NIS2

Představení navrhované úpravy regulace kybernetické bezpečnosti v EU
Dopady do budoucí regulace kritické informační infrastruktury

NÚKIB

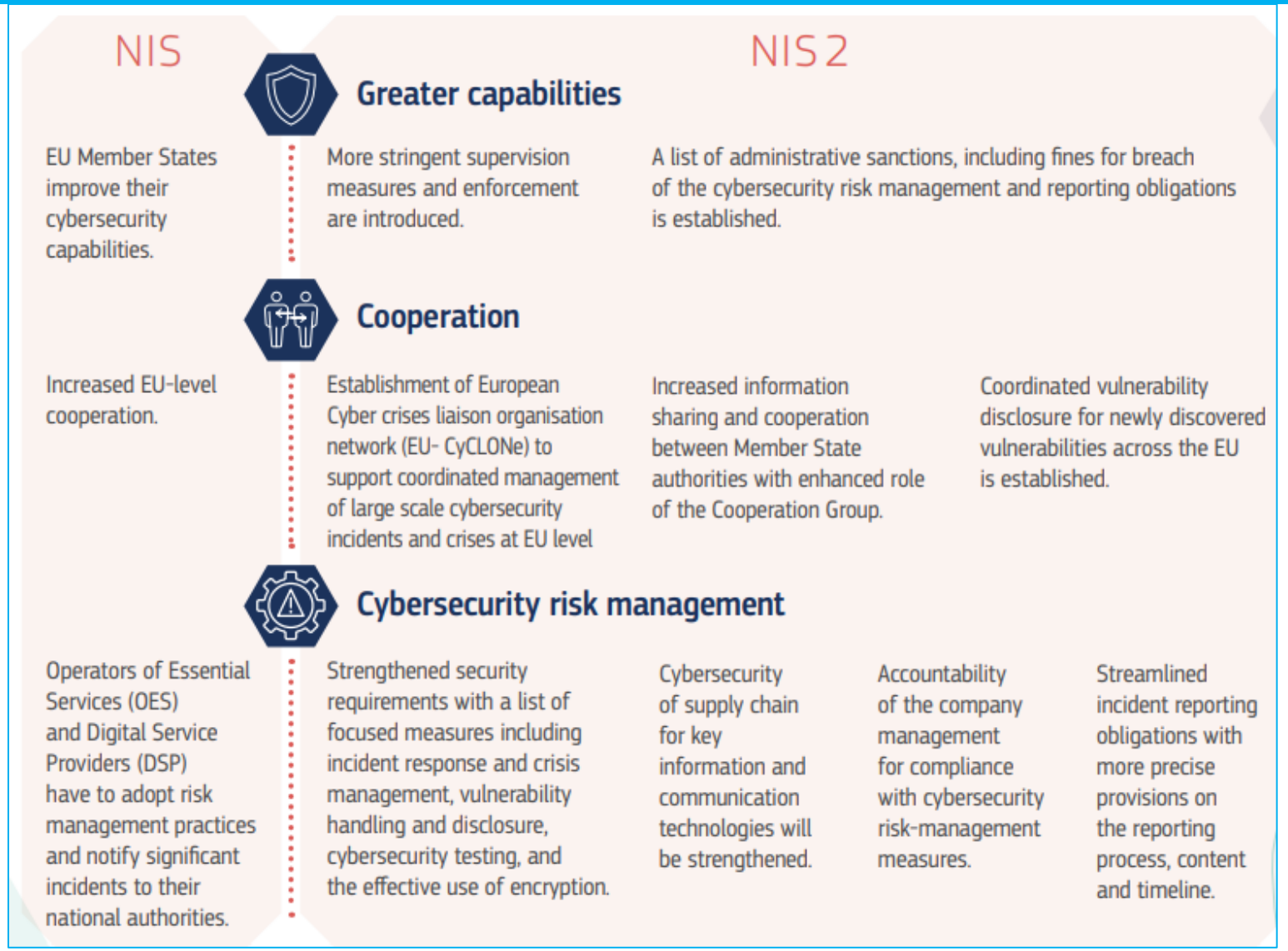
Národní úřad pro kybernetickou a informační bezpečnost

30. května 2022
TLP: WHITE

Vladěna Sasková
NÚKIB

Struktura NIS2

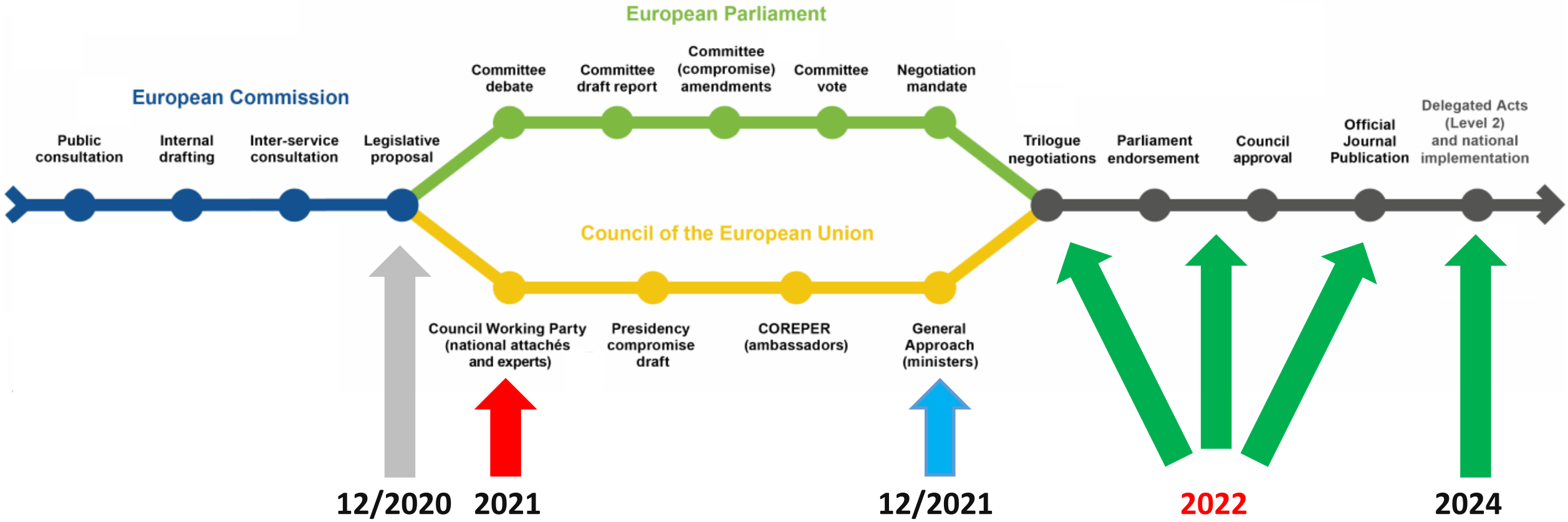
- Na konci roku 2020 zahájena z podnětu Evropské Komise revize směrnice NIS **– tzv. směrnice NIS2.**
- Návrh zachovává původní strukturu a mnoho institutů z původní směrnice NIS, většinu z nich však prohlubuje (směrem k ZKB)
- NIS2 → ZKB, VKB jednotné pro EU i non-EU regulované subjekty (obdobně jako dnes)



Zdroj schématu: Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe's digital future (europa.eu)

Vývoj vyjednávání

- Aktuální stav a časový odhad legislativního procesu:



- Shoda s EP nalezena, finalizován text, **publikace plánována v říjnu 2022** (transpoziční lhůta 21 měsíců)

Nové neregulační (policy) aspekty v NIS2

- Povinné přijetí konkrétních KB politik
- Zpráva o stavu KB v Unii
- EU-CyCLONe
- Vzájemná dobrovolná hodnocení (peer review)
- Coordinated Vulnerability Disclosure (CSIRT jako možný zprostředkovatel a koordinátor)
- Registr zranitelností vedený ENISA
- WHOIS databáze (domain name registration data, koordinuje stát)
- Koordinované posuzování rizik kritických dodavatelských řetězců v EU (obdobně jako 5G Toolbox)
- Povinné certifikace kybernetické bezpečnosti (stát x Komise)

Návrh NIS2 z pohledu regulace povinných osob

Rozdíly (aktuální návrh) **oproti NIS, část v ZKB/VKB již dnes:**

Minimální rozdíly oproti ZKB/VKB:

- Větší pravomoci dozorových orgánů (NÚKIB)
- Větší pravomoci CSIRT týmů
- Smysluplnější hlášení incidentů
- Podrobnější bezpečnostní opatření, risk-based approach

Novinky:

- Dvě skupiny povinných osob, způsob identifikace povinné osoby
- Rozsah regulovaných systémů
- Dobrovolné hlášení relevantních událostí a hrozeb, sdílení informací o zranitelnostech (registr ENISA)
- Povinné vzdělávání managementu, větší odpovědnost (+ dočasný zákaz výkonu fce)
- Vyšší pokuty za porušení povinností (inspirace GDPR; EE: 2 % z obratu / 10 mil. EUR, IE: 1,4 % z obratu / 7 mil. EUR)
- Spolupráce členských států na kontrolách a na výměně informací (i ve vztahu k „DSPs“)
- Sdílení informací mezi povinnými subjekty (stát má zajistit platformu)
- Užší spolupráce NÚKIB s dozorovými orgány z jiných oblastí (ÚOOÚ, ČTÚ, …)
- Do budoucna možnost povinných certifikací produktů
- Cloud computing = standardní povinná osoba (**!** výlučná jurisdikce)
- Rozšíření působnosti NIS2, zahrnutí veřejné správy

Návrh NIS2 – proces určování

- Původní směrnice NIS vycházela z předpokladu, že některé organizace nejsou na ICT závislé nebo ICT ovlivnitelné – návrh NIS2 toto opouští
- Unifikovaný způsob regulace = **konec odvětvových a dopadových kritérií systému**
- **Základní mechanismus:**
  - Subjekt vykonává činnost v regulovaném odvětví
  - Subjekt je střední nebo velký podnik ve smyslu Doporučení Komise ze dne 6. března 2003 = **50 a více zaměstnanců nebo roční obrat nebo rozvaha více než 10 mil. EUR**

- **Bez ohledu na velikost**:
  - poskytovatelé sítí elektronických nebo veřejně dostupných služeb elektronických komunikací
  - poskytovatelé služeb poskytujících důvěru
  - registry internetových domén nejvyšší úrovně (TLD)
  - orgány veřejné správy (ústřední orgány, volitelně regionální/lokální)
- Dodatečný mechanismus (určení státem):
  - výhradní dodavatelé služeb v členském státě nezbytných pro zajištění základních společenských nebo ekonomických činností
  - subjekty, u kterých by narušení jimi poskytovaných služeb mohlo mít vliv na veřejný pořádek, veřejnou bezpečnost nebo ochranu zdraví
  - subjekty, u kterých by narušení jimi poskytovaných služeb mohlo vyvolat systémová rizika, zejména pro ta odvětví, kde by takové narušení mohlo mít přeshraniční dopad
  - subjekty kritické vzhledem ke svému specifickému významu na regionální nebo vnitrostátní úrovni pro konkrétní odvětví nebo druh služby nebo pro jiná vzájemně závislá odvětví v členském státě
  - subjekty označené za kritické podle směrnice CER nebo za subjekty rovnocenné kritickým subjektům podle národní úpravy (banky, digi služby)
  - vzdělávací instituce

Návrh NIS2 – proces určování

! Opouští se princip určení informačního systému

Identifikace = **celá entita**, která vykonává regulovanou činnost v regulovaném odvětví

Regulace = **celá organizace**, nikoli systém, na němž je závislé fungování základní služby („ČEZ peče chleba“)

		economic activity
3. Manufacture, production and distribution of chemicals		Undertakings carrying out the manufacture, production and distribution of substances and articles referred to in points (4), (9) and (14) of Article 3 of Regulation (EC) No 1907/2006 ([30])
4. Food production, processing and distribution		Food businesses referred to in point (2) of Article 3 of Regulation (EC) No 178/2002 ([31])
5. Manufacturing	(a) Manufacture of medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices referred to in Article 2 point 1 of Regulation (EU) 2017/745([32]), and entities manufacturing in vitro diagnostic medical devices referred to in Article 2 point 2 of Regulation (EU) 2017/746 ([33]) with exception of entities manufacturing medical devices mentioned in Annex 1, point 5.
	(b) Manufacture of computer, electronic and optical products	Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
	(c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2
	(d) Manufacture of machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2
	(e) Manufacture of	Undertakings carrying out any of the economic activities referred

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	— Electricity undertakings referred to in point (57) of Article 2 of Directive (EU) 2019/944, which carry out the function of ‘supply’ referred to in point (12) of Article 2 of that Directive ([1])
		— Distribution system operators referred to in point (29) of Article 2 of Directive (EU) 2019/944
		— Transmission system operators referred to in point (35) of Article 2 of Directive (EU) 2019/944
		— Producers referred to in point (38) of Article 2 of Directive (EU) 2019/944
		—Nominated electricity market operators referred to in point 8 of Article 2 of Regulation (EU) 2019/943 ([2])
		— Electricity market participants referred to in point (25) of Article 2 of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services referred to in points (18), (20) and (59) of Article 2 of Directive (EU) 2019/944
	(b) District heating and cooling	— District heating or district cooling referred to in point (19) of Article 2 of the Directive (EU) 2018/2001 ([3]) on the promotion of the use of energy from renewable sources
	(c) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
		—Central oil stockholding entities referred to in point (f) of Article 2 of Council Directive 2009/119/EC ([4])
	(d) Gas	— Supply undertakings referred to in point (8) of Article 2 of Directive (EU) 2009/73/EC ([5])
		— Distribution system operators referred to in point (6) of Article 2 of

Návrh NIS2 – dvourychlostní regulace

Essential (základní) vs. **important** (důležité) entities

Rozdíly v regulaci:

- Rozsah bezpečnostních opatření (?)
- Kontrola (*ex ante* vs. *ex post*; risk-based approach)
- Dozorové pravomoci (EE+: rozsah vyžádaných informací, pozastavení platnosti certifikace, pozastavení výkonu manažerské funkce)

Návrh NIS2 – předpokládaná podoba národní transpozice

Identifikace povinných osob:

- Samoidentifikace (samonahlášení) – subjekty podle velikosti
- Rozhodnutí NÚKIB – subjekty podle dodatečných kritérií

Rozsah regulace (zavádění BO, hlášení incidentů):

- ISMS pro celou organizaci
- Cíle ISMS = služby, pro které byl subjekt určen

Kategorizace povinných osob:

- Národní bezpečnost/národní regulace (zde část KII, PZS, VIS)
- Essential entities (zde zbytek KII, PZS, část VIS)
- Important entites (zde zbytek VIS)

Rozsah služeb NÚKIB:

- Plný rozsah – národní regulace, essential ent.
- Omezený rozsah – important ent.

Bezpečnostní opatření, obsah ISMS:

- VKB – pro národní regulaci a essential ent.
- Minimální bezpečnostní standard – pro important ent.

Kontrola dodržování VKB:

- Plná kontrola NÚKIB ex-ante / ex-post
- Plná kontrola jinou autoritou
- Povinné audity (zasílání NÚKIB)

Důsledky přijetí NIS2 pro regulované subjekty

- **Určené subjekty zůstanou určeny** (kromě bank☹)
  - kritérium velikosti organizace
  - kritérium důležitosti pro sektor (bez ohledu na obrat nebo počet zaměstnanců)
  - národní úprava (KII, VIS)
- **Dosavadní PZS a KII** – zachována dosavadní úroveň regulace
  - otázka co s VIS
- **Rozsah zabezpečení informačních systémů se rozšíří na celou organizaci**, nejen na systém používaný pro výkon základní služby

  x risk-based approach

- **Větší zapojení Evropské komise** – prováděcí akty Komise – bezpečnostní opatření, hlášení incidentů

  ! ISO 27k → VKB
- **Vyšší pokuty** za neplnění bezpečnostních opatření (dnes max. 5 mil. Kč)
- **Větší důraz** na sdílení informací mezi určenými subjekty
- **Rozsah služeb NÚKIB** – VIP klub

Budoucnost regulovaných KII

- Odluka od krizového zákona (národní / essential ent.)
  - hledáme náhradní řešení
- Konec pravidelného přeurčování
  - subjekt bude regulován automaticky celý
  - subjekt bude určen rozhodnutím NÚKIB celý
  - cíl ISMS – služba, pro kterou spadl do regulace
  - → konec sporů o vymezení regulovaného systému (systém vs. služba)
  - → konec sporů o vymezení rozsahu ISMS (celá organizace)
  - → konec sporů o zařazení komunikační složky (IS KII vs. KS KII)
- Užší spolupráce NÚKIB s gestorem „fyzické“ KI (směrnice CER)

Dotazy?

Děkuji za pozornost!

regulace@nukib.cz
v.saskova@nukib.cz