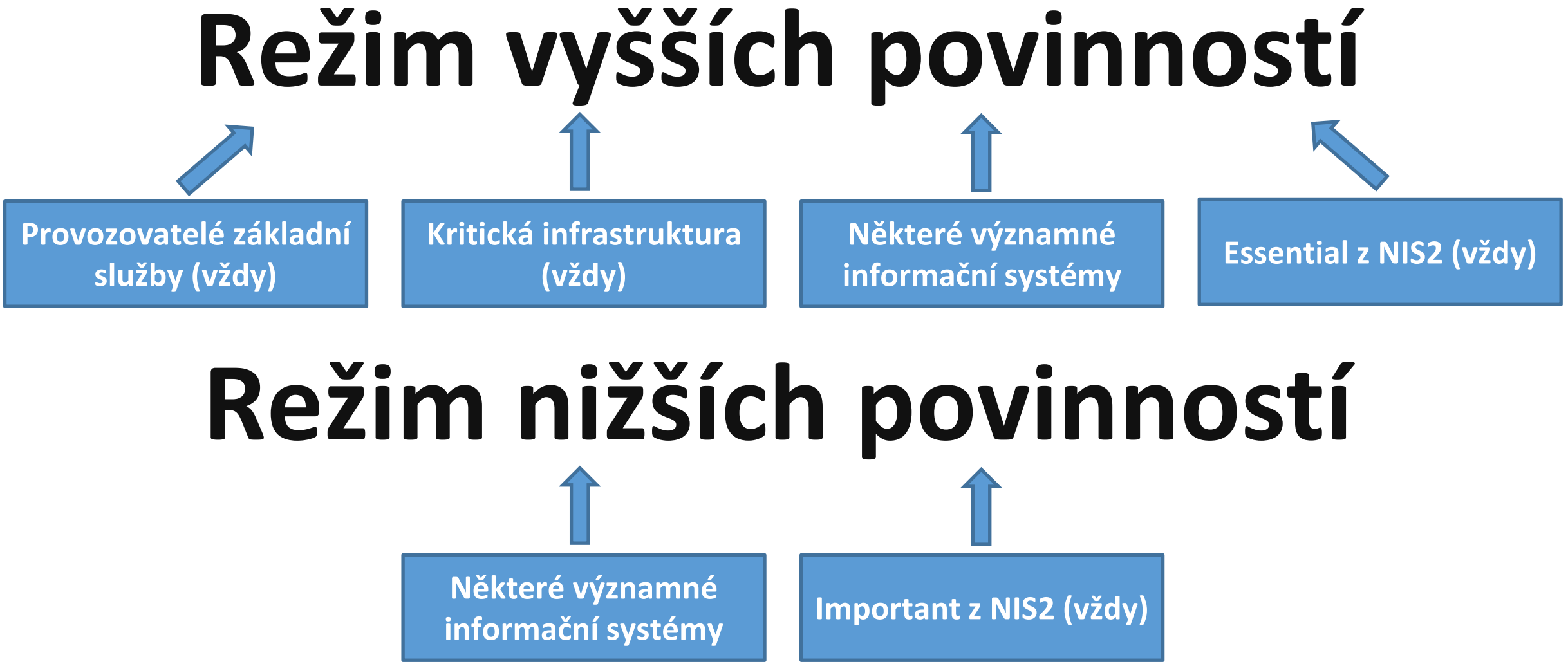
Režimy povinné osoby podle směrnice NIS2

*„Entities falling within the scope of this Directive should be **classified into two categories,** essential and important reflecting the level of criticality of the sector or of the type of services they provide, as well as their size.“*

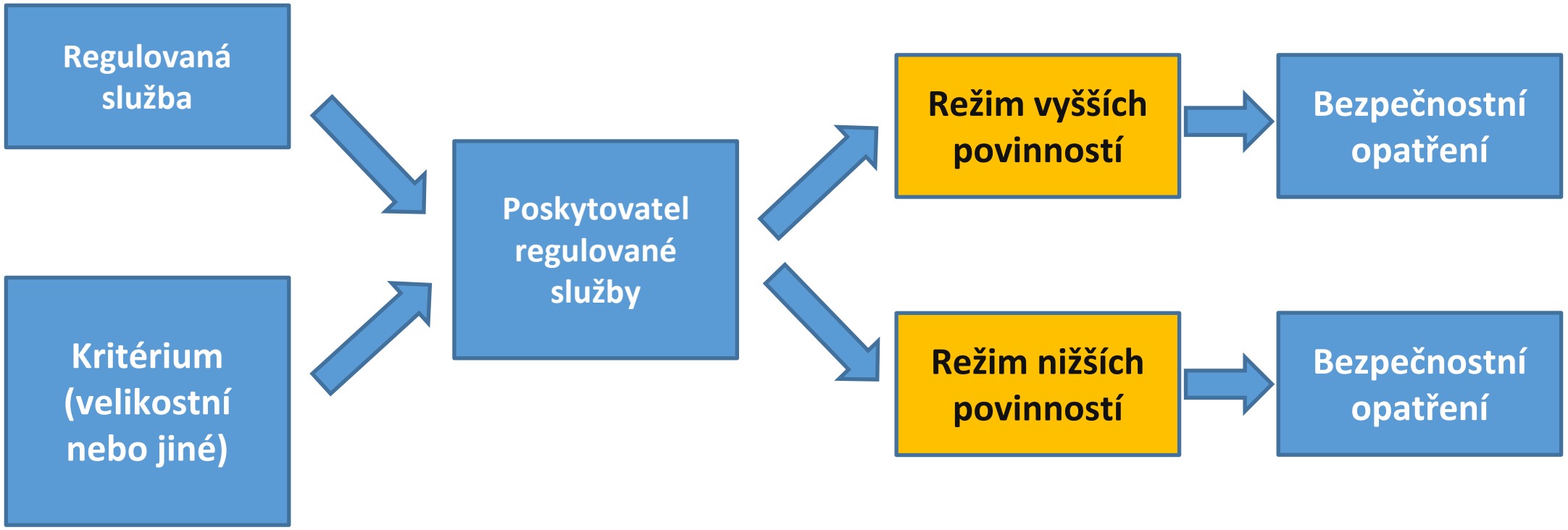
Essential entities (základní)

Important entities (významné)

Nové znění zákona o kybernetické bezpečnosti



Shrnutí stanovení povinných osob



Bezpečnostní opatření

Směrnice stanovuje okruhy bezpečnostních opatření, které mají členské státy rozpracovat ve svých právních předpisech a uložit je budoucím povinným osobám (aktuální čl. 18 NIS2):

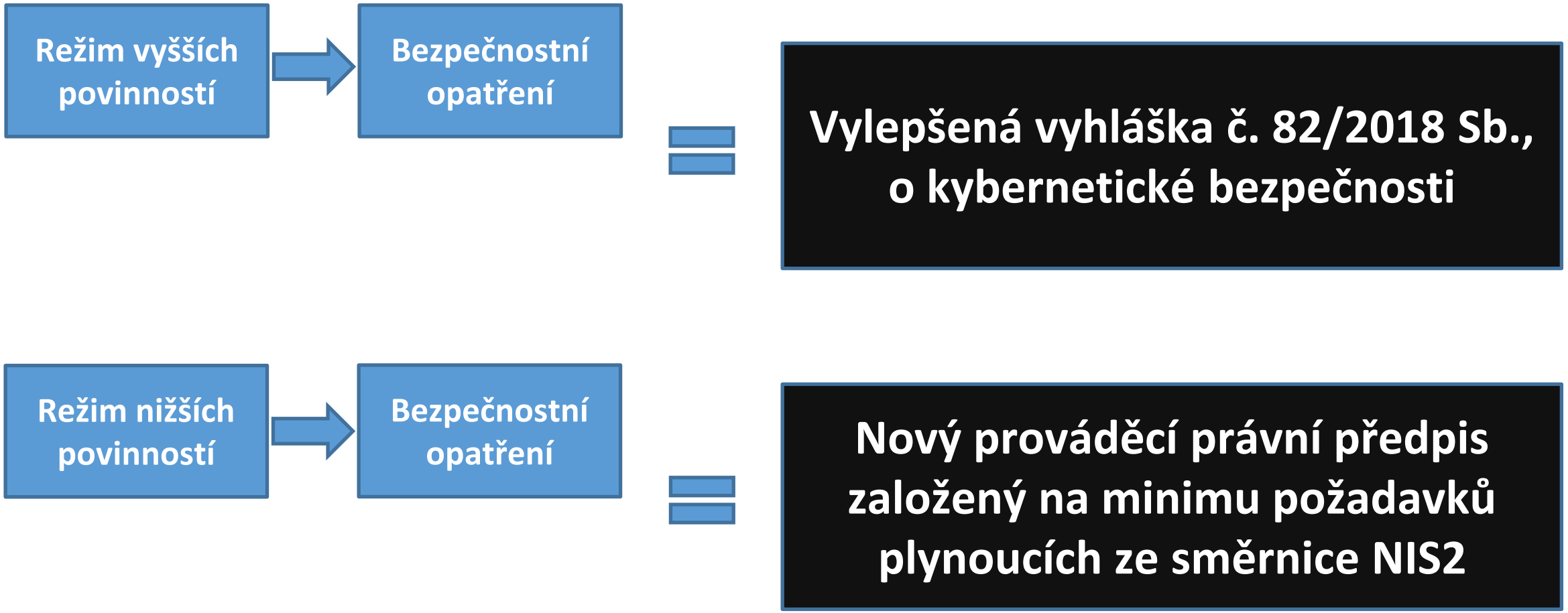
- **Analýza rizik** a **politiky bezpečnosti informací;**
- **Zvládání incidentů;**
- **Kontinuita činností** (tj. business kontinuita), přičemž směrnice tento okruh ještě rozvádí o příklad zálohování, zotavení (disaster recovery) a krizové řízení;
- Bezpečnost v rámci **dodavatelského řetězce;**
- Bezpečnost v rámci **pořízení, vývoje a údržby systémů;**
- Politiky a postupy pro hodnocení účinnosti bezpečnostních opatření (tj. **audit**);
- Praktiky **základní počítačové hygieny a vzdělávání** v oblasti kybernetické bezpečnosti;
- Politiky a postupy týkající se využívání **kryptografie** a tam, kde je to vhodné, také šifrování;
- **Bezpečnost lidských zdrojů, řízení přístupů a aktiv;**
- Využívání **vícefaktorového ověření identity, bezpečných komunikačních nástrojů** a **nástrojů pro nouzovou komunikaci.**

+ Povinné vzdělávání vrcholového vedení organizace (aktuální čl. 17 NIS2)**.**

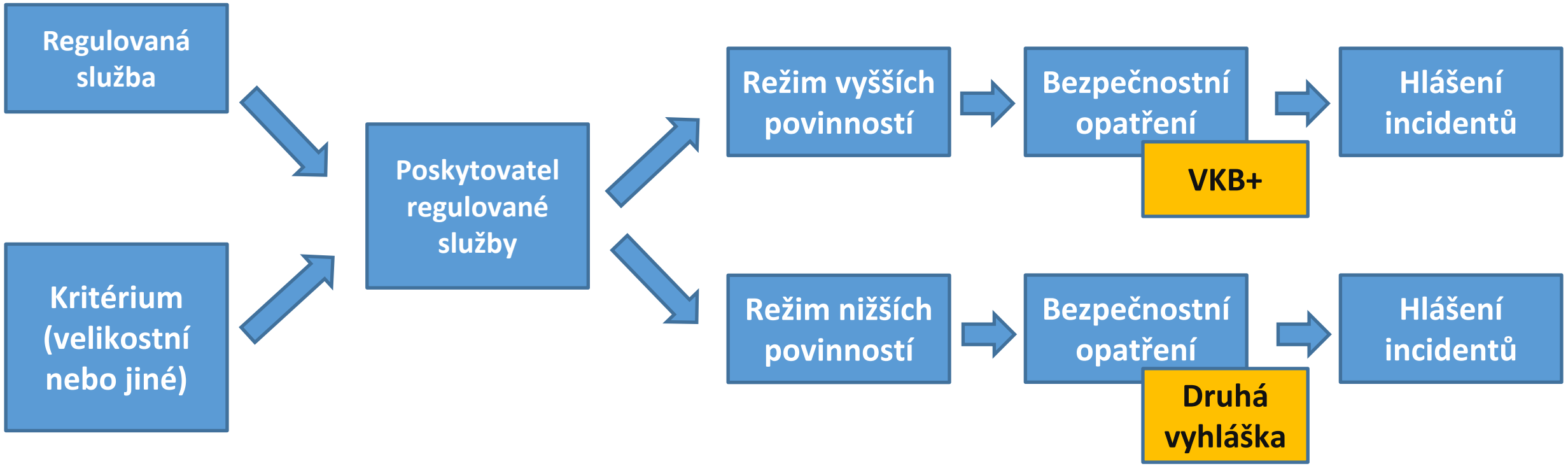
*„**All-hazard approach** includes the **protection of network and information systems and their physical environment from any event such as theft, fire, flood, telecommunications or power failures or from any unauthorised physical access and damage to and interference with the entity's information and information processing facilities** that could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.*

***The risk management measures** should therefore also address the **physical and environmental security** by including measures to protect the entity's **network and information systems from system failures, human error, malicious actions or natural phenomena** (…). In this regard, entities should, as part of their risk management measures, also address **human resources security** and have in place appropriate **access control policies**."*

Shrnutí stanovení povinných osob



Shrnutí stanovení povinných osob



Hlášení kybernetických bezpečnostních incidentů

Kybernetickým bezpečnostním incidentem se rozumí narušení bezpečnosti informací v rámci aktiv (související s regulovanou službou).

Hlášení kybernetického bezpečnostního incidentu na NÚKIB

= jen ty, které mají původ v kybernetickém prostoru.

Pro hlášení je potřeba posoudit dvě situace:

1) **významný dopad na poskytování regulované služby**
2) **? úmyslné zavinění kybernetického bezpečnostního incidentu**

Shrnutí hlášení incidentů

Poskytovatel regulované služby

Režim vyšších povinností

Hlásí vše
(s původem v kybernetickém prostoru)

Režim nižších povinností

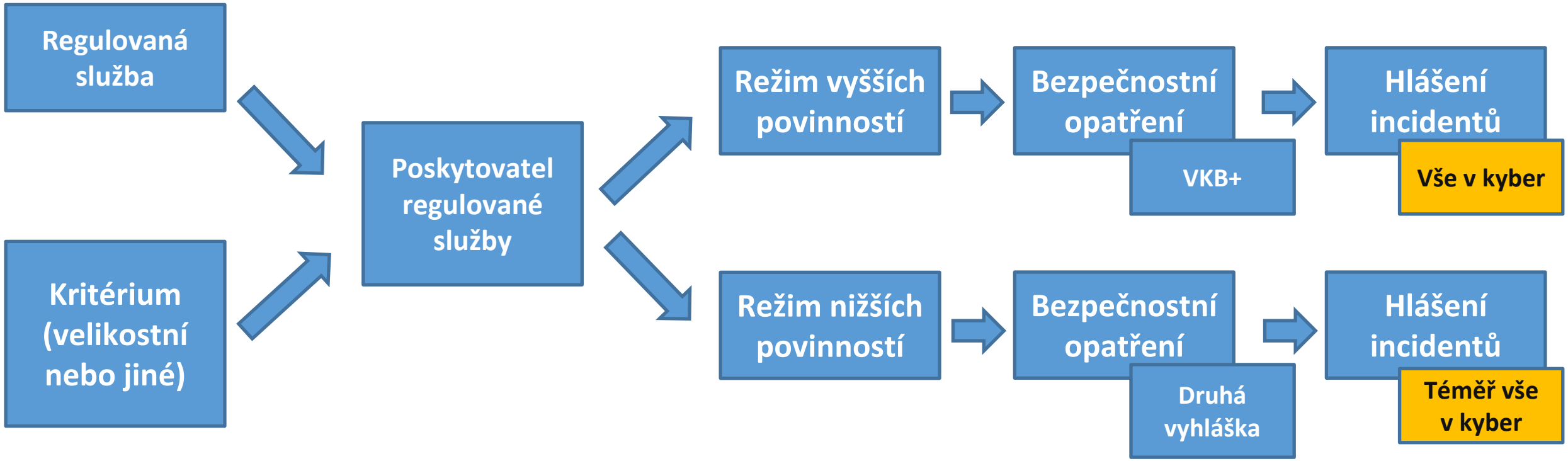
významný dopad
+
úmyslné zavinění

významný dopad
+
neúmyslné zavinění

nevýznamný dopad
+
úmyslné zavinění

*významnost stanoví sám subjekt dle co nejjednoduššího postupu v prováděcím právním předpise

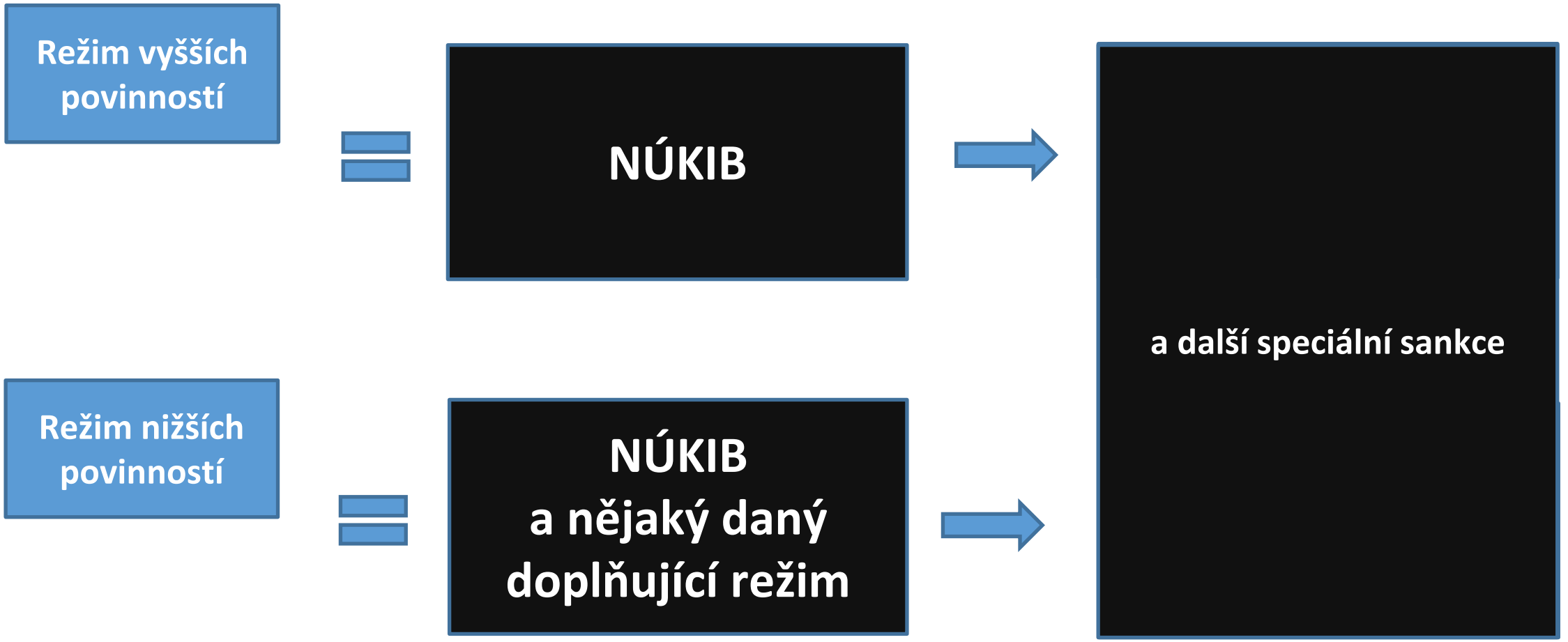
Shrnutí stanovení povinných osob



Opatření

Až na drobné, spíše procesní a textové, změny zůstávají tak jako nyní.

Kontrola a sankce



Registrace a komunikace s NÚKIB

- Aby to celé fungovalo je nezbytné změnit styl, jakým dnes probíhá
  - určování povinných osob (nově primárně samoidentifikací)
  - hlášení kybernetických bezpečnostních incidentů
  - komunikace s Úřadem
  - sdílení informací o zranitelnostech

- Aby to fungovalo rychle, pružně a bez zbytečné administrativy je třeba všechny tyto činnosti komplet **elektronizovat** a **zautomatizovat**.

- Řešením je **vznik jednotného systému,** skrze který bude realizována
  - registrace poskytovatele regulované služby,
  - hlášení incidentů (nejen) poskytovatele regulované služby,
  - sdílení informací o známých zranitelnostech a hrozbách.

One more thing...

na NÚKIB vznikla díky spolupráci odboru regulace, oddělení komunikace a oddělení vzdělávání

stránka

nis2.nukib.cz

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Prostor pro dotazy

(pokračují dotazy NÚKIB)

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Konkrétní otázky

Směrnice NIS2

Rec 86: Research activities play a key role in the development of new ICT products and ICT processes. Many of those activities are carried out by entities that share, disseminate or exploit the results of their research for commercial purposes. Those entities can therefore be important players in value chains, which makes the security of their network and information systems an integral part of the overall cybersecurity of the internal market. Research organisations should be understood to include entities which focus the essential part of their activities on the conduct of applied research or experimental development, within the meaning of the Organisation for Economic Cooperation and Development's Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development, with a view to exploiting their results for commercial purposes, such as the manufacturing and marketing of a product, process or the provision of a service.

Čl. 2/3: Member States may provide for this Directive to apply to: (…)

(b) education institutions, in particular where they carry out critical research activities.

Čl. 6/41: 'research organisation' means an entity which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions.

Čl. 7/2/g): As part of the national cybersecurity strategy, Member States shall in particular adopt policies (…) g) supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure

Příloha II, Sector 7. Research; Type of Entity: Research organisations

Regulovaná služba	
Služba	Kritérium **poskytovatele regulované služby**
Výzkum a vývoj	Vysoká škola provádějící [kritickou] výzkumnou činnost nebo výzkumná organizace, jejímž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj za účelem využití tohoto výzkumu pro komerční účely, je I) poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je správcem velké výzkumné infrastruktury, b) je v rámci modulu [xy podle M17] hodnocena jako [xy] Nebo v rámci metodiky úrovně technologické připravenosti hodnotí zralost technologií na úrovni TRL 5 a vyšší II) poskytovatel regulované služby v režimu nižších povinností, v případě, že: a) je velkým podnikem, b) je středním podnikem, c) je Akademií věd České republiky, nebo d) většina prováděných výzkumných projektů je financována z více než 50 % z veřejných zdrojů.

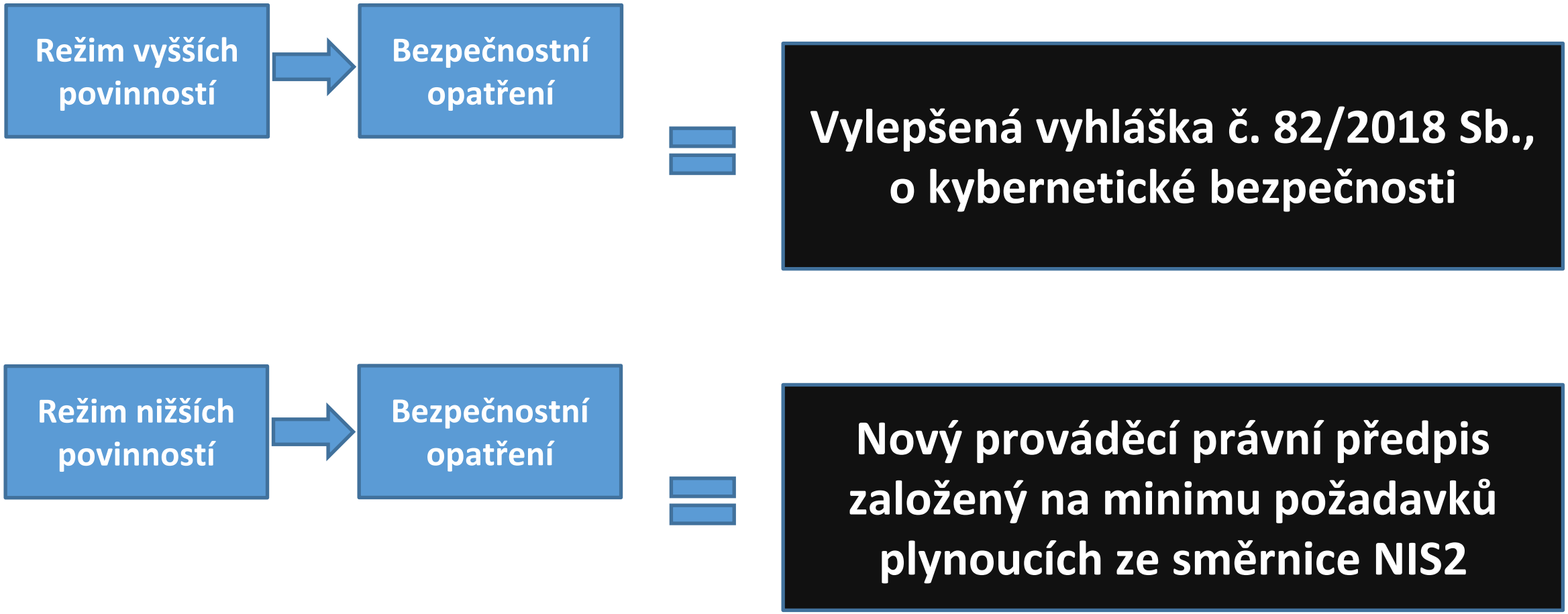
NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

1. Chybějící služby?
2. Chybějící kritéria?
3. Zlepšení srozumitelnosti a pochopitelnosti? Nekonzistentnost?
4. Další poznámky/připomínky?

Regulovaná služba	
Služba	Kritérium **poskytovatele regulované služby**
Výzkum a vývoj	Vysoká škola provádějící [kritickou] výzkumnou činnost nebo výzkumná organizace, jejímž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj za účelem využití tohoto výzkumu pro komerční účely, je I) poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je správcem velké výzkumné infrastruktury, b) je v rámci modulu [xy podle M17] hodnocena jako [xy] Nebo v rámci metodiky úrovně technologické připravenosti hodnotí zralost technologií na úrovni TRL 5 a vyšší II) poskytovatel regulované služby v režimu nižších povinností, v případě, že: a) je velkým podnikem, b) je středním podnikem, c) je Akademií věd České republiky, nebo d) většina prováděných výzkumných projektů je financována z více než 50 % z veřejných zdrojů.

Konkrétní otázky – bezpečnostní opatření



NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Povinnostní vyhlášky

Dotaz na již určené povinné osoby mezi vámi:

1. Jakou máte zkušenost s implementací zákonných povinností dle aktuálního znění zákona o kybernetické bezpečnosti a jeho prováděcích předpisů?
2. Na základě zkušeností s dosavadní regulací kybernetické bezpečnosti, napadají Vás nějaké podněty k jejímu zlepšení?
3. Jakým způsobem s Vámi dodavatelé ICT technologií spolupracují na plnění Vašich bezpečnostních požadavků k řádnému zabezpečení Vašich ICT systému?
4. Pokud jste správci informačního a komunikačního systému, kolik máte určených významných dodavatelů (vůči celkovému počtu dodavatelů)?
5. Je pro Vás nějaká oblast v rámci Systému řízení bezpečnosti informací ve Vaší organizaci problematická?

Konkrétní otázky – hlášení incidentů

Kybernetickým bezpečnostním incidentem se rozumí narušení bezpečnosti informací v rámci aktiv (související s regulovanou službou).

Hlášení kybernetického bezpečnostního incidentu na NÚKIB

= jen ty, které mají původ v kybernetickém prostoru.

Pro hlášení je potřeba posoudit dvě situace:

1) **významný dopad na poskytování regulované služby**
2) **? úmyslné zavinění kybernetického bezpečnostního incidentu**

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Hlášení incidentů

1. Jakým způsobem ve Vaší organizaci vyhodnocujete incidenty?
2. Kolik různých i jiným subjektům nežli NÚKIB (co a kam)?
3. Jaká je podle Vás schopnost vyhodnotit:
   - zda má KBI „původ v kybernetickém prostoru“
   - dopad a jak se proměňuje v čase
   - úmyslnost zavinění

Dotaz na již určené povinné osoby mezi vámi:

1. Zajímá nás konktrétně jakým způsobem určíte co je provozní událost a co je již pro Vás kybernetický incident ve smyslu § 7 zákona o kybernetické bezpečnosti?
2. Byla vám ze strany CERT poskytnuta relevantní podpora?

Děkujeme za spolupráci!

regulace@nukib.cz