NIS2 AKTUÁLNĚ

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Rok informatiky
31. května 2023
Telč
TLP:CLEAR

Adam Kučínský
ředitel odboru regulace
Daniela Procházková
vedoucí oddělení regulace veřejného sektoru

Co potřebujeme vědět na začátku

- *Prezentace má informační a osvětových charakter a informace v ní obsažené se mohou se v čase změnit.*

- Základem změn je nově přicházející **směrnice NIS2** (= viz dále), ale také potřeba zákon o kybernetické bezpečnosti aktualizovat
- Do návrhu zákona jsou promítnuty také vnitrostátní instituty, zejména Mechanismus prověřování bezpečnosti dodavatelského řetězce
- Směrnice obecně je legislativní akt Evropské unie, který není sám o sobě aplikovatelný **(= musí nejdříve vzniknout národní úprava)**
- Národní úřad pro kybernetickou a informační bezpečnost **připravil návrh nového zákona o kybernetické bezpečnosti** (= zveřejněn k zasílání podnětů, aktuálně ukončeno)
- Návrh zákona a prováděcích právních předpisů bude **předložen do legislativního procesu v květnu/červnu 2023**
- **Nová pravidla by měla platit v polovině roku 2024** (do 17. října 2024 v souladu se směrnicí NIS2)
- Jsme na začátku oficiálního legislativního procesu – může proběhnout ještě řada změn

Regulované služby (směrnice NIS2)

Směrnice NIS1 (stávající ZKB):

30 služeb v 7 odvětvích

Kritéria dopadu incidentu

⇒ **cca 400 povinných osob**

Směrnice NIS2 (nový ZKB):

60 služeb v 18 odvětvích

Kritérium velikosti subjektu

⇒ **cca 6000 povinných osob**

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 s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.

Subjekty poskytující službu dálkového vytápění nebo chlazení.

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

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

Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

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 provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

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 computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB

Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA

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

VESMÍR

V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

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.

POŠTOVNÍ SLUŽBY

Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ

Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL

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

POTRAVINÁŘSTVÍ

Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA

Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB

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

VÝZKUM

Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.

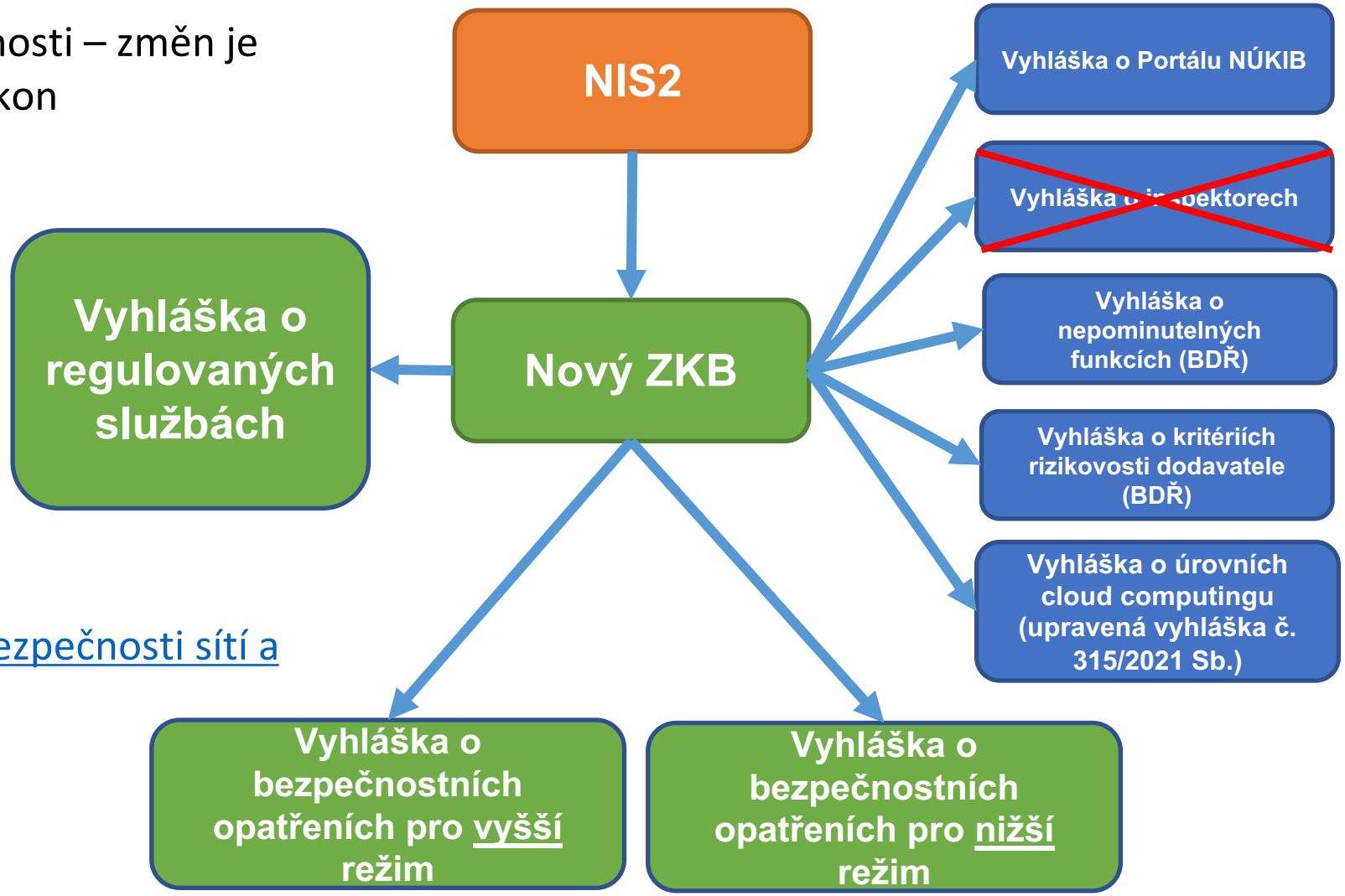
Nový zákon o kybernetické bezpečnosti (NZKB)

Nový zákon o kybernetické bezpečnosti – změn je tolik, že bylo třeba vytvořit nový zákon

zcela nová úprava – cca 60 paragrafů

Zveřejněný návrh má aktuálně navíc 8 vyhlášek

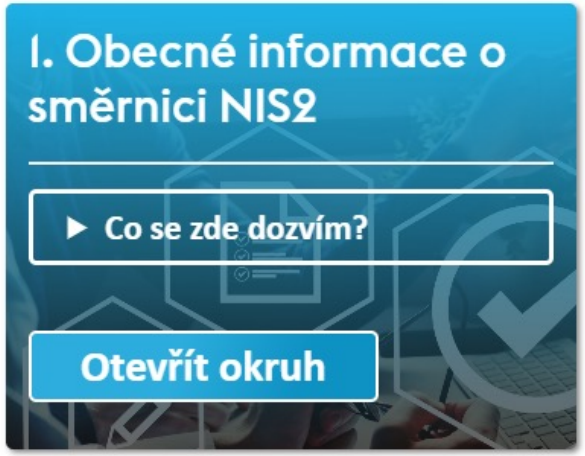
Celý návrh zveřejněn zde: Course: Nová směrnice EU o bezpečnosti sítí a informací (nukib.cz)

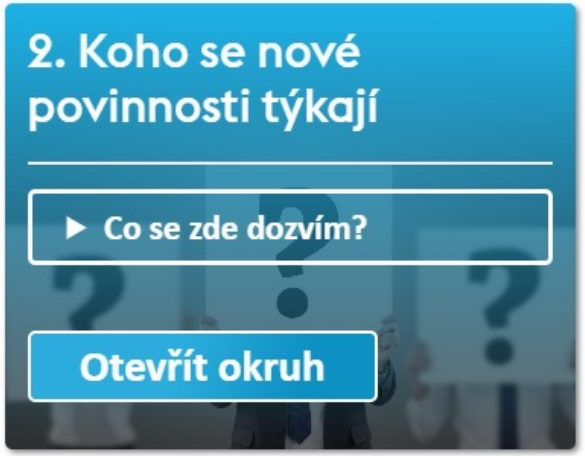


Web NÚKIB k směrnici NIS2

- Spuštěn web – dostupný zde: nis2.nukib.cz

- Návrhy předpisů byly zveřejněny zde
- Proběhly veřejné konzultace
- Zde budou zveřejněny:
  - revidované návrhy
  - Anonymizované podněty a jejich zpracování (v květnu/červnu – společně s počátkem MPŘ)





NZKB – povinné osoby

- Povinné osoby budou určovány **primárně na základě velikosti** (střední a velké podniky) a poskytované služby
- **Poskytovatel regulované služby**
  - Jediná povinná osoba
  - Poskytuje regulovanou službu = služba splňující kritéria stanovená vyhláškou
- **Režim poskytovatele regulované služby**
  - Stanovuje **míru povinností** – vyšší režim / nižší režim (vyšší cca 1000 povinných osob, nižší cca 5000)
  - Ke každému režimu bude vyhláška, která bude definovat bezpečnostní opatření
  - Režim regulace má také vliv na výši možných sankcí a hlášení incidentů
- Naplnění kritérií je povinen hlásit poskytovatel služby = každý si musí vyhodnotit kritéria sám
  - Nejpozději do 90 dní ode dne, kdy k naplnění došlo
- NÚKIB muže zaregistrovat i sám dozví-li se o naplnění kritérií

NZKB – povinné osoby ve veřejné správě

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
1.1. Výkon svěřených pravomocí	Orgán nebo osoba je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je a) ústředním orgánem státní správy, b) správním úřadem s celostátní působností, a to včetně ústředí a generálního ředitelství územně dekoncentrovaných (specializovaných) orgánů státní správy, c) Kanceláří prezidenta republiky, d) Kanceláří Senátu, e) Kanceláří Poslanecké sněmovny, f) Kanceláří Veřejného ochránce práv, g) Českou národní bankou, h) Nejvyšším kontrolním úřadem, i) Policejním prezidiem, j) útvarem policie s celostátní působností, k) orgánem soudní moci, l) státním zastupitelstvím, m) zdravotní pojišťovnou, n) krajem, o) hlavním městem Praha, nebo p) obcí s rozšířenou působností s nejméně 125 000 obyvateli, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je a) územně dekoncentrovaným (specializovaným) orgánem státní správy, b) profesní komorou, c) vysokou školou, d) Akademií věd České republiky, nebo e) obcí s rozšířenou působností s počtem obyvatel do 125 000.

NZKB - Poskytovatel regulované služby

10. Vodní hospodářství

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
10.1. Provozování vodovodu	Provozovatel vodovodu podle zákona o vodovodech a kanalizacích je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, nebo b) zásobuje pitnou vodou alespoň 50 000 obyvatel, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.
10.2. Provozování kanalizace	Provozovatel kanalizace podle zákona o vodovodech a kanalizacích je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, nebo b) poskytuje služby odvádění nebo čištění odpadních vod alespoň 50 000 obyvatelům, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

18. Zdravotnictví

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
18.1. Poskytování zdravotní péče	Poskytovatel zdravotní péče podle zákona o zdravotních službách je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, b) disponuje počtem lůžek akutní péče nejméně 270, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

11. Odpadové hospodářství

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
11.1. Provoz zařízení určeného pro nakládání s odpady	Provozovatel zařízení určeného pro nakládání s odpady podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.
11.2. Obchodování s odpadem	Obchodník s odpady podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.
11.3. Zprostředkování nakládání s odpadem	Zprostředkovatel nakládání s odpady podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.
11.4. Přeprava odpadu	Dopravce odpadu podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.

NZKB – shrnutí povinností

- Hlavní povinnosti
  - Hlásit kontaktní a další údaje
  - Stanovit rozsah řízení kybernetické bezpečnosti – definuje rozsah regulace v organizaci
  - Zavádět bezpečnosti opatření – podle režimu v kterém je služba určena (vyšší/nižší)
  - Hlásit kybernetické bezpečnostní incidenty – podle režimu v kterém je služba určena (vyšší/nižší)
  - Informovat zákazníky o incidentech a hrozbách
  - Provádět protiopatření
  - Plnit povinnosti z Mechanismu prověřování bezpečnosti dodavatelského řetězce u strategicky významných služeb
  - Zajistit dostupnost strategicky významných služeb

NZKB – povinnosti

- **Hlášení údajů**
  - Registrační údaje – info o organizaci
  - Kontaktní údaje – info o zástupci, měl by být zastupitelný
  - Doplňující údaje – IP rozsahy a další
  - Potřeba hlásit i změny (těch údajů, které nelze dohledat v rejstřících)
  - Náležitosti – vyhláška o Portálu NÚKIB

- **Stanovení rozsahu řízení bezpečnosti**
  - Identifikace primárních aktiv v rámci celé organizace
  - Určí, která primární aktiva souvisí s poskytováním regulované služby
  - Určí, které organizační částí a podpůrná aktiva, která souvisí s poskytováním regulované služby
  - Ty aktiva a organizační části, které takto určí, spadají do rozsahu regulace
  - Dokud/pokud to neudělá = rozsah celá organizace

NZKB – povinnosti

- **Bezpečnostní opatření**
  - Zavádí se v rámci stanoveného rozsahu
  - Začínají se plnit **nejpozději do 1 roku od registrace** služby
  - V rámci vyššího/nižšího režimu:

organizační opatření – **vyšší** režim

1. systém řízení bezpečnosti informací,
2. Povinnosti pro vrcholové vedení,
3. bezpečnostní role,
4. řízení bezpečnostní politiky a bezpečnostní dokumentace,
5. řízení aktiv,
6. řízení rizik,
7. řízení dodavatelů,
8. bezpečnost lidských zdrojů,
9. řízení změn,
10. akvizice, vývoj a údržba,
11. řízení přístupu,
12. zvládání kybernetických bezpečnostních událostí a incidentů,
13. řízení kontinuity činností a
14. audit kybernetické bezpečnosti

technická opatření – **vyšší** režim

1. fyzická bezpečnost,
2. bezpečnost komunikačních sítí,
3. správa a ověřování identit,
4. řízení přístupových oprávnění,
5. detekce kybernetických bezpečnostních událostí,
6. zaznamenávání událostí,
7. vyhodnocování kybernetických bezpečnostních událostí,
8. aplikační bezpečnost,
9. kryptografické algoritmy,
10. zajišťování dostupnosti regulované služby,
11. zabezpečení průmyslových, řídící a obdobná specifických aktiv

bezpečnostní opatření – **nižší** režim

1. povinnosti vrcholového vedení
2. bezpečnost lidských zdrojů
3. řízení kontinuity činností
4. řízení přístupu
5. řízení identit a jejich oprávnění
6. detekce a zaznamenávání kybernetických bezpečnostních událostí
7. řešení kybernetických bezpečnostních incidentů
8. bezpečnost komunikačních sítí
9. aplikační bezpečnost
10. kryptografické algoritmy

Hlavní rozdíl v rámci jednotlivých režimů u bezpečnostních opatření je ale v jejich náročnosti, obsahu a rozsahu

NZKB - povinnosti

- **Hlášení incidentů**
  - Přechodná lhůta jeden rok na povinné hlášení, hlášení možné i dobrovolné
  - Lze hlásit i zranitelnosti
  - Hlásit se má primárně přes Portál NÚKIB (až bude)
- **Náležitosti hlášení incidentů**
  - Prvotní hlášení do 24 hodin
  - Na žádost musí organizace předložit upřesnění
  - Do 30 dnů o zjištění závěrečná zpráva, pokud incident trvá, tak 30 dní od vyřešení

Režim vyšších povinností

- Hlásí **všechny** incidenty s původem v kyberprostoru
- Hlásí **NÚKIB**
- Na prvotní hlášení Úřad v odpovědi sdělí, zda má významný dopad na bezpečnost státu -> do 72 hodin upřesňující hlášení (indikátory, dopad)

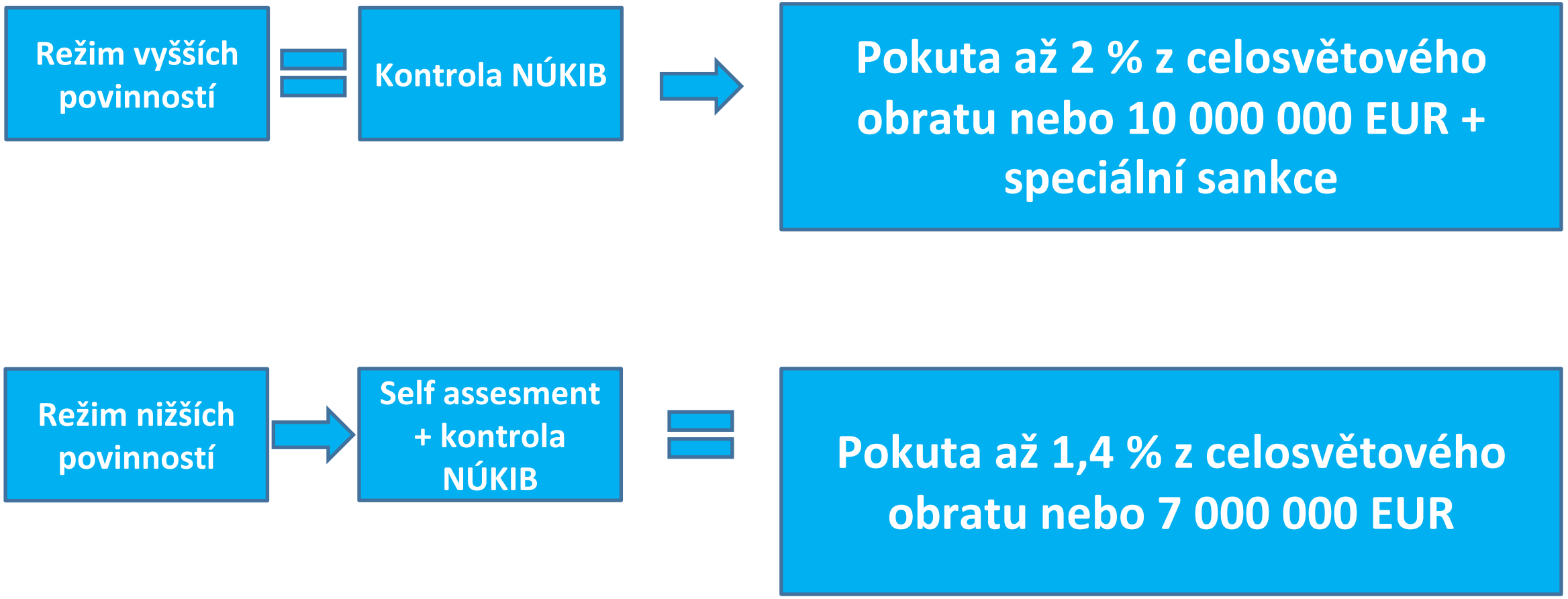
Režim nižších povinností

- Hlásí incidenty s původem v kyberprostoru a **s významným dopadem na službu**
- Hlásí **národnímu CERT**

NZKB – povinnosti

- **Opatření (nově Protiopatření)**
  - K podstatným změnám v logice opatření nedochází, mění se textace a některé detaily
  - Staronový institut – **Výstraha**
    - Jde o upozornění, které je veřejné, nezávazné
    - Vydává se z důvodu ochrany, pořádku, bezpečnosti, života a zdraví nebo ekonomiky
    - Muže být vydáno jako info o incidentu nebo o porušování ZKB
  - **Varování** – o hrozbě nebo zranitelnosti – veřejné i neveřejné, musí se promítnout do analýzy rizik u vyššího režimu
  - **Reaktivní protiopatření** – k řešení incidentu, zabezpečení před incidentem, ke zvýšení ochrany aktiv
    - Konkrétní úkony, technická opatření či postupy – pro adresáty povinné
    - Rozhodnuti – adresné (konkrétní adresát, konkrétní povinnost)
    - Opatření obecné povahy – neadresné (nekonkrétní adresát, konkrétní povinnost)

NZKB - Kontrola a sankce



NZKB – hlavní dopady na organizace

Nové povinné osoby

- Primárně **v režimu nižších povinností**:
  - ⇒ Povinnost zaregistrovat se a udat kontaktní údaje NÚKIB
  - ⇒ Základní úroveň bezpečnostních opatření
  - ⇒ Hlášení významných kybernetických incidentů
  - ⇒ Řízení se reaktivními protiopatřeními vydanými NÚKIB

Původní subjekty dle ZKB

- Primárně **v režimu vyšších povinností**:
  - ⇒ Bezpečnostní opatření jsou vymezeny službou – může dojít k rozšíření okruhu, na který budou bezpečnost zavádět, ale konkrétní opatření se pro vyšší režim mění pouze minimálně
  - ⇒ NIS2 stanovuje vyšší sankce za porušení – blíže GDPR
  - ⇒ Povinnost samoidentifikace spíše než kontaktování ze strany NÚKIB

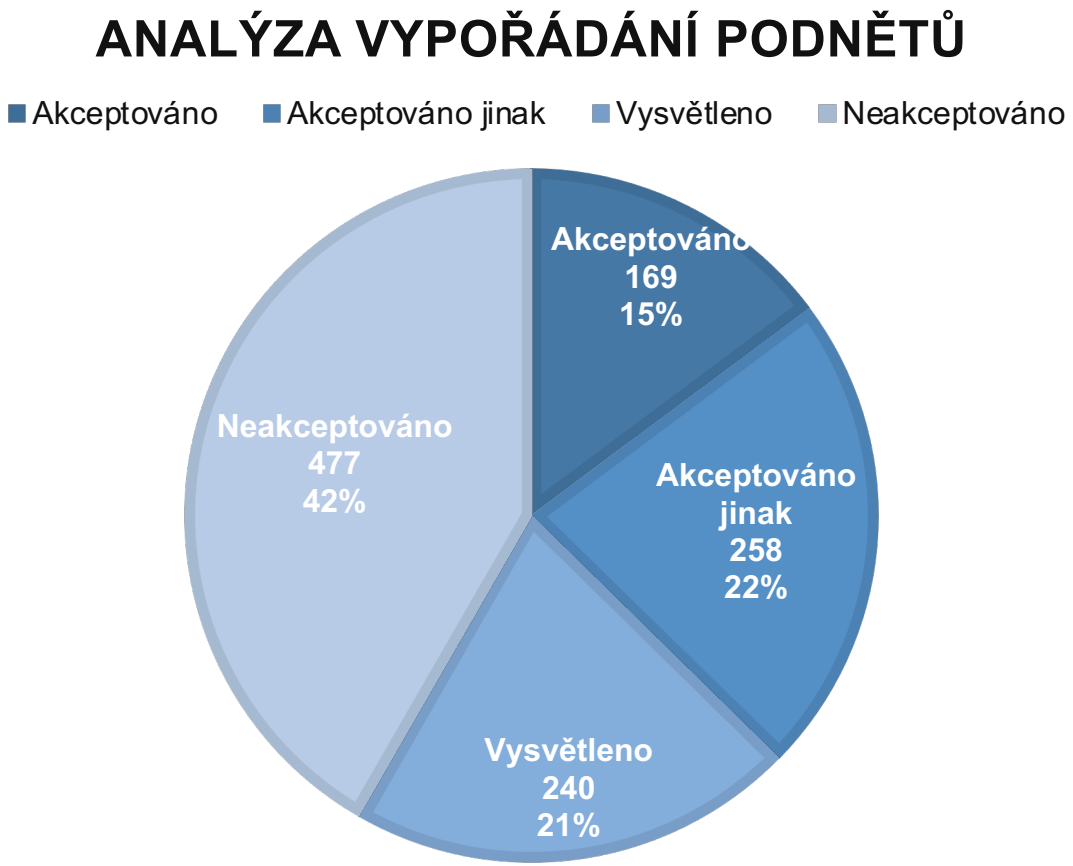
… kde začít?

- Analýza stávajícího stavu
  - **Zmapováním aktuálního stavu organizace**
  - Vypracování **business impact analýzy** (z pohledu narušení důvěrnosti, dostupnosti a integrity).
- Stanovení výběru konkrétních bezpečnostních opatření
  - **Nutno zohlednit specifika organizace a důležitost jednotlivých systémů a služeb**
  - Není smyslem zavádět nesmyslná a nákladná řešení tam, kde to pro vaši organizaci nemá význam.
- Stanovení jednotlivých priorit a bezpečnostních projektů
  - **Analýza rizik**
  - **školení relevantních osob**
  - Řešení největších problémů
  - Stanovení plánu od budoucna
  - Technická opatření – typicky **firewally**, **antiviry** a **zálohovací řešení.**

- V případě nejasností – zeptejte se NÚKIB

Komunikace návrhů – veřejné konzultace

- V rámci veřejných konzultací bylo od 26. ledna do 12. března zasláno 1144 podnětů od odborné veřejnosti i veřejné správy



- **Akceptováno** – podnět byl zapracován do návrhu zákona či doprovodných dokumentů (RIA, důvodová zpráva, návrhy vyhlášek);
- **Akceptováno jinak** – podnět byl v návrhu zákona či doprovodných dokumentech zohledněn jinak;
- **Vysvětleno** – podnět byl shledán spíše jako dotaz nebo konstatování, tudíž byl vysvětlen či okomentován;
- **Neakceptováno** – podnět nebylo možné zapracovat do návrhu zákona či doprovodných materiálů.

Veřejné konzultace – hlavní změny

- **Nastavení inspektorů** - > zrušení institutu
- Obsah **vyhlášky o bezpečnostních opatřeních pro režim nižších povinností** - > významné zeštíhlení, zjednodušení
- **Určovací a identifikační kritéria** ve vyhlášce - > přesun určovacích kritérií a odvětví do zákona
- **Vydefinování strategicky významné služby** pro účely BDŘ a zajištění dostupnosti služeb z ČR (cca 150 povinných osob)
  - Odvětví v nichž lze určit strategicky významnou službu byla rovněž přesunuta z vyhlášky do zákona
- **Lokalizace** informací a dat při zpracování v zahraničí - > zajištění dostupnosti strategicky významných služeb z ČR
- **BDŘ** – procesní posílení pozice adresátů (např. výjimky na žádost)

Další předpokládané kroky

- **Květen/červen 2023** – start Mezirezortního připomínkového řízení (MPŘ)
  - Oficiální zahájení legislativního procesu
  - Zveřejnění došlých podnětů veřejnosti vč. vypořádání
  - Zveřejnění návrhů předložených do MPŘ
- Legislativní rada vlády – **3/4Q 2023**
- Poslanecká sněmovna – **konec 2023**
- Vydání zákona **říjen 2024** (konec transpoziční lhůty)

NZKB – povinnosti – vyhlášky srovnání úrovní

NIŽŠÍ REŽIM

§ 7
Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

1. v rámci primárních aktiv stanoví jejich prioritu a pořadí a postupy jejich obnovy,
2. stanoví odpovědnosti a povinností při obnově podle písm. a),
3. vytváří pravidelné zálohy nastavení technických aktiv, informací a dat nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.

VYŠŠÍ REŽIM

§ 16
Řízení kontinuity činností

1. Povinná osoba v rámci řízení kontinuity činností
2. stanoví metodiku pro provedení analýzy dopadů,
3. pomocí analýzy dopadů vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a zohlední hodnocení rizik podle § 9, v rámci kterého posoudí možná rizika související s ohrožením kontinuity činností,
4. na základě výstupů analýzy dopadů a hodnocení rizik podle písmene b) stanoví cíle řízení kontinuity činností formou určení
    5. minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu regulované služby,
    6. doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb regulované služby a
    7. bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,
8. stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů podle písmene c) a stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,
9. vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a plány obnovy související s poskytováním regulované služby a
10. realizuje bezpečnostní opatření pro zvýšení odolnosti podle § 27.
11. Cíle řízení kontinuity podle odst. 1 písm. c) tohoto ustanovení jsou stanoveným časem a kvalitou regulované služby podle § X [Zajištění dostupnosti strategicky významné služby] zákona. Stanoveným časem je doba obnovení chodu podle odst. 1 písm. c) bod ii) tohoto ustanovení a stanovenou kvalitou regulované služby je minimální úroveň poskytovaných služeb podle odst. 1 písm. c) bod i) tohoto ustanovení.

NZKB – povinnosti – vyhláška nižší režim

- **§ 4 Zajišťování kybernetické bezpečnosti:**
  - **Princip přiměřenosti** (zavádí se přiměřená opatření se zohledněním bezpečnostních potřeb organizace)
  - Ústřední dokument: **Přehled bezpečnostních opatření** (zavedená/nezavedená/kdy budou zavedená + odůvodnění)
  - Určení **osoby zodpovědné za KB**
  - Pořízení a schválení **bezpečnostní politiky**, vedení bezpečnostní dokumentace
  - Stanovení **pravidel ochrany aktiv** a přípustné způsoby jejich používání
  - Zohlednění **požadavků na dodavatele** ve smluvním vztahu
  - Stanoví bezpečnostní požadavky v souvislosti s **akvizicí, vývojem a údržbou**
- **§ 5 Povinnosti vrcholového vedení:**
  - Vedení zná své povinnosti a **odpovědnosti**
  - Zajišťuje potřebné **zdroje**
  - **Seznamuje se s plněním přehledu bezpečnostních opatření**

NZKB – povinnosti – vyhláška nižší režim

- **§ 6 Bezpečnost lidských zdrojů**
  - **Politika bezpečného chování uživatelů**
  - Pravidla rozvoje bezpečnostního povědomí **(školení zaměstnanců)**
- **§ 7 Řízení kontinuity činností**
  - **Prioritizace primárních aktiv pro obnovu** a postup obnovy včetně odpovědných osob
  - **Zálohování**
- **§ 8 Řízení přístupů**
  - Zajištění **řízenosti přístupů a pravidel pro privilegované účty** – nezbytně nutné
  - Bezpečnost **mobilních zařízení**
- **§ 9 Řízení identit a jejich oprávnění**
  - Disponovat **nástrojem pro řízení identit a jejich oprávnění**
  - **Vícefaktorová autentizace** (+ délky hesel do doby zavedení vícefaktorové autentizace)
  - Pravidla pro tvorbu a nakládání s hesly

NZKB – povinnosti – vyhláška nižší režim

- **§ 10 Detekce a zaznamenávání kybernetických bezpečnostních událostí**
  - **Detekce událostí na perimetru +** vedení záznamů o nich
  - Nástroj pro nepřetržitou a automatickou **ochranu před škodlivým kódem** na relevantních aktivech
- **§ 11 Řešení kybernetických bezpečnostních incidentů**
  - **Zavede postupy pro oznamování podezření na incidenty/události**
  - **Metodika pro posuzování incidentů a událostí +** posouzení těch významných, které jsou hlášeny
  - **Zajistit řešení incidentů**
  - **Další postupy v souladu s požadavky na hlášení incidentů dle ZKB**
- **§ 12 Bezpečnost komunikačních**
  - **Segmentace** (zálohy vs. provozní prostředí)
  - **Omezení příchozí a odchozí komunikace na perimetru na nutnou**
  - Užívání aktuálně odolných a **bezpečných síťových protokolů**
  - Zajišťuje bezpečnost **vzdálených připojení a vzdálené správy** technických aktiv

NZKB – povinnosti – vyhláška nižší režim

- **§ 13 Aplikační bezpečnost**
  - **Bezodkladné aplikování bezpečnostních aktualizací**
  - Řídí bezpečnost **technických aktiv, která již nemají podporu** (vede evidenci, zavádí dodatečná bezpečnostní opatření)
  - **Skenování zranitelností** relevantních technických aktiv
- **§ 14 Kryptografické algoritmy**
  - Používá **šifrování pomocí aktuálně odolných kryptografických algoritmů, kde je to vhodné**
  - **Zohledňuje doporučení a metodiky** v oblasti kryptografických algoritmů **vydané Úřadem**
  - Zajišťuje **bezpečnou hlasovou, textovou a audiovizuální komunikaci** (vč. e-mailů a nouzové komunikace)
- **§ 15 Stanovení významnosti dopadu kybernetického bezpečnostního incidentu**
  - Obsahuje **pravidla pro stanovení významnosti dopadu incidentů** a tedy pro jeho hlášení

Služby - technické

- **NeWeb**
  - neweb@nukib.cz
- **HONEYPOTY**
  - oasp@nukib.cz
- **PROAKTIVNÍ SÍŤOVÝ MONITORING (THREAT HUNTING)**
  - oasp@nukib.cz
- **PROJEKT SYSTÉM DETEKCE**
  - oasp@nukib.cz
- **SLUŽBA SKENOVÁNÍ ZRANITELNOSTÍ NÚKIB**
  - oasp@nukib.cz

Služby - technické

- **POLYGON OPERAČNÍCH TECHNOLOGIÍ - OT POLYGON**
  - scada@nukib.cz
- **FORENZNÍ A MALWARE ANALÝZA (nerežimová)**
  - oa@nukib.cz
- **CERTIFIKOVANÁ FORENZNÍ LABORATOŘ (režimová)**
  - oa@nukib.cz

Služby - netechnické

- **KONZULTACE ZKB**
  - regulace@nukib.cz
- **CVIČENÍ**
  - vzdelavani@nukib.cz
  - Příklady realizovaných cvičení
    - ČEPS
    - SPCSS
    - HEALTH CZECH
    - ČSÚ
- **PODPŮRNÉ MATERIÁLY**
  - https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

Služby - netechnické

- **VZDĚLÁVÁNÍ – e-learning**
  - **Zdarma**

Děkujeme za pozornost!

regulace@nukib.cz