cesnet

NIS 2

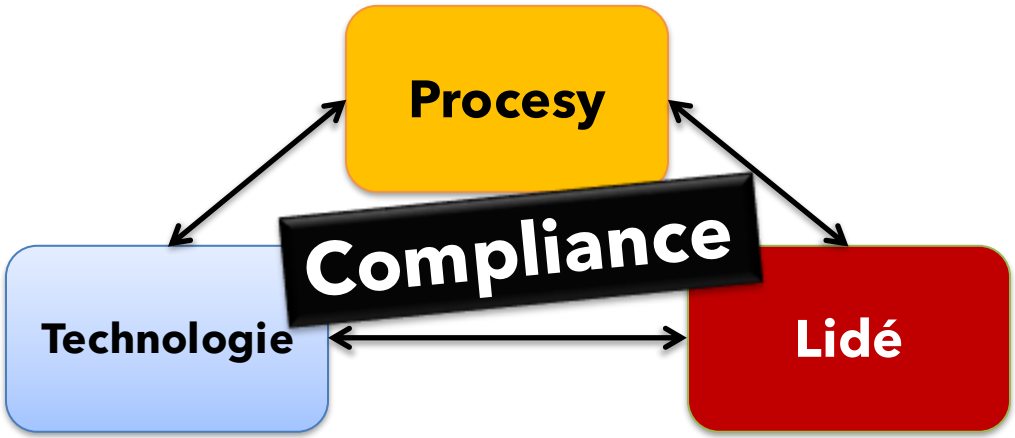
Jan Kolouch

CESNET

4. září 2024
VUT - CESNET DAY

https://blog.gutenberg-technology.com/en/why-universities-are-going-digital

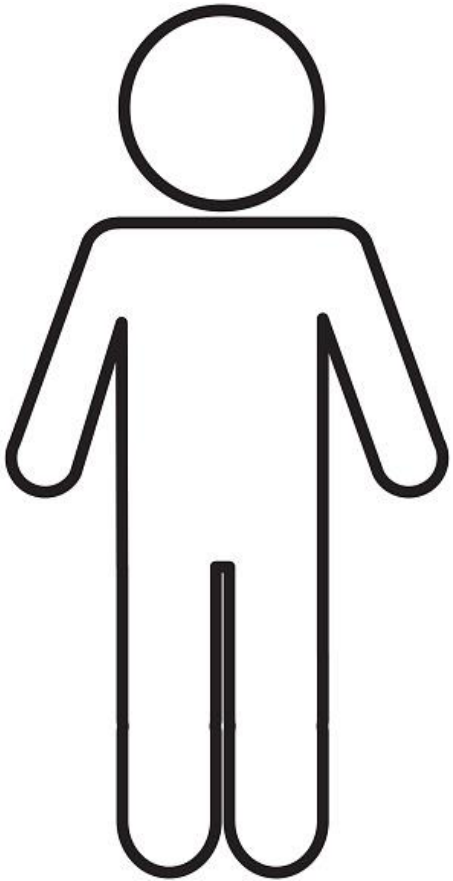
- Design
- Default
- Deployment

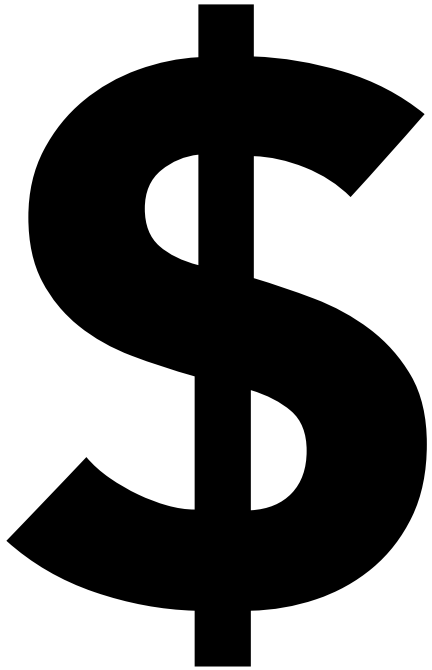


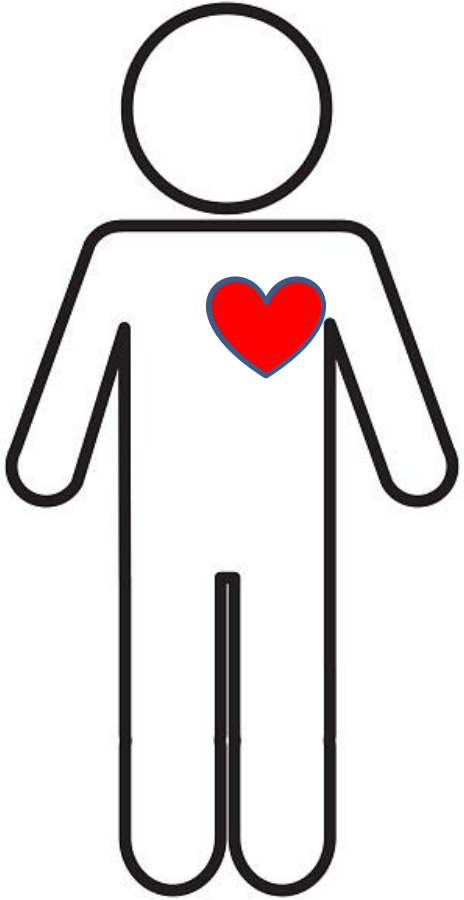
- PDCA cycle

cesnet

Co chybí?







cesnet

CO S TÍM?

cesnet

ZÁKONODÁRCI

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

cesnet

KYBERBEZPEČNOST

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

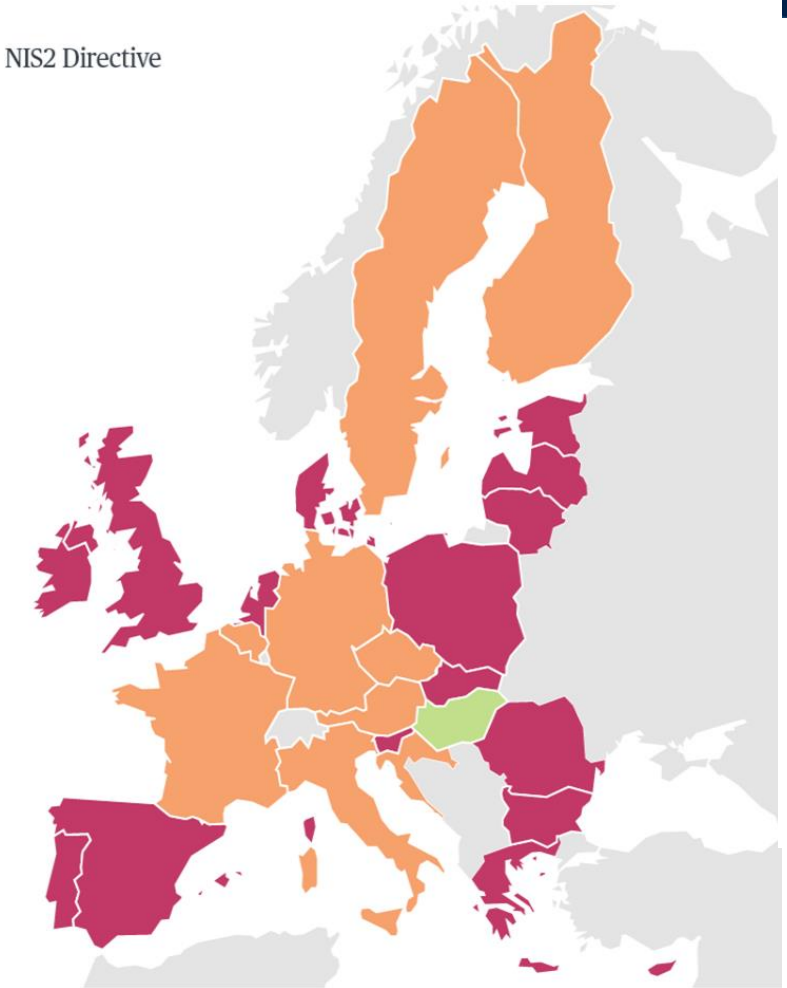
o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 **(směrnice NIS 2)**

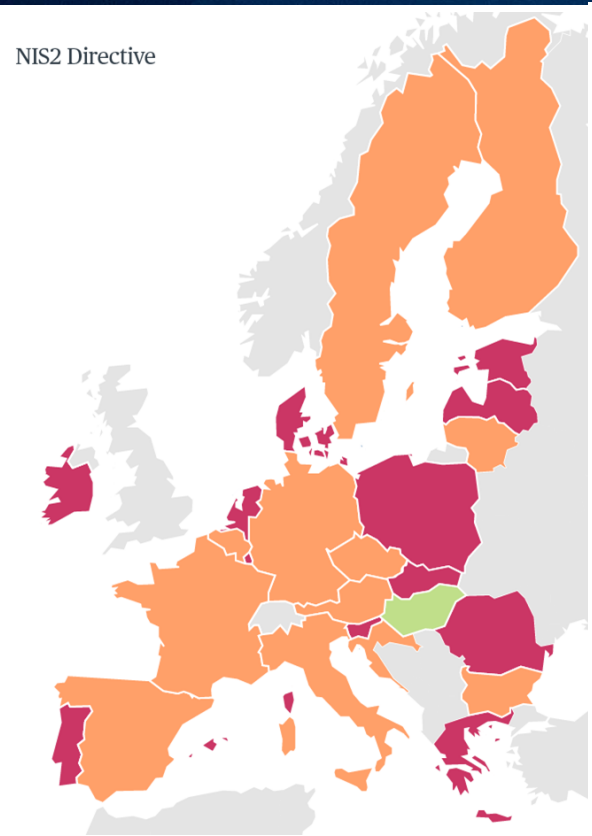
https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.CES&toc=OJ%3AL%3A2022%3A333%3ATOC

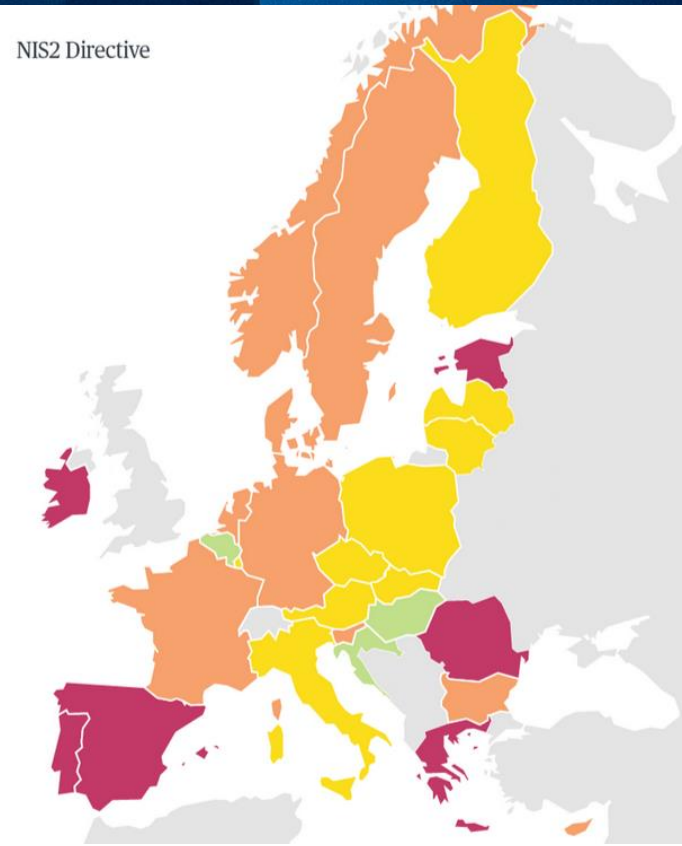
Směrnice **vstoupila v platnost 16. ledna 2023** a jednotlivé členské státy mají od tohoto dne **21 měsíců pro implementaci směrnice** do vlastního právního řádu (předpokládán je **říjen 2024**).

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://portal.nukib.gov.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**

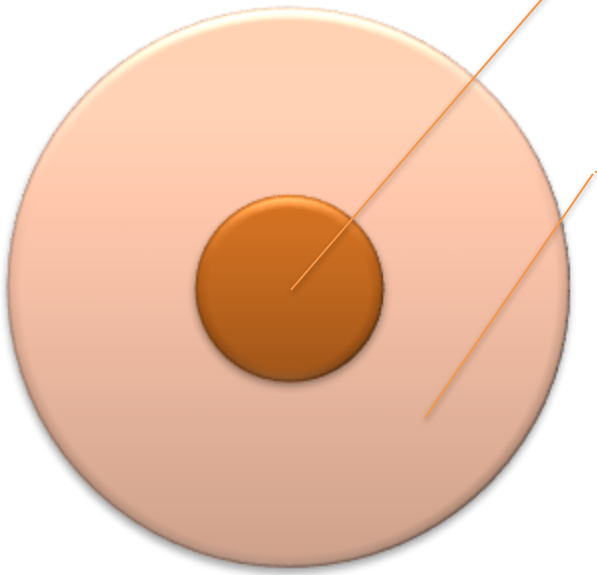
Doporučení Komise 2003/361/ES z 6. května 2003
https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=LEGISSUM:n26026

- **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,

Regulovaný subjekt



Essential entities

Important entities

Režim vyšších povinností

Režim nižších povinností

cesnet

Významné informační systémy
(181/2014 Sb.)

- Orientace na systém
- Správce VIS/KII
- Dopadová kritéria a povinné systémy
- Výjimka z regulace pro obce
- Jedna sada bezpečnostních opatření pro všechny organizace

Poskytovatel regulované služby
(nZKB)

- **Orientace na službu**
- **Poskytovatel regulované služby**
- Vyjmenované organizace
- Zahrnutí ORP – nižší režim
- Dvě sady bezpečnostních opatření pro různé organizace

AKTUÁLNÍ STAV NOVÉHO NÁVRHU ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI
Adam Kučínský, ředitel, odbor regulace, NÚKIB
E-government 20:10, Mikulov, 3.9.2024

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

Příloha k vyhlášce č. [bude doplněno] Sb.

1. Veřejná správa a výkon veřejné moci

Regulovaná služba	
Služba	**Podmínky významnosti poskytovatele regulované služby a jeho režim**
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) jiným správním úřadem s celostátní působností neuvedeným v písm. a), 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) Českou národní bankou, g) Policejním prezidiem, h) útvarem policie s celostátní působností, i) Generální inspekcí bezpečnostních sborů j) Generálním ředitelstvím hasičského záchranného sboru, k) krajským ředitelstvím hasičského záchranného sboru, l) Kanceláří Veřejného ochránce práv, m) Nejvyšším kontrolním úřadem, n) Úřadem pro zastupování státu ve věcech majetkových o) Správou úložišť radioaktivních odpadů, p) orgánem soudní moci, q) státním zastupitelstvím, r) zdravotní pojišťovnou, s) krajem, nebo t) hlavním městem Praha. II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je a) územně dekoncentrovaným (specializovaným) orgánem státní správy, b) profesní komorou[7], c) vysokou školou, d) Akademií věd České republiky, nebo e) obcí s rozšířenou působností,

19.1. Výzkum a vývoj	Výzkumná instituce, výzkumná organizace podle přímo použitelného předpisu Evropské unie[45], veřejná výzkumná instituce[46] nebo vysoká škola je poskytovatelem regulované služby v režimu vyšších povinností v případě, že provádí citlivou výzkumnou činnost. Výzkumná instituce, která neprovádí citlivou výzkumnou činnost, je poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním nebo velkým podnikem. Výzkumná organizace podle přímo použitelného předpisu Evropské unie[47], veřejná výzkumná instituce[48] nebo vysoká škola, která neprovádí citlivou výzkumnou činnost, je poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním nebo velkým podnikem a současně provádí aplikovaný výzkum[49] v některém z následujících oborů výzkumu a vývoje podle Struktury oborů FORD[50]: a) 1.2 Počítačové a informační vědy, b) 1.3 Fyzikální vědy, c) 1.4 Chemické vědy, d) 1.6 Biologické vědy, e) 2.2 Elektrické, elektronické a informační technologie, f) 2.3 Mechanické technologie, g) 2.4 Chemické technologie, h) 2.5 Materiálové inženýrství, i) 2.7 Environmentální technologie, j) 2.8 Environmentální biotechnologie, k) 2.9 Industriální biotechnologie, l) 2.10 Nanotechnologie, m) 2.11 Ostatní inženýrství a technologie, n) 3.1 Základní medicína, o) 3.2 Klinická medicína, p) 3.3 Zdravotní vědy,

	q) 3.4 Medicínská biotechnologie, r) 4.4 Zemědělská biotechnologie, s výjimkou výzkumu a vývoje léčivých přípravků naplňujícího kritéria pro identifikaci regulované služby podle bodu 18.4.
19.2. Provozování velké výzkumné infrastruktury	Hostitelská nebo partnerská instituce velké výzkumné infrastruktury[51] nebo konsorcium evropské výzkumné infrastruktury[52] je poskytovatelem regulované služby v režimu vyšších povinností.

18.4. Výzkum a vývoj léčivých přípravků	Zadavatel klinických hodnocení podle přímo použitelného předpisu Evropské unie[41] je I. poskytovatel regulované služby v režimu vyšších povinností v případě, že je velkým podnikem, II. poskytovatel regulované služby v režimu nižších povinností v případě, že je středním podnikem.

cesnet

Bude se vaše společnost řídit novým zákonem? Použijte naši kalkulačku

Výběr služby

V této rychlé kalkulačce můžete zjistit, zda vámi poskytovaná služba bude regulovaná a do jakého režimu (vyšší/nižší) bude pravděpodobně spadat. Pokud poskytujete více služeb a některé z nich budou regulované, pak bude celá organizace regulovaná podle nejvyššího režimu, na který některá ze služeb dosáhne.

Odvětví poskytované služby Vyberte odvětví

Poskytovaná služba Vyberte službu

Dále

https://portal.nukib.gov.cz/

Jeden režim.

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

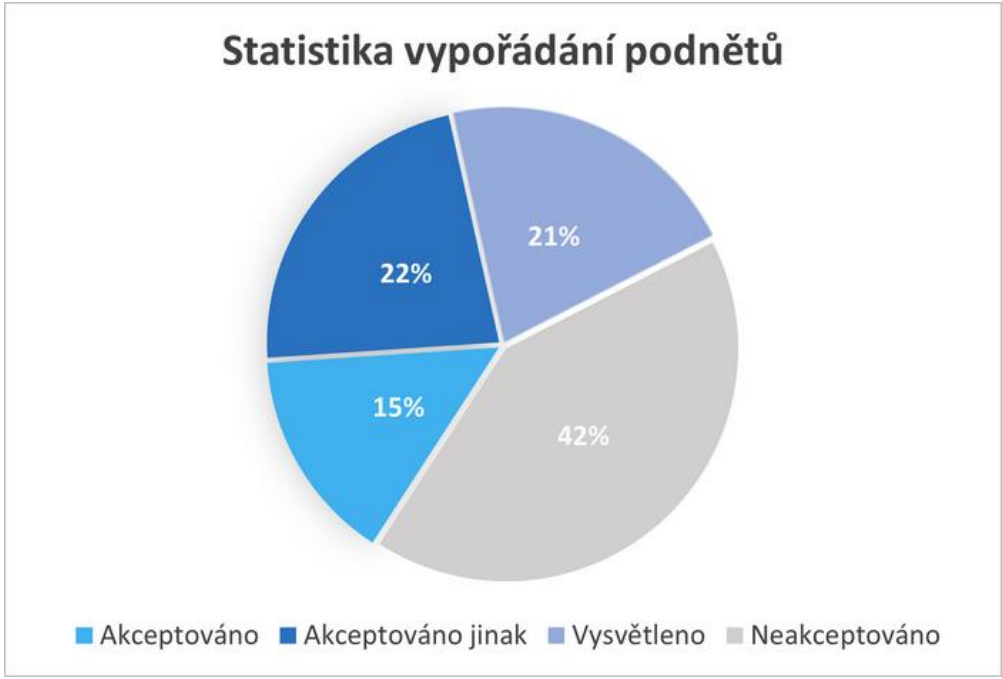
Permanentně?

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?

Sněmovní tisk 759
Vládní návrh zákona o kybernetické bezpečnosti - EU

Stav projednávání ke dni: 4. září 2024

Vysvětlení legislativního procesu

PŘEDKLADATEL

Vláda **předložila**sněmovně návrh zákona 25. 7. 2024.
Zástupce navrhovatele: předseda vlády.

POSLANECKÁ SNĚMOVNA

Návrh zákona rozeslán poslancům jako tisk 759/0 dne 25. 7. 2024.
Návrh zaevidován v systému **eKLEP** pod čj. OVA 68/24, PID ALBSCSSFKU7S.

Předsedkyně sněmovny projednání zákona **doporučila** 13. 8. 2024. Určila zpravodaje: Petr Letocha a navrhla přikázat k projednání výborům: Hospodářský výbor, Výbor pro bezpečnost (rozhodnutí č. 75)

Sněmovní tisk 759 (psp.cz)

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

Technická opatření

- **Zabezpečení** sítí, aplikací, systémů a softwaru
- **Zajištění** síťové **bezpečnosti** a IT infrastruktury **na fyzické i digitální úrovni**
- **Detekce a vyhodnocování** a aktivní řešení kybernetických hrozeb
- **Ochrana dat** prostřednictvím zálohování, autentizace, šifrování apod.
- Zvýšení odolnosti IS proti napadení, selhání, případně výpadku

Management, organizace a řídicí procesy

- **Analýza rizik** a bezpečnosti IS
- **Řízení kontinuity** (zálohování, obnova, krizové řízení,…)
- **Zabezpečení dodavatelských řetězců** a pořizování, vývoje a údržby sítí a IS
- Vytvoření politik a postupů určených k posouzení účinnosti opatření k řízení kybernetických rizik
- **Bezpečnost lidských zdrojů** (postupy kontroly přístupu a správa aktiv)

Dokumentace, vzdělávání a hlášení

- **Tvorba bezpečnostní dokumentace**
- **Vzdělávání** v oblasti kybernetické hygieny a kybernetické bezpečnosti
- Zajištění dokumentace z níž plyne plnění požadavků
- **Oznamovací povinnost** významných incidentů

cesnet

VÍCE AKTIV...

JASNÁ IDENTIFIKACE VŠECH AKTIV

§ 12 - Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby

(1) **Součástí rozsahu řízení kybernetické bezpečnosti (dále jen „stanovený rozsah“) jsou aktiva související s poskytováním regulované služby.**

(2) **Za účelem vymezení stanoveného rozsahu poskytovatel regulované služby**

a) **určí všechna svá primární aktiva,**

b) **posoudí, zda primární aktiva souvisí s poskytováním regulované služby**, a

c) u primárních aktiv podle písmene b) určí podpůrná aktiva.

(3) **Poskytovatel regulované služby eviduje aktiva, která jsou součástí stanoveného rozsahu, a primární aktiva, která byla ze stanoveného rozsahu vyjmuta, včetně důvodů jejich vyjmutí.**

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		✓

cesnet

PRIMÁRNÍ AKTIVUM

§ 2 Vymezení pojmů

c) **aktivem fyzický nebo digitální prostředek**, **osoba** nebo **činnost související se zpracováváním informací a dat v elektronické podobě**,

d) **primárním aktivem** aktivum v podobě **zpracovávané informace** nebo **poskytované služby**,

e) **podpůrným aktivem** aktivum zajišťující **fungování primárních aktiv**, zejména **zaměstnanec**, **dodavatel**, **technické aktivum**, **budova** a jiný ohraničený prostor, ve kterém se nachází aktivum regulované služby, a

f) **technickým aktivem technický** nebo **programový prostředek** anebo **vybavení**.

§ 2 Vymezení pojmů

a) **daty** záznamy jednání, skutečností nebo informací a soubory takových jednání, skutečností nebo informací, **včetně provozních údajů** a **metadat**, **zejména v podobě textu, čísel, grafů, obrazů, zvuku a videa**,

b) **informací** zpracovaná, interpretovaná nebo uspořádaná **data, která mají význam a kontext**,

PŘESTUPKY - § 59 ODST. 2?

2) Poskytovatel regulované služby v režimu nižších povinností se dopustí přestupku tím, že

a) neohlásí změnu regulované služby podle § 9 odst. 1,
b) neohlásí kontaktní nebo doplňující údaje nebo jejich změnu podle § 11,
c) **neurčí** za účelem vymezení stanoveného rozsahu **všechna primární aktiva** podle § 12 odst. 2 písm. a) **nebo podpůrná aktiva** podle § 12 odst. 2 písm. c), **nebo jejich určení pravidelně nepřezkoumá nebo neaktualizuje** podle § 12 odst. 5,
d) **neposoudí** za účelem vymezení stanoveného rozsahu, **zda primární aktiva** určená podle § 12 odst. 2 písm. a) **souvisí s poskytováním regulované služby**, nebo toto posouzení pravidelně nepřezkoumá nebo neaktualizuje podle § 12 odst. 5,
e) **neeviduje aktiva** podle § 12 odst. 3,
f) **nezavede nebo neprovede bezpečnostní opatření** podle § 13 odst. 2 nebo § 18 odst. 1,
g) **nevybírá svého dodavatele v souladu s požadavky** vyplývajícími z bezpečnostního opatření nebo nezahrnuje požadavky vyplývající z bezpečnostního opatření do smlouvy s dodavatelem v rozporu s § 13 odst. 5,
h) nepředloží prvotní hlášení o incidentu podle § 16 odst. 1 nebo nedoplní některý z údajů o incidentu podle § 16 odst. 3 nebo nenahlásí kybernetický bezpečnostní incident podle § 18 odst. 2,
i) neposkytne informace nebo součinnost při zvládání incidentu podle § 17 odst. 3,
j) nesplní povinnost nebo zákaz informovat uživatele regulované služby o kybernetickém bezpečnostním incidentu s významným dopadem stanovený rozhodnutím podle § 19 odst. 1,
k) neinformuje uživatele regulované služby o významné hrozbě nebo krocích, které může uživatel služby učinit v reakci na ni, podle § 19 odst. 2,
l) nesplní povinnost uloženou rozhodnutím o výstraze podle § 21 odst. 1,
m) nesplní reaktivní protiopatření uložené podle § 23 odst. 1 nebo § 23 odst. 4,
n) neoznámí provedení reaktivního protiopatření nebo jeho výsledek podle § 23 odst. 6, nebo
o) nesplní povinnost uloženou nápravným opatřením podle § 56 odst. 1.

- **Správná identifikace všech aktiv je základním předpokladem pro zavádění všech navazujících bezpečnostních opatření.**

cesnet

HLÁŠENÍ

§ 15 Hlášení kybernetických bezpečnostních incidentů

(1) Poskytovatel regulované služby v režimu vyšších povinností je povinen hlásit Úřadu postupem podle § 16 kybernetické bezpečnostní incidenty, které se projevily ve stanoveném rozsahu, mají původ v kybernetickém prostoru a nelze u nich ve lhůtě podle § 16 odst. 1 vyloučit úmyslné zavinění.

(2) Poskytovatel regulované služby v režimu nižších povinností je povinen hlásit národnímu týmu koordinace a zvládání kybernetických bezpečnostních incidentů, událostí a hrozeb (dále jen „**Národní CERT**“) postupem podle § 16 **kybernetické bezpečnostní incidenty, které se projevily ve stanoveném rozsahu, mají původ v kybernetickém prostoru**, **mají významný dopad na poskytování regulované služby** a nelze u nich ve lhůtě podle § 16 odst. 1 vyloučit úmyslné zavinění.

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

ŘEŠENÍ?

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

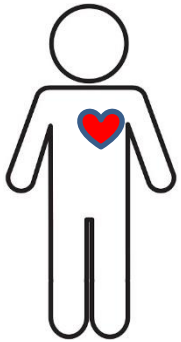
Obchod se strachem

Celé si to koupím!

Komplexní balíček nástrojů pro zavedení kryptografie a vícefaktorového přihlašování pro malé organizace:

- Vstupní analýza současného stavu
- Vybudování PKI infrastruktury (identita zaměstnance a vícefaktorové ověření)
- Moduly pro management metod a digitálních certifikátů
- Zaměstnanecké metody - čipové karty, mobilní aplikace
- Implementace řešení

- Capacity building
- Lidé na straně koncové organizace
- Nečekat, až…
  - se to stane znovu
  - bude ZoKB v 2.0
  - NIS 3?
- Komunitní spolupráce

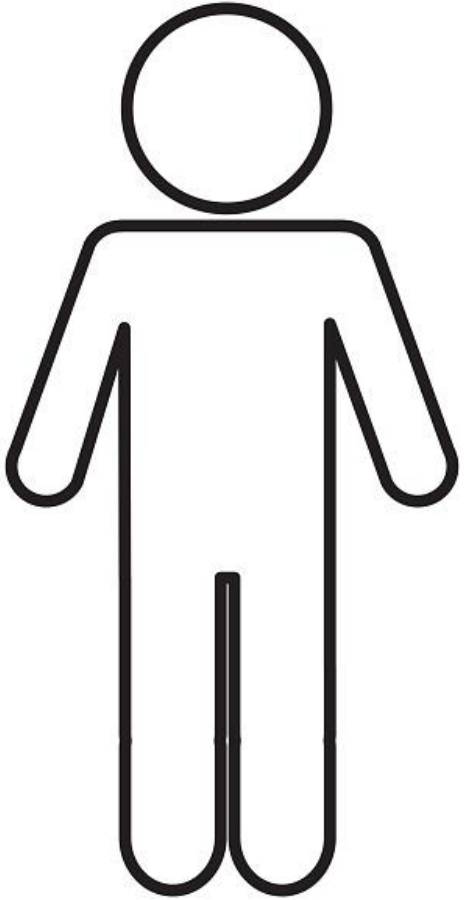


cesnet

KOOPERACE A KOMUNIKACE

KOOPERACE INTERNÍ

- IT/ICT
- „bezpečáci“
- vlastníci aktiv
- právníci
- management



Jasné rozhodnutí…
i nepopulární…

Přehled v organizaci

- Jaké vykonávám agendy a poskytuji služby?
- Co pro výkon těchto agend potřebuji?
- Z toho vyplývá rozsah, ve kterém KB řeším.

Aktuální stav KB

- Mám již zavedena některá opatření?
- Zdokumentuji aktuální stav zavedených a nezavedených opatření.

Určení priorit

- Jaké mám finanční a personální kapacity?
- Co je má prioritní služba?
- Provedu analýzy, stanovím plán se zohledněním kapacit a priorit.

Zavádění opatření

- Určím osobu odpovědnou za KB.
- Priorita je vzdělávání zaměstnanců včetně vedení.
- Vytvořím bezpečnostní politiku, kterou lze fakticky používat.
- Pokračuji dle plánu.

Zásada přiměřenosti:

- Náklady na zaváděné opatření by neměly převyšovat náklady na případnou realizaci kybernetického incidentu.
- Nechci všechno najednou, postupně se zlepšuji.

AKTUÁLNÍ STAV NOVÉHO NÁVRHU ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI

Adam Kučínský, ředitel, odbor regulace, NÚKIB

E-government 20:10, Mikulov, 3.9.2024


cesnet
ČAS?

cesnet

MŮJ OSOBNÍ NÁZOR: 06/2025

cesnet

„AI“…

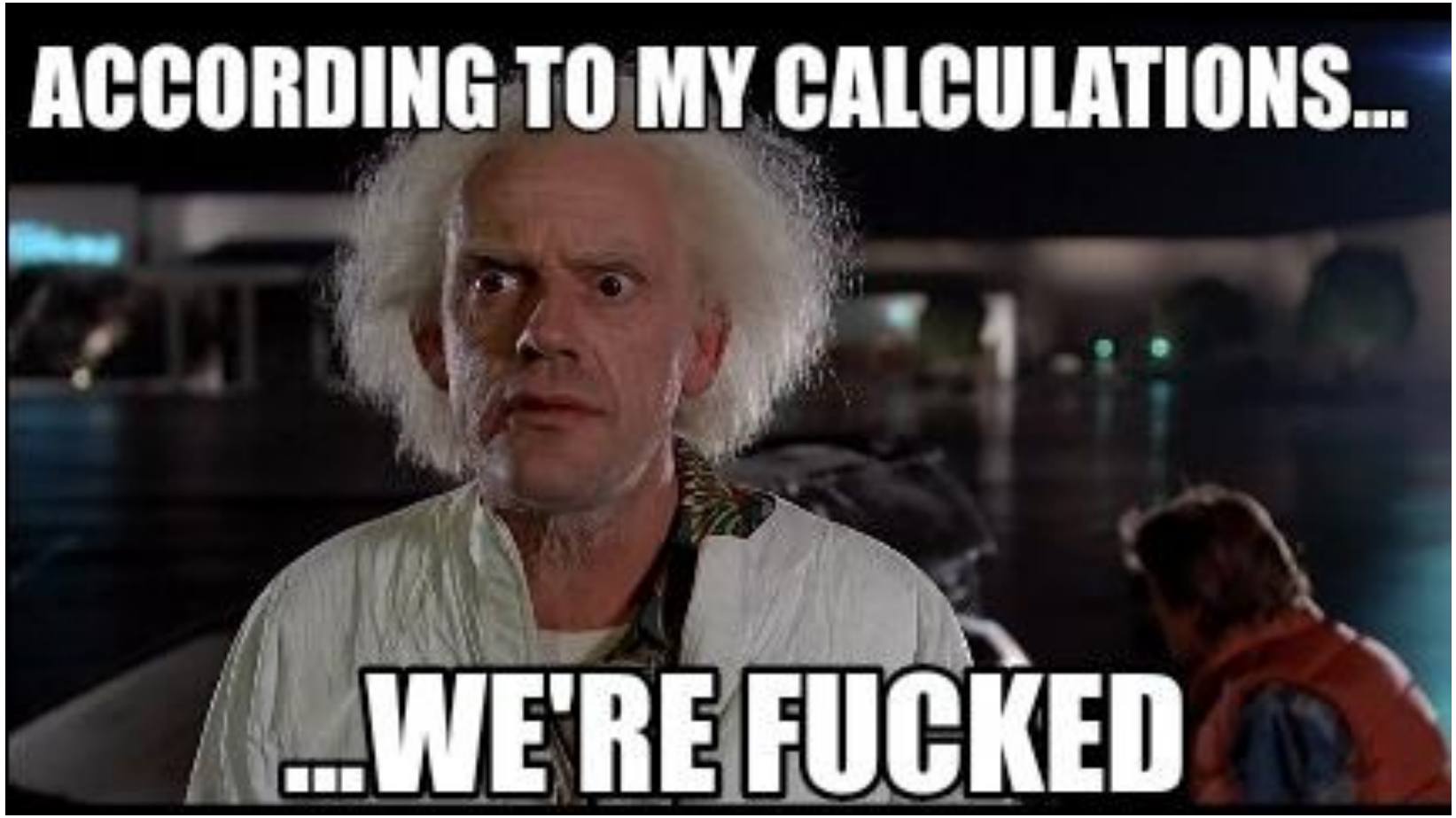
Nařízení

Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) **2020/1828** (**akt o umělé inteligenci**)

https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX%3A32024R1689

cesnet

1. **The directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)**
2. **The Digital Operation Resilience Act (DORA)**
3. **The Critical Entities Resilience Directive (CER)**
4. **The Cybersecurity Act (CSA)**
5. **The European Cyber Resilience Act (CRA)**
6. EU Cyber Solidarity Act
7. **The General Data Protection Regulation (GDPR)**
8. The European ePrivacy Regulation
9. The European Data Governance Act (DGA)
10. The Digital Services Act (DSA)
11. The Digital Markets Act (DMA)
12. The European Chips Act
13. The European Data Act
14. The Artificial Intelligence Act
15. The Strategic Compass for Security and Defence
16. The European Cyber Defence Policy Framework
17. The EU Cyber Diplomacy Toolbox
18. 5G Toolbox
19. Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union
20. The European Health Data Space (EHDS)
21. … and more…


ACCORDING TO MY CALCULATIONS...
...WE'RE FUCKED

cesnet

"It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it".

Stephane Nappo

cesnet

DĚKUJI ZA POZORNOST

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