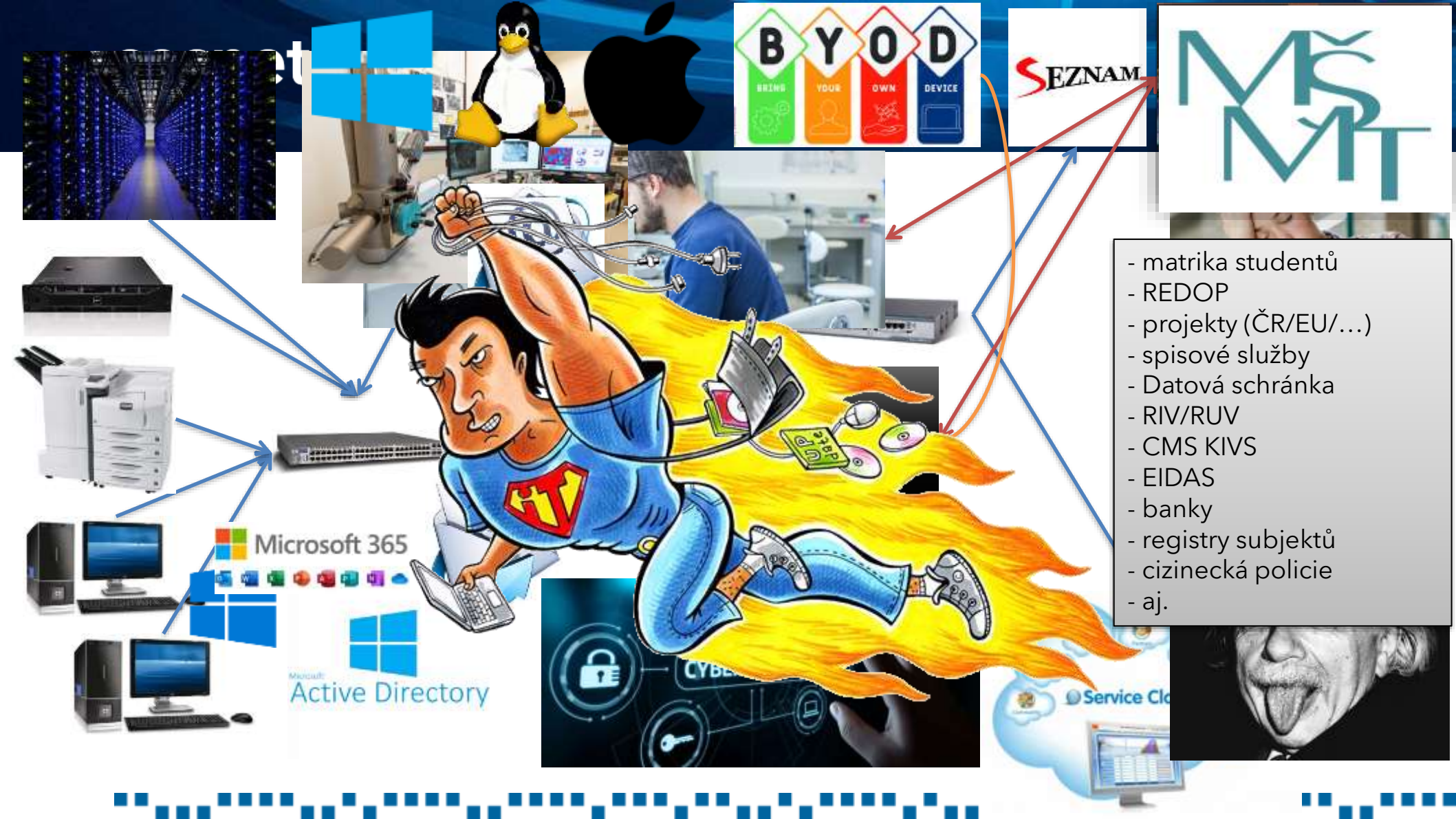
cesnet

NIS 2

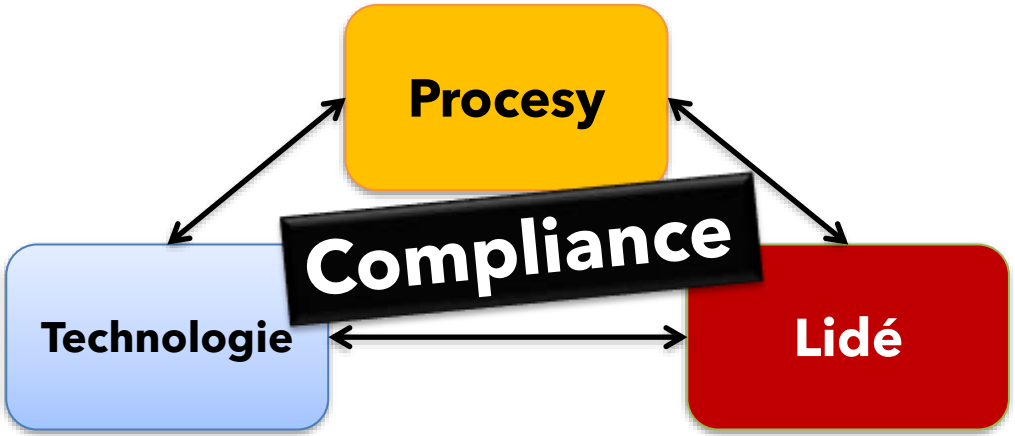
Jan Kolouch

CESNET

15. května 2024
ČZU – CESNET DAY

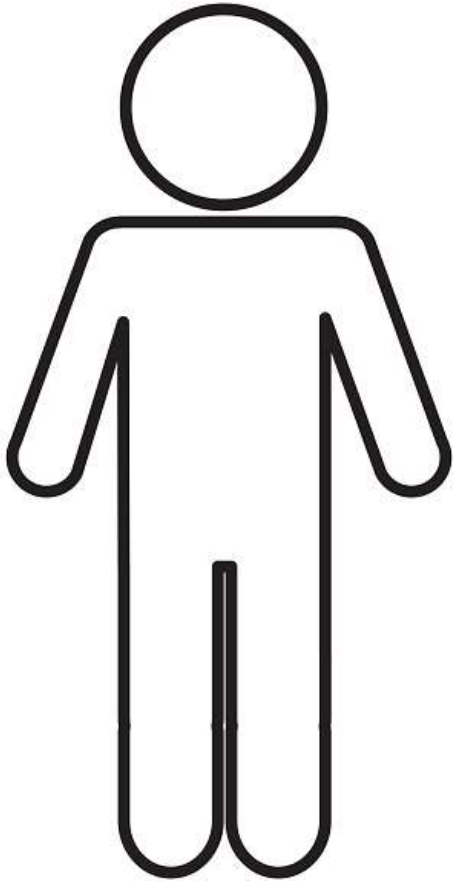

BYOD
BRING YOUR OWN DEVICE
SEZNAM
MŠMT
Microsoft 365
Active Directory
- matrika studentů
- REDOP
- projekty (ČR/EU/…)
- spisové služby
- Datová schránka
- RIV/RUV
- CMS KIVS
- EIDAS
- banky
- registry subjektů
- cizinecká policie
- aj.

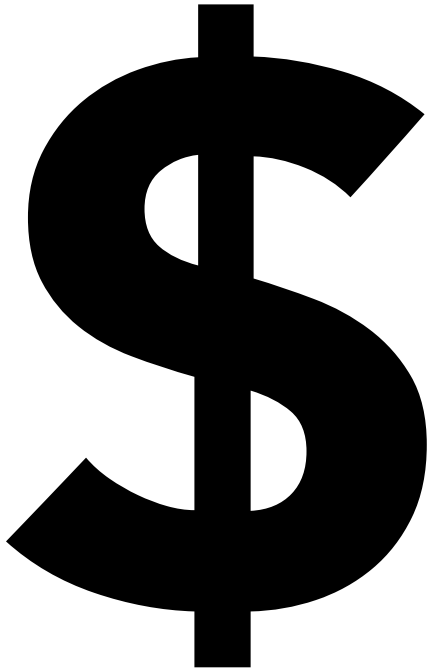
- Design
- Default
- Deployment
- PDCA cycle

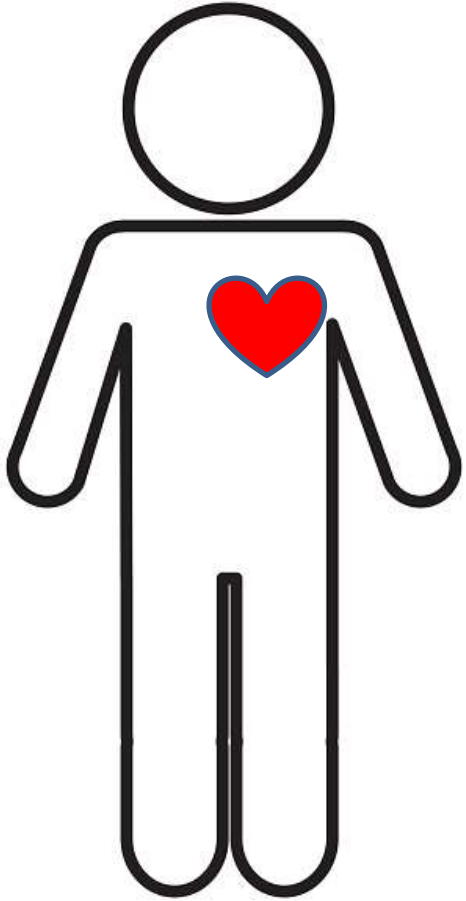


cesnet

Co chybí?







cesnet

CO S TÍM?

cesnet

ZÁKONODÁRCI

EU SCOPE

https://cclab.com/news-details/european-union-to-regulate-it-security-of-critical-infrastructures/106

cesnet

KYBERBEZPEČNOST

NIS1 + ZoKB

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 **o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii**

https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32016L1148

zákon č. 181/2014 Sb., o kybernetické bezpečnosti

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

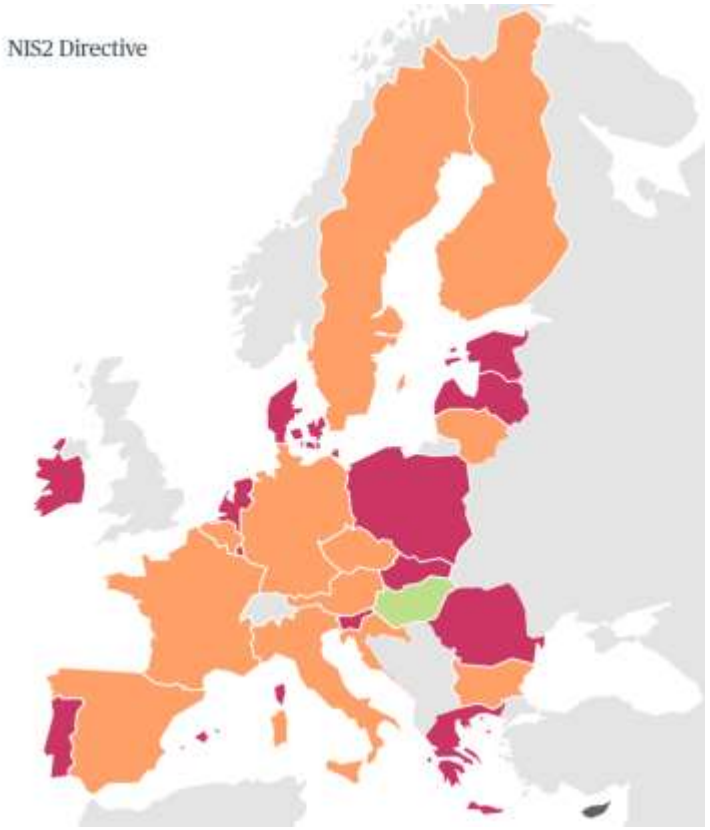
o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 **(směrnice NIS 2)**

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**).

JAK JSME NA TOM V EU?

	Adoption of the national implementing act
	Publication of the proposal
	Consultation phase
	No developments



https://www.twobirds.com/en/trending-topics/cybersecurity/nisd-tracker

https://nis2.nukib.cz

cesnet

CO SE ZMĚNÍ?

LEGISLATIVA

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~~

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

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.

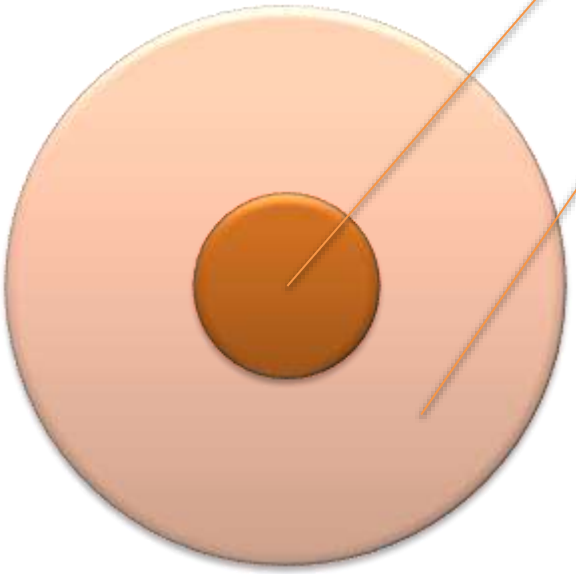
SUBJEKTY, KTERÝM PLYNOU POVINNOSTI Z NIS2, ALE NESPADAJÍ DO REŽIMU ESSENTIAL, ANI IMPORTANT

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

Regulovaný subjekt



Essential entities

Important entities

Režim vyšších povinností

Režim nižších povinností

Jeden režim.

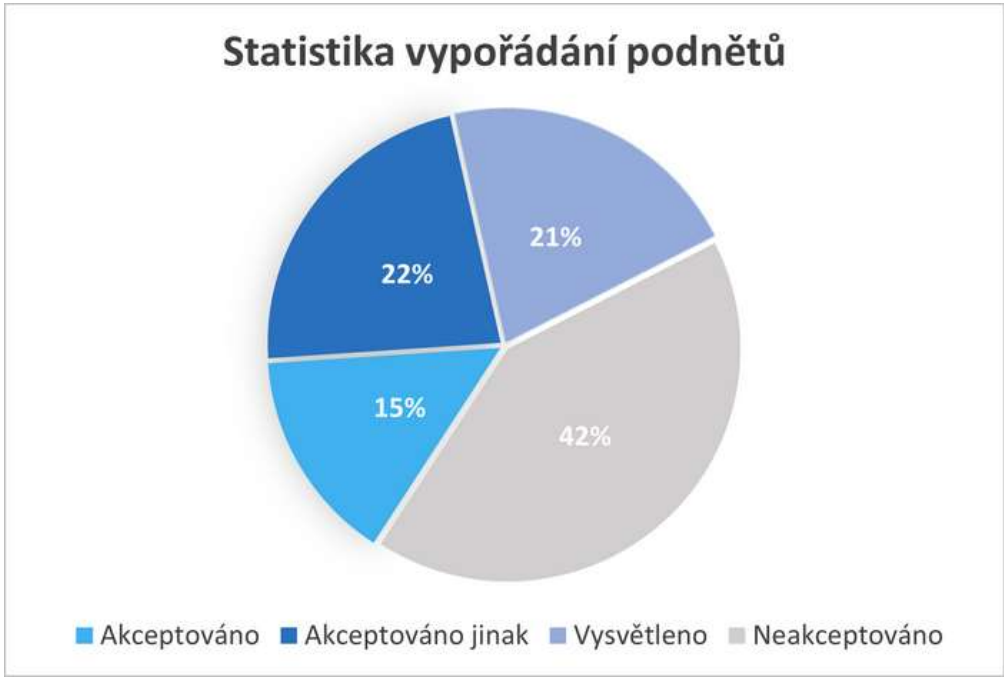
NA CELOU ORGANIZACI, nikoli na jeden či více systémů, služeb.

cesnet

JAK MOC JSME „BLÍZKO“

VEŘEJNÁ KONZULTACE

- **Od 26.1. do 12. 3. 2023**
- **1144 unikátních připomínek**
- **Pracovní tým:**
  - Jan Kolouch (CESNET, z.s.p.o)
  - Tomáš Plesník (Masarykova univerzita)
  - Jakub Harašta (Masarykova univerzita)
  - Michal Javorník (Masarykova univerzita)
  - Daniel Tovarňák (Masarykova univerzita)
  - František Hostek (Univerzita Karlova)
  - **98 připomínek + 5 variantní řešení**



MEZIRESORTNÍ PŘIPOMÍNKOVÉ ŘÍZENÍ

- **Od 19.6. do 26. 7. 2023**
- **864 připomínek** (**682 stran** vypořádací tabulky)
  - https://www.odok.cz/portal/veklep/material/ALBSCSSG44YX/
  - https://www.odok.cz/portal/veklep/material/pripominky/ALBSCSSFKU7S/
- **Pracovní tým rozšířen o:**
  - František Kasl (Masarykova univerzita)
  - Pavel Loutocký (Masarykova univerzita)
  - Václav Stupka (Masarykova univerzita)
  - Jakub Vostoupal (Masarykova univerzita)

MEZIRESORTNÍ PŘIPOMÍNKOVÉ ŘÍZENÍ

- **25 připomínek (posláno ČKR, samostatně pak CESNET a hSOC)**
- **Vypořádání:**
  - Akceptováno: **4**
  - Akceptováno jinak: **5**
  - Vysvětleno: **1**
  - Neakceptováno: **16**
- **26 reakcí**
- **1 připomínka** (č. 141) **MŠMT:**

K důvodové zprávě, zvláštní část k § 61 na str. 157: V závěrečné větě druhého odstavce na předmětné straně důvodové zprávy **požadujeme za slovo „děkan" vložit slovo „fakulty" a za slovo „veřejné" požadujeme vložit slova „či státní"**. V čele vysoké školy může totiž stát jen rektor, nikoliv děkan, který stojí v čele fakulty. Úprava děkanů a rektorů vysokých škol je totožná i pro vysoké školy státní, je nutné proto výslovně zmínit i je.	**Akceptováno** Důvodová zpráva byla upravena.

cesnet

LRV...

A DÁL?

- *Předložení návrhu zákona do Poslanecké sněmovny Parlamentu České republiky předpokládá NÚKIB ve čtvrtém kvartálu roku 2023.*

cesnet

BEZPEČNOSTNÍ OPATŘENÍ

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		✔

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	✔	
Řízení identit a jejich oprávnění		✔
Řešení kybernetických bezpečnostních incidentů		✔

cesnet

VÍCE AKTIV...

JASNÁ IDENTIFIKACE VŠECH AKTIV

§ 13 - Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby

(1) Poskytovatel regulované služby

a) ~~identifikuje všechna~~ **určí primární aktiva v rámci celé organizace,**

b) ~~určí~~ rozhodne, která primární aktiva ~~identifikovaná~~ určená podle písmene a) souvisejí s poskytováním regulované služby, a

c) u primárních aktiv ~~určených~~ souvisejících s poskytováním regulované služby podle písmene b) ~~identifikuje a~~ určí související organizační části organizace a podpůrná aktiva.

(2) Organizační části, primární aktiva a podpůrná aktiva ~~určená~~ související s poskytováním regulované služby podle odstavce 1 písm. b) a c) tvoří rozsah řízení kybernetické bezpečnosti (dále jen „stanovený rozsah").

- **Přestupek dle § 58 odst. 1 písm. d)** – při stanovení rozsahu řízení kybernetické bezpečnosti **neidentifikuje všechna primární aktiva** podle § 13 odst. 1 písm. a),

cesnet

PRIMÁRNÍ AKTIVUM

- *„primárním aktivem jsou **informace a služby***
  - *informacemi se rozumí také data, včetně provozních údajů, a službou se rozumí také procesy“*
- *Podpůrným aktivem jsou **zaměstnanci, dodavatelé, objekty a technická aktiva.***

PRIMÁRNÍ AKTIVUM – PO LRV

- *„primárním aktivem jsou **informace a služby**, **které mají pro poskytovatele regulované služby hodnotu,***

- *Podpůrným aktivem jsou **zaměstnanci, dodavatelé, ~~objekty a~~ technická aktiva,** **budovy a jiné ohraničené prostory, ve kterých se nachází aktiva regulované služby, a které mají pro poskytovatele regulované služby hodnotu a***

TECHNICKÉ AKTIVUM

- **„technickým aktivem technické a programové prostředky a vybavení, a to včetně průmyslových, řídicích nebo jiných obdobných specifických aktiv“**
- **Výčet prvků**, které zcela jistě spadají do kategorie technických aktiv, **má za cíl posílit právní jistotu adresátů** a **jednoznačně stanovit, že tato aktiva spadají do kategorie podpůrných aktiv** (což bylo v praxi ne vždy respektováno). …nejde o taxativní výčet.
- Byl odstraněn demonstrativní výčet, kdy současně **byla zachována část, kterou povinné osoby často opomíjí při identifikaci technických aktiv**, na které se vztahují bezpečnostní opatření vyhlášek, potažmo ZKB. Dle Úřadu, **nově navrhované znění tak nad rámec velice obecné definice konkretizuje, že OT je součástí technických aktiv, což posiluje právní jistotu**.

PŘESTUPKY?

- **Přestupek dle § 59 odst. 1 písm. d)** – při stanovení rozsahu řízení kybernetické bezpečnosti **neidentifikuje všechna primární aktiva** podle § 13 odst. 1 písm. a),
  - Je požadováno i současné identifikování **všech relevantních organizačních částí a podpůrných aktiv**, což vzhledem k rozsahu organizací může být problematické, někdy je nereálné určit všechna podpůrná aktiva.
- Správná identifikace všech aktiv je základním předpokladem pro zavádění všech navazujících bezpečnostních opatření.

cesnet

HLÁŠENÍ

HLÁŠENÍ

§ 16 odst. 1

„Poskytovatel regulované služby v režimu vyšších povinností ***je povinen*** *v rámci stanoveného rozsahu* ***hlásit*** *Úřadu* ***všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru****.“*

- **Univerzita: 100/1000/10 000 za….**
- **Možní duplicitní příjemci hlášení dle legislativy (stávající či připravované):**
  - 1) jako poskytovatel služby: *NIS2* -> národní autorita
  - 2) jako tvůrce digitálního produktu vč. SW: Cyber Resilience Act (*CRA*, též v přípravě) -> ENISA
  - 3) jako tvůrce SW pro finanční entity: Digital Operational Resilience Act (*DORA*) -> finanční instituce
  - 4) jako zpracovatel osobních údajů: *GDPR*? -> ÚOOU

POVINNOSTI VRCHOLOVÉHO VEDENÍ - § 5 VoRS

- je povinností vrcholového vedení **účastnit se prokazatelně školení v oblasti kybernetické bezpečnosti,**
- **zajistit stanovení politik a cílů,**
- **zajistit dostupnost zdrojů a**
- **plnit další povinnosti neodmyslitelně spjaté s řádnou schopností vykonávat v zajištění kybernetické bezpečnosti svou roli a**
- **plnit péči řádného hospodáře.**

a) se prokazatelně účastní školení podle § 11 odst. 3 písm. a) VoRS,

b) zajistí stanovení bezpečnostní politiky a cílů systému řízení bezpečnosti informací podle § 4, slučitelných se strategickým směřováním povinné osoby,

c) **zajistí integraci systému řízení bezpečnosti informací do procesů povinné osoby**,

d) **zajistí dostupnost zdrojů potřebných pro systém řízení bezpečnosti informací**,

e) informuje zaměstnance o významu systému řízení bezpečnosti informací a významu dosažení shody s jeho požadavky se všemi dotčenými stranami,

f) **zajistí podporu k dosažení cílů systému řízení bezpečnosti informací**,

g) vede zaměstnance k rozvíjení efektivity systému řízení bezpečnosti informací a podporuje je při tomto rozvíjení,

h) **se podílí na vypracování analýzy dopadů** podle § 16,

i) prosazuje neustálé zlepšovaní systému řízení bezpečnosti informací,

j) podporuje osoby zastávající bezpečnostní role při prosazovaní kybernetické bezpečnosti v oblastech jejich odpovědnosti,

k) zajistí stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role,

l) zajistí, aby byla zachována mlčenlivost administrátorů a osob zastávajících bezpečnostní role,

m) **pro osoby zastávající bezpečnostní role zajistí příslušné pravomoci a zdroje včetně rozpočtových prostředků k naplňovaní jejich rolí a plnění souvisejících úkolů a**

n) **zajistí testování plánů kontinuity činností, plánů obnovy** a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.

CO DÁL?

- **Řízení dodavatelů**
- **DRP**
- **Log management**
- **AAI** (primárně více faktorová autentizace)
- **vzdělávání**


cesnet
„AI“...

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, KTERÝM SE STANOVÍ HARMONIZOVANÁ PRAVIDLA PRO UMĚLOU INTELIGENCI (**AKT O UMĚLÉ INTELIGENCI**) A MĚNÍ URČITÉ LEGISLATIVNÍ AKTY UNIE

COM/2021/206 final

https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52021PC0206

cesnet

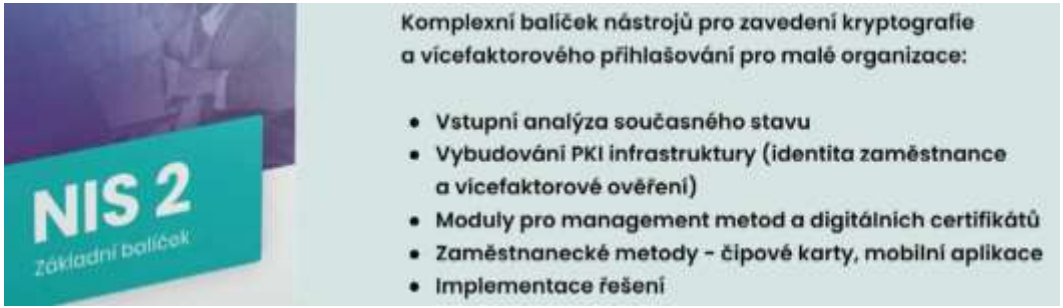
ŘEŠENÍ?

cesnet

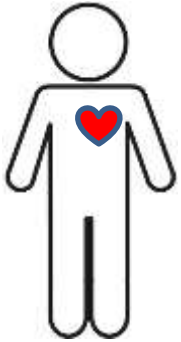
No. 1

https://practicalhealthpsychology.com/cz/2020/05/stop-being-an-ostrich-the-benefits-of-helping-people-to-monitor-their-progress/

Celé si to koupím!



- Capacity building
- Lidé na straně koncové organizace
- Nečekat, až…
  - se to stane znovu
  - bude ZoKB v 2.0
- Komunitní spolupráce



cesnet

DĚKUJI ZA POZORNOST

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