cesnet

NIS 2 – Lightning talk...

Jan Kolouch

CESNET

7. února 2023
Seminář o bezpečnosti sítí a služeb 2023

Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022

o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 **(směrnice NIS 2)**

https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.CES&toc=OJ%3AL%3A2022%3A333%3ATOC

Směrnice **vstoupila v platnost 16. ledna 2023** a jednotlivé členské státy mají od tohoto dne **21 měsíců pro implementaci směrnice** do vlastního právního řádu (předpokládán je **říjen 2024**).

V této souvislosti je v ČR již několik měsíců **připravována rekodifikace zákona č. 181/2014 Sb.**, o kybernetické bezpečnosti.

cesnet

https://nis2.nukib.cz

CO SE ZMĚNÍ?

NIS2

Nový ZoKB

CER

Vyhlášky

- o regulovaných službách
- o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
- o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností
- o portálu NÚKIB
- o neopominutelných funkcích stanoveného rozsahu
- O kritériích rizikovosti dodavatele
- o inspektorech
- o bezpečnostních úrovních při využívání cloud computingu

~~Vyhlášky~~

- ~~č. 82/2018 Sb., o kybernetické bezpečnosti~~
- ~~č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby~~
- ~~č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích~~
- ~~č. 316/2014 Sb., o kybernetické bezpečnosti~~

Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES

https://eur-lex.europa.eu/eli/dir/2022/2557/oj?locale=cs

~~Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury~~

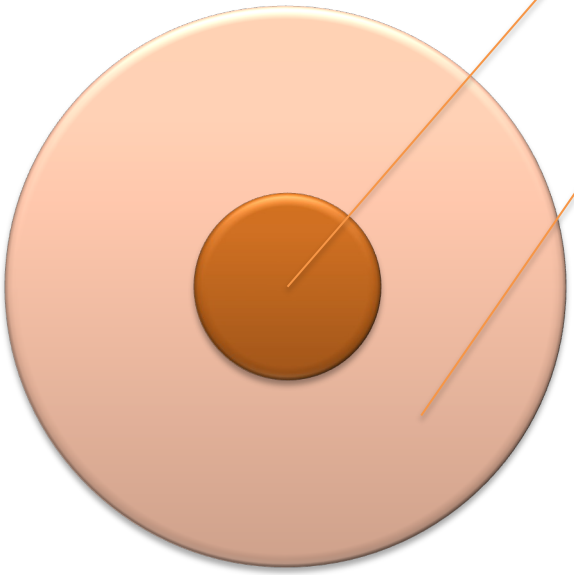
cesnet

Dopad?

Sectors covered by NIS 1	Sectors covered by NIS 2 proposal
"Operators of essential services" category	"Essential entities"
	All sectors from NIS 1
Healthcare providers	Additional health-related services - including pharma, some medical device manufacturers, researchers
Digital infrastructure - IXPs, DNS services, TLD registries)	Additional digital infrastructure services - cloud computing services, data centers, CDNs, network providers
Drinking water	Waste water
Transport	Space
Financial market infrastructure	Public Administration
Energy	
Banking	
"Digital service providers" category	"Important entities"
Online marketplaces	Online marketplaces
Online search services	Online search services
Cloud services	Social networking services
	Food production & distribution
	Postal services
	Waste management
	Chemical manufacturers
	Manufacturing - medical devices, electronic products and equipment, machinery, vehicles and transport equipment

https://www.rapid7.com/blog/post/2021/04/20/overview-of-the-eus-draft-nis-2-directive/

Regulovaný subjekt



Essential entities

Important entities

Režim vyšších povinností

Režim nižších povinností

KDO BUDE REGULOVÁN?

- **velký podnik**

Doporučení Komise 2003/361/ES z 6. května 2003
https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=LEGISSUM:n26026

- **střední podnik:**
  - méně než 250 zaměstnanců a
  - roční obrat do 50 milionů EUR nebo
  - rozvaha do 43 milionů EUR.

- **malý podnik:**
  - méně než **50 zaměstnanců** a
  - roční **obrat nebo**
  - **rozvaha do 10 milionů EUR**,
- **mikropodnik:**
  - méně než 10 zaměstnanců a
  - roční obrat (finanční částka získaná za určité období) nebo
  - rozvaha (výkaz aktiv a pasiv společnosti) do 2 milionů EUR,

cesnet

TLP: CLEAR

Národní úřad pro kybernetickou a informační bezpečnost
NÚKIB

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.

SUBJEKTY, KTERÝM PLYNOU POVINNOSTI Z NIS2, ALE NESPADAJÍ DO REŽIMU ESSENTIAL, ANI IMPORTANT

Subjekty shromažďující a udržující přesnou a úplnou registraci názvu domén.

verze 1.0, platná ke dni 16.08.2022

https://osveta.nukib.cz/pluginfile.php/58365/mod_page/content/323/Priloha-1_Graficke-znazorneni-bez-nazvu_logo_v1.0.pdf

16.6. Poskytování služby cloud computingu

Poskytovatel služby cloud computingu je
I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že
a) je velkým podnikem,
b) je poskytovatelem státního cloud computingu podle zákona o informačních systémech veřejné správy,
II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

Služba

Kritérium poskytovatele regulované služby

NÚKIB bude mít, dle § 4 odst. 2 VoRS, možnost určit jako regulovanou službu i další službu nad rámec kritérií stanovených přílohou VoRS, v případě, že její **narušení může způsobit závažný zásah do života postihující více než 125 000 osob**, a to prostřednictvím ohrožení života, zdraví, majetkové hodnoty, vnitřního pořádku, bezpečnosti nebo životního prostředí.

cca 15 – 20 x více subjektů

cesnet

OK...VÍCE SLUŽEB...A?

Každý poskytovatel regulované služby má jen jeden režim a ten stanovuje, jaké povinnosti mu ze zákona plynou.

„Vyšší bere.“

NA CELOU ORGANIZACI, nikoli na jeden či více systémů, služeb.

Výjimky…

cesnet

REGISTRACE

- **„self assesment“ naplněnosti kritérií pro identifikaci regulované služby**
- **Portál NÚKIB**
  - Vyplnění registračních údajů
  - Do 30 dní, nejpozději však do 90 dnů ode dne, kdy k naplnění kritérií pro identifikaci regulované služby došlo, nebo
  - NÚKIB provede registraci poskytovatele regulované služby v případě, kdy se dozví o naplnění kritérií pro identifikaci regulované služby podle prováděcího právního předpisu a poskytovatel regulované služby neprovede registraci
- **Zápis do evidence** poskytovatelů regulovaných služeb

POVINNOSTI POSKYTOVATELE RS

- **Hlášení údajů**
- **Stanovení rozsahu řízení kybernetické bezpečnosti**
  - Identifikace **primárních aktiv v rámci celého orgánu, nebo osoby**
    - **Informace**
    - **Data**
    - **Služby**
  - **Určení, která primární aktiva souvisí s poskytováním regulované služby**
  - S ohledem na primární aktiva identifikuje a určí **organizační části** orgánu nebo osoby **a podpůrná aktiva**
    - **Zaměstnanci**
    - **Dodavatelé**
    - **Objekty**
    - **Technická aktiva**
      - Technické prostředky
      - Programové prostředky
      - Vybavení

Komunikační prostředky, sítě elektronických komunikací, průmyslová, řídící nebo jiná obdobná specifická aktiva.

BEZPEČNOSTNÍ OPATŘENÍ

Organizační opatření	Režim vyšších povinností	Režim nižších povinností
Systém řízení bezpečnosti informací	✓	
Povinnosti vrcholového vedení	✓	✓
Bezpečnostní role	✓	✓
Řízení bezpečnostní politiky a bezpečnostní dokumentace	✓	✓
Řízení aktiv	✓	✓
Řízení rizik	✓	
Řízení dodavatelů	✓	✓
Bezpečnost lidských zdrojů	✓	✓
Řízení změn	✓	
Akvizice, vývoj a údržba	✓	
Řízení přístupu	✓	✓
Zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	✓	✓
Řízení kontinuity činností	✓	✓
Audit kybernetické bezpečnosti	✓	
Zajišťování minimální úrovně kybernetické bezpečnosti	✓	✓
Řízení změn, akvizice, vývoje a údržby		✓

BEZPEČNOSTNÍ OPATŘENÍ

Technická opatření	Režim vyšších povinností	Režim nižších povinností
Fyzická bezpečnost	✓	✓
Bezpečnost komunikačních sítí	✓	✓
Správa a ověřování identit	✓	✓
Řízení přístupových oprávnění	✓	✓
Detekce kybernetických bezpečnostních událostí	✓	✓
Zaznamenávání bezpečnostních a relevantních provozních událostí	✓	✓
Vyhodnocování kybernetických bezpečnostních událostí	✓	
Aplikační bezpečnost	✓	✓
Kryptografické algoritmy	✓	✓
Zajišťování dostupnosti regulované služby	✓	✓
Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv	✓	✓

HLÁŠENÍ KBI

NÚKIB

- Kybernetický bezpečnostní **incident mající původ v kybernetickém prostoru**
  - **prostředí tvořené aktivy umožňující vznik, výměnu a další zpracování informací a dat**

Národní CSIRT

- Kybernetický bezpečnostní **incident mající původ v kybernetickém prostoru a mající významný dopad** na poskytování regulované služby
  - **?**

cesnet

TO JE TEPRVE ZAČÁTEK...

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

544

21.1.2023

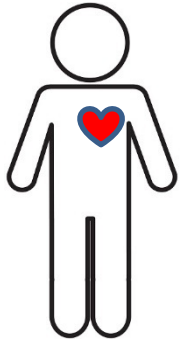
-

26.2.2023

57	Nový zákon o kybernetické bezpečnosti
70	Odůvodnění zákona o kybernetické bezpečnost
22	Odůvodnění - zákon o kybernetické bezpečnosti - Bezpečnost dodavatelského řetězce
41	Bezpečnost dodavatelského řetězce - RIA -Zákon o kybernetické bezpečnosti
24	Vyhláška o regulovaných službách
75	Odůvodnění vyhlášky o regulovaných službách
50	Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
30	Odůvodnění Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
35	Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností
20	Odůvodnění Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností
6	Vyhláška o portálu NÚKIB
4	Odůvodnění Vyhlášky o portálu NÚKIB
5	Vyhláška o nepominutelných funkcích stanoveného rozsahu
21	Odůvodnění Vyhlášky o nepominutelných funkcích stanoveného rozsahu
18	Vyhláška o kritériích rizikovosti dodavatele
18	Odůvodnění Vyhlášky o kritériích rizikovosti dodavatele
12	Vyhláška o autorizovaných inspektorech
8	Odůvodnění Vyhlášky o autorizovaných inspektorech
8	Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy
20	Odůvodnění Vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy

ŘEŠENÍ?

- **Capacity building**
- **Lidé na straně koncové organizace**



- **Nečekat, až…**
  - se to stane,
  - bude ZoKB,
  - bude platný/účinný…

- **Spolupráce**
- **Koupím si to!**
  - SOC za vás vyřeší NIS2 - NE
  - Jde si soulad koupit – NE
  - **I srdcaři mají své limity…a pozorujeme jejich přetíženost…**

cesnet

DĚKUJI ZA POZORNOST

doc. JUDr. Jan Kolouch, Ph.D.
jan.kolouch@cesnet.cz