cesnet

NIS 2 a její transpozice v ČR

Jan Kolouch

CESNET

17. května 2023
CSNOG 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~~

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

544

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

CO SE ZMĚNÍ?

NIS2

Nový ZoKB

CER

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

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~~

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

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

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.

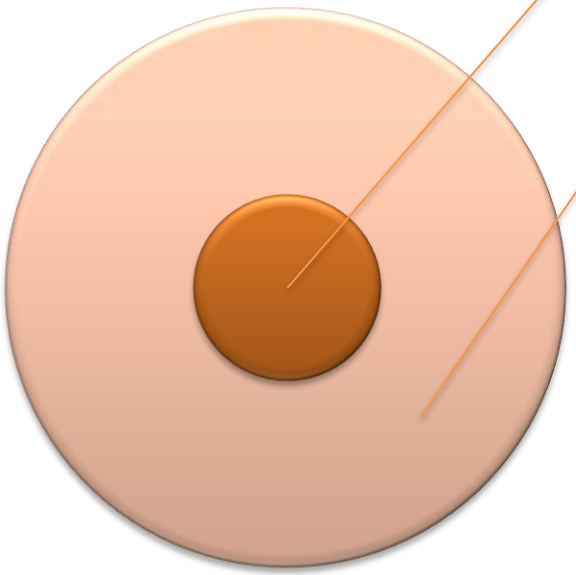
SUBJEKTY, KTERÝM PLYNOU POVINNOSTI Z NIS2, ALE NESPADAJÍ DO REŽIMU ESSENTIAL, ANI IMPORTANT

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

Regulovaný subjekt



Essential entities

Important entities

Režim vyšších povinností

Režim nižších povinností

cesnet

VÍCE SLUŽEB...

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

Jeden režim.
„Vyšší bere.“

Výjimky…

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	✔	✔

cesnet

Připomínkové řízení široké veřejnosti

cesnet

PODÁNÍ PŘIPOMÍNEK

Od 26.1. do 12. 3. 2023

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

cesnet

VYPOŘÁDÁNÍ PŘIPOMÍNEK

- **ze strany NÚKIB zasláno 20. 4. 2023**
- **Z 98 připomínek bylo:**

  - 17 plně akceptováno
  - 17 akceptováno jinak
  - 27 vysvětleno
  - 37 neakceptováno

cesnet

Vymezení pojmů

PRIMÁRNÍ AKTIVUM

- *„primárním aktivem jsou **informace a služby**. Informacemi se rozumí také data, **včetně provozních údajů**.“*
- Doporučujeme vypuštění slov: **„včetně provozních údajů“**
  - Vlastní pojem může být vykládán značně různorodě. Může se jednat o data spadající např. pod § 97 odst. 4 zák. č. 127/2005 Sb., o elektronických komunikacích, ale také se může jednat např. o údaje v podobě „data sheetu“, na kterém budou zaznamenány údaje o provozu. **Provozní údaje jsou stále data.**
- Explicitní uvedení provozních údajů je v zákoně obsaženo z důvodu, **aby se na tato data nezapomínalo při identifikaci a hodnocení aktiv**. Míříme hlavně na metadata, struktury databází apod., tedy údaje, které jsou v praxi mnohdy opomíjeny. **Provozní údaje jsou v aktuálním ZKB uvedeny v § 6a a § 15a**, v návrhu zákona se tento pojem jen „přestěhoval“ do pojmů.
  - Ano jsou, ale **vztahují se ke KII či KKI** (tedy dle nového k vyššímu režimu povinností). U § 15a je to o vyžádání dat k incidentu
  - **Nově povinnost pro všechny regulované subjekty.**

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		✔

- *„primárním aktivem jsou informace a služby. Informacemi se rozumí také data, včetně provozních údajů.“*
- Doporučujeme: **„primárním aktivem jsou data, informace a služby“**
  - Pokud chcete jako primární aktivum označit i data, pak nelze dát rovnítko mezi pojem informace a data.
- Zařazení dat do výčtu toho, co je primárním aktivem, bylo zamítnuto z důvodu, **aby data bez kontextu nebyla evidována jako samostatná primární aktiva**. Současně je však potřeba s nimi tam, kde je to relevantní, dále pracovat, z toho důvodu jsou zařazena do kategorie „informace“.
  - **V kontextu znění definice a vysvětlení provozních dat…toto vysvětlení moc nedává smysl.**

- *„primárním aktivem jsou informace a služby. Informacemi se rozumí také data, včetně provozních údajů.* ***Službou se rozumí také procesy.“***
- Doporučujeme: **„primárním aktivem jsou data, informace, služby a procesy “**
  - V kontextu předchozí připomínky je třeba uvést, že služby nejsou totéž, co procesy. Pokud chcete vymezit procesy jako primární aktivum, bylo by vhodnější uvést definici ve které procesy přímo označíte za primární aktivum. **Otázkou je, zda je nezbytné vyčleňovat procesy samostatně**.
- **Zahrnutí procesů do kategorie služeb bylo provedeno s ohledem na praktické zkušenosti s identifikací primárních aktiv** v regulovaných organizacích.
- Toto chápání procesů je součástí praxe již v rámci dosavadní právní úpravy, a odpovídá tak běžné praxi na poli kybernetické bezpečnosti, nicméně výslovné uvedení by mělo vést k posílení právní jistoty adresátů. **Zároveň se zachovává primární použití pojmu „služba“ (namísto procesů, se kterými pracují normy ISO řady 27000)**, **neboť primárním aktivem může být ve vhodných případech i celá regulovaná služba.**
- Opuštění tohoto pojmosloví a nahrazení procesem by mohlo vést ke zmatení adresátů normy.
  - Tvořen je nový zákon a prováděcí předpisy. **Zmatení uživatelů nastane.** Ale tady to alespoň jednotíme.

TECHNICKÉ AKTIVUM

- ***„technickým aktivem jsou technické a programové prostředky a vybavení.*** *~~Technickým a programovým prostředkem a vybavením se rozumí také komunikační prostředky, sítě elektronických komunikací a průmyslová, řídící nebo jiná obdobná specifická aktiva,“~~*
  - **Doporučujeme vypuštění**
  - Dle vašeho odůvodnění dochází k výslovnému uvedení některých typických technických aktiv, jejichž interpretace jako technického aktiva nemusela být vždy na první pohled zřejmá. **Domníváme se, že by zákon měl být dostatečně srozumitelný, ale na druhou stranu dostatečně obecný** a neomezující vývoj ICT. Z tohoto důvodu se domníváme, že **je vhodné odstranit vámi uváděný demonstrativní výčet**.
- **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.
- Zvolená **formulace je dle našeho názoru dostatečně obecná, aby pokryla velké množství (v současné praxi běžně používaných) prostředků**, zároveň poskytuje prostor pro další, výslovně neuvedené.

cesnet

VÝZNAMNÝ DOPAD

- **Definování pojmu významný dopad pro oba regulované subjekty. Stanovit jasně kritéria pro určení významného dopadu.**
  - V zákoně i prováděcích předpisech **pracujete s pojmem „významný dopad"**, ale tento je do určité míry definován jen k poskytovateli v režimu nižších povinností (viz § 25 vyhlášky o nižších povinnostech). **Ale s pojem významný dopad je pracováno i ve vztahu k poskytovateli v režimu vyšších povinností** – viz např.
    - § X Náležitosti hlášení kybernetických bezpečnostních incidentů, odst. 2, 3
    - Zvládání kybernetických bezpečnostních incidentů, odst. 2
    - Informační povinnost poskytovatele regulované služby, odst. 1
    - Národní úřad pro kybernetickou a informační bezpečnost, odst. 5 písm. j)
  - Ve vyhlášce o vyšších povinnostech je tento pojem použit: § 2 písm. e)
  - Pojem je použit i v § 4 Vyhlášky o regulovaných službách vztahující se na oba subjekty regulace.
- Domníváme se, že by bylo vhodné vydefinovat pojem významný dopad obecně. Navrhujeme uvést, že **významný dopad a jeho hodnocení je uvedeno v jednotlivých vyhláškách vztahujících se k poskytovatelům regulovaných služeb.**
- Je zřejmé, že pro každého poskytovatele může významný dopad představovat jinou situaci.

VÝZNAMNÝ DOPAD

- Pojem významný dopad je v rámci zákona **používán pro různé situace a pokaždé je vysvětlen** v prováděcích předpisech.
  - **Není.**
- Významný dopad v definici regulované služby je definován kritérii pro identifikaci a určení regulované služby (*§ X Kritéria regulované služby: 1) Regulovaná služba je stanovena kritérii pro identifikaci regulované služby ve vymezených odvětvích nebo kritérii pro určení regulované služby,* ***která vymezují významnost dopadu služby na zabezpečení důležitých společenských nebo ekonomických činností.***
  - **Významnost dopadu služby ≠ významný dopad.**
- **Kritéria pro určení významnosti incidentu u režimu nižších povinností** jsou stanovena příslušnou vyhláškou a tato kritéria **budou využita i pro potřeby identifikace incidentu, na který se vztahu informační povinnost poskytovatele regulované služby**.
  - **Ok. A režim vyšších povinností?**
- S ohledem na skutečnost, že **pojem „významný dopad" je v zákoně a jeho prováděcích předpisech používán v několika mírně odlišných významech** (a za tím účelem je vždy doplněn o specifikaci dopadu, např. „incident s významným dopadem na poskytování regulované služby"), **nejeví se stanovení univerzální definice jako vhodné**, neboť by byla poměrně obecná a nepřinášela by adresátům normy zrádnou přidanou hodnotu.
  - **Ok?**

- *„digitální prostředí tvořené aktivy umožňující vznik, výměnu a další zpracování informací a dat,“*

- Doporučujeme:
  - prostředí tvořené aktivy umožňující vznik, **změnu, zánik** ~~výměnu~~ a další zpracování informací a dat,
  - prostředí tvořené aktivy umožňující ~~vznik, výměnu a další~~ **zpracování** informací a dat,
  - prostředí tvořené aktivy umožňující vznik, **změnu, zánik** a další zpracování informací a dat, **tvořené informačními systémy, a službami a sítěmi**

- **Zpracováním se ve smyslu GDPR myslí v zásadě jakékoli nakládání s daty a informacemi**, z této premisy vycházíme a **„vznik a výměna“ jsou v definici *de facto* nadbytečné**, protože jsou již obsaženy v pojmu „zpracování“. **Jejich explicitní uvedení je spíše pro posílení právní jistoty adresátů** a navazuje na definici kybernetického prostu v současném ZKB.

- Co se týče dalšího rozšiřování pojmu, zde podle našeho názoru postačí interpretace v odůvodnění normy, konkrétně: Definice kybernetického prostoru v zásadě přejímá definici obsaženou v dosavadním zákoně o kybernetické bezpečnosti
  - Zmatení uživatelů nastalo (181/2014: *„kybernetickým prostorem digitální* ***prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“***

cesnet

Zmatení uživatelů nastane.

cesnet

42

- *„bezpečností informací zajištění dostupnosti, důvěrnosti a integrity informací a dat“*
- Doporučujeme: bezpečností informací zajištění dostupnosti, důvěrnosti, integrity **a autentičnosti** informací a dat
  - Původní triáda CIA je v současné době ne zcela dostačující. **Specificky je chráněna i autentičnost** (tj. pravost, původnost) dat. (EU) 2022/2555 explicitně tuto oblast zmiňuje… v současné době…**bude na místě se zaměřit právě na problematiku autentičnosti, tedy např. potvrzení toho, že konkrétní úkon učinila oprávněná osoba**.
- Nahrazení CIA modelu jiným konceptem je na NÚKIB pravidelně diskutovaná otázka a prozatím jsme vždy došli k závěru, že je stávající pojetí dostatečné. **Zákon o kybernetické bezpečnosti má sloužit jako univerzální předpis řešící kybernetickou bezpečnost různých druhů služeb, které reguluje**. **Navrhované doplnění se v převážné míře váže na oblast digitálních podpisů nebo obecně služeb vytvářejících důvěru a upravuje trochu jinou otázku**, než která je předmětem úpravy kybernetické bezpečnosti v navrhovaném zákoně. Legislativa, která odvětví služeb vytvářejících důvěru reguluje, však i nadále zůstává v platnosti (pouze část kybernetické bezpečnosti je nově přenesena do zákona o kybernetické bezpečnosti), problematiku jdoucí nad rámec zákona o kybernetické bezpečnosti tedy budou i nadále řešit k tomu příslušné předpisy a příslušní regulátoři.
- **Pojem bezpečnost informací se netýká obsahu informace, ale pouze funkčnosti prostředí, v němž je informace tvořena, zpracována, uchovávána a komunikována**. Narušením autenticity obsahu informace ovšem zároveň dochází k narušení integrity tohoto funkčního prostředí. Autenticita informace je tedy pro potřeby zákona o kybernetické bezpečnosti chápána jako součást integrity.
  - **CIA informací a dat?**
- Nadto lze doplnit, že autenticitu lze chápat i jako součást integrity, tedy v zákoně zahrnuta je.

KYBERNETICKÁ BEZPEČNOSTNÍ UDÁLOST

Hrozba:

„jakákoliv potenciální okolnost, ***událost*** *nebo jednání,* ***které mohou poškodit, narušit*** *nebo jinak nepříznivě ovlivnit aktiva, jejich uživatele nebo další osoby,* ***a tím způsobit*** *kybernetickou bezpečnostní* ***událost nebo*** *kybernetický bezpečnostní* ***incident****“*

Událost:

„kybernetickou bezpečnostní ***událostí událost****,* ***která může způsobit*** *kybernetický bezpečnostní incident“*

Příklad:

Událostí může reálně být i přijetí phishingového e-mailu.
Phishingový e-mail s malwarem v příloze svojí povahou bude spíše významnou bezpečnostní událostí, neboť by mohl téměř způsobit bezpečnostní incident, ale můj AV program či EDR tento e-mail detekovaly a odstranily.
Ve vztahu k tomuto případu: je cílem detekovat všechny phishingové e-maily, nebo jen ty „s přidanou hodnotou“?
Jsem reálně schopen zavést taková opatření abych detekoval všechny události? Domnívám se, že nikoliv. V ten okamžik ale pak nejsem v souladu s technickými bezpečnostními opatřeními.

- Pojem „**událost**“ použitý v definici hrozby **je třeba vykládat jako obecný pojem směřující na mnoho různých situací, které mohou představovat kybernetickou bezpečnostní hrozbu**.
- KBU je pak událost, která může způsobit incident (ten se ale nakonec nestal, např. v důsledku toho, že se situace dále nevyvíjela, nebo že zafungovala bezpečnostní opatření). **Zákon požaduje** v rámci bezpečnostních opatření **detekovat a zvládat KBÚ, ne každou událost, která sice představuje hrozbu, ale není KBÚ**. **I zde se pak uplatní přiměřenost**, se kterou povinná osoba ve vyšším režimu volí způsob a rozsah zavádění bezpečnostních opatření v organizaci.
- **Režim nižších povinností?**

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		✔

cesnet

SEZNAM BEZPEČNOSTNÍCH OPATŘENÍ POSKYTOVATELE REGULOVANÉ SLUŽBY

- **Faktický rozdíl mezi povinnostmi jednotlivých poskytovatelů je minimální** (viz předložená komparace)
- Ne zcela logické je **nevyhodnocovat kybernetické bezpečnostní události, když už mám povinnost je detekovat.**
- Obecně rozdíl nebyl v názvech/typech opatření, ale v množství/míře detailu toho, co musely subjekty plnit, **jak rozsáhlou musely mít dokumentaci** atd., z toho plyne např. i to, že jsme v rámci vyhlášky spojili oblasti, které si byly *„blízké“* a kde se zmenšilo množství povinností, aby nebyly samostatné § o jednom bodě. **Není tam vyhodnocování KBU, ale posuzování KBU, což vnímáme jako to stejné.**
- **Zmatení uživatelé?**

- **Nebudeme v současné době institut autorizovaných inspektorů zavádět.**
- Zároveň **došlo ke zjednodušení vyhlášky pro režim nižších povinností** a upřednostnění reaktivní kontroly (resp. ex post).
- Naším **cílem je** v prvé řadě **získat přehled o nových subjektech** včetně informací, které získáme kontrolou subjektů v nižším režimu povinností.

~~Významná kybernetická bezpečnostní událost~~

- jsou podmnožinou KBU, u nichž došlo k zafungování zavedených bezpečnostních opatření. Tento pojem byl vydefinován především s ohledem na požadavky NIS2, která vyžaduje, aby členské státy přijímaly dobrovolná hlášení významných kybernetických událostí a agregované anonymizované informace o takto nahlášených událostech pak předávaly agentuře ENISA. **Jinde tento pojem uplatnění nemá a z toho důvodu bude ze zákona odstraněn.**

cesnet

Další připomínky…

PROVĚŘOVÁNÍ RIZIK SPOJENÝCH S DODAVATELEM

- *„i) technického prostředku nebo vybavení **~~s výpočetní kapacitou~~**,*
  ii) programového prostředku nebo vybavení, nebo
  iii) informační či komunikační služby,“
  - **Proč jsou zaváděny nové, neurčité pojmy:**
    - vybavení **s výpočetní kapacitou**
  - **Doporučujeme vypustit a ponechat pouze definovaný pojem vybavení.**
    - **informační či komunikační služby**
  - **Doporučujeme vypustit a ponechat pouze definovaný pojem služby.**
- **Definice** dotčených pojmů vzešly z opakovaných konzultací návrhu a **odpovídají potřebě zaměření omezení rizikových dodavatelů pouze ve vztahu k takovému plnění, které může mít pravděpodobný dopad na bezpečnost zajišťování dotčené strategicky významné služby.**
- **Pro tento okamžik…Když se cokoliv změní, budeme měnit zákon, nebo ohýbat výklad.**

OMEZENÍ RIZIK SPOJENÝCH S DODAVATELEM

- *„Úřad přezkoumá alespoň jednou za ~~tři roky~~ **12 měsíců** trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle odstavce 1.“*
- **V oblasti ICT jsou 3 roky neúměrně dlouhá doba.**
  - Řešením může být **zkrácení doby, nebo podnět dodavatele** bezpečnostně významné dodávky v kritické části stanoveného rozsahu, **ve kterém např. doloží nápravu původního nežádoucího stavu.**
- Lhůta stanoví nejzazší termín. V případě, že se tedy Úřad ještě před uplynutím lhůty dozví o tom, že skutečnosti, na jejichž základě bylo opatření vydáno pominuly, **bez zbytečného odkladu opatření odpovídajícím způsobem změní** či zruší.
- **Proč to tedy není jasně stanoveno?**

- **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*? -> dozorový úřad
- **Bude snahou souvisejících prováděcích opatření dosáhnout stavu, kdy stačí incident nahlásit na zvolenou, domněle nejspecializovanější autoritu (z množiny existujících či připravovaných: NÚKIB, ENISA, ÚOOÚ apod.), která potřebné informace o incidentu implicitně zpropaguje všemi dalšími, související legislativou předepsanými směry? (*při incidentu v reálném světě se také nevolá zvlášť hasičům, záchrance a policii, třebaže je zapotřebí více složek*).** Doplnit případně chybějící údaje z iniciativy dané, takto nepřímo zapojené autority by už pak mohla být pouhá formalita, navíc by velká část takové propagace informací měla jít zautomatizovat, a to na jednom jediném místě (srov. s pokusy každé dotčené organizace si takto předem očekávatelné mnohačetné hlášení zautomatizovat na vlastní pěst a nekonzistentně, navíc při do budoucna neodhadnutelném růstu typů incidentů, které se budou dle legislativy muset hlásit na další a další nová místa).
- **Jedním z cílů Úřadu je zprovoznit platformu pro jednotné hlášení incidentů, přes kterou by byly hlášeny incidenty i mimo oblast kybernetické bezpečnosti.**
- **Takže jen k incidentům…**

cesnet

NÁLEŽITOSTI HLÁŠENÍ

- *„Poskytovatel regulované služby **hlásí kybernetické bezpečnostní incidenty** včetně dobrovolných hlášení podle tohoto zákona vždy prostřednictvím Portálu NÚKIB. **Nelze-li využít Portálu NÚKIB, zašle** poskytovatel regulované služby v režimu vyšší povinností hlášení **na adresu elektronické pošty** Úřadu určenou pro příjem hlášení kybernetických bezpečnostních incidentů, **nebo do datové schránky Úřadu.**“*

- **Veškeré hlášení máte vztaženo toliko k elektronické komunikaci.**
  - **Absolutně nepočítáte s výpadkem těchto služeb.** Tím de facto odporujete § 26 odst. 1 písm. a) Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. Obdobně i povinnosti v nižším režimu.
  - Domníváme se, že byste měli definovat i jinou možnou komunikaci v případě hlášení incidentu než jen tu, kterou uvádíte v tomto ustanovení.

cesnet

NÁLEŽITOSTI HLÁŠENÍ

- **V případě útoku** velkého rozsahu, **který by byl způsobilý zcela vyřadit fungovaní Portálu, informačního systému datových schránek a zároveň fungování elektronické pošty by velmi pravděpodobně bylo vyhlášen stav kybernetického nebezpečí**, kdy by koordinace a komunikace byla řešena dle dostupných prostředků, konkrétní situace a odpovídajících krizových plánů. **Vládní CERT má i v současnosti zveřejněné telefonní číslo**, skrze které jde incidenty v krajních případech nahlásit a neprodleně řešit, s ohledem na odhadovaný počet regulovaných subjektů a kapacity vládního CERT však nemůže jít o standardně používaný způsob hlášení incidentů. **Obdobně si nemyslíme, že je reálné zakotvit jako efektivní náhradní způsob hlášení např. poslání dopisu**.
- **Ne to není. Nicméně požadováno je hlášení jedním způsobem a není připuštěn způsob jiný.**
- **Nesplním-li povinnost dle zákona, hrozí mi sankce**

- *„Má se za to, že čin, který vykazuje formální znaky přestupku podle tohoto zákona, je společensky škodlivý.“*
  - Vedle materiálního znaku: škodlivosti, musí být splněny znaky formální: uvedené v zákoně.
  - Konstatování: *„formální znaky **dle tohoto zákona = škodlivost**“* jde proti obecné definici přestupku.
  - Viz § 5 zák. č. 250/2016: *„Přestupkem je **společensky škodlivý** protiprávní čin, **který je v zákoně za přestupek výslovně označen** a který vykazuje znaky stanovené zákonem, nejde-li o trestný čin.“*

- **Jak budete postupovat v případě, že budou naplněny formální znaky, ale nebude naplněn znak materiální?**

- **Materiálně-formální pojetí přestupků se pro oblast regulace kybernetické bezpečnosti nejeví jako zcela vhodné.**

  Společenská škodlivost je u těchto přestupků s ohledem na specifickou oblast kybernetické bezpečnosti dána již samotným naplněním skutkové podstaty přestupku. V případě, že by konkrétní společenská škodlivost protiprávního jednání nedosahovala ani minimální hranice typové škodlivosti, nebyl by dán veřejný zájem na jeho stíhání.

- *„Při stanovení rozsahu řízení kybernetické bezpečnosti* ***neurčí nebo neidentifikuje všechna primární aktiva*** *související s poskytováním regulované služby ~~nebo relevantní organizační části a podpůrná aktiva~~“*
  - 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.

VoBOPRSRVP-§ 20 ODST. 2 PÍSM. f)

- *„Nástroj pro správu a ověření identity administrátorů, uživatelů a technických aktiv zajišťuje*

  f) pokud to je s ohledem na správu a ověření možné,

  centralizovanou správu identit s ohledem na vazby mezi aktivy.“

  - Rozumíme tomu, že **směřujete k centralizovaně řízeným systémům**. Ale povinným subjektem můžu být i v případě, že takovýto systém nemám. Provádím např. izolovaný výzkum za účelem dvojího užití. V **některých typech organizací jakákoliv centrální správa nedává smysl a není aplikovatelná.** Tím, že nutíte jít centralizovaným řešením omezujete de facto funkčnost/činnost povinného subjektu.

- Toto písmeno již obsahuje centrálnost nástroje na základě vazeb mezi jednotlivými aktivy. Navíc možnost či **nemožnost centrální správu identit aplikovat, povinná osoba zjistí prostřednictvím správně implementovaného procesu řízení rizik a následného prohlášení o aplikovatelnosti.**

VoBOPRSRVP-§ 25 ODST. 4 PÍSM. a, b)

- *„Povinná osoba provádí pravidelné skenování zranitelnosti technických aktiv regulované služby*

  a) ***z interní a externí komunikační sítě a***

  b) alespoň jednou ročně.“

  - Proč bych měl provádět sken zranitelností z externí sítě, pokud mé technické aktivum není v této externí síti?

- Pokud dané aktivum není dostupné z externí sítě není možné sken z externí sítě ani fakticky realizovat, **tím pádem je nutné například správně zdokumentovat nemožnost zavedení tohoto bezpečnostního opatření a postupovat v rámci procesu řízení rizik.**

cesnet

Co bude dál?

- ze strany NÚKIB dochází k **finálním legislativním pracím** jednotlivých návrhů předpisů a v rámci tohoto procesu **může ještě dojít k dílčím změnám textu jednotlivých dokumentů.**
- **v polovině května 2023 k zahájení mezirezortního připomínkového řízení.** Mezirezortní připomínkové řízení k návrhu zákona by mělo být ukončeno v druhé polovině srpna 2023. Po něm bude následovat předložení návrhu legislativní radě vlády. Předložení návrhu zákona do Poslanecké sněmovny Parlamentu České republiky předpokládá NÚKIB ve čtvrtém kvartálu roku 2023.

cesnet

DĚKUJI ZA POZORNOST

doc. JUDr. Jan Kolouch, Ph.D.
jan.kolouch@cesnet.cz
CESNET
jan.kolouch@law.muni.cz
Masarykova univerzita

Prezentace částečně vznikla v rámci projektu „Centrum excelence pro kyberkriminalitu, kyberbezpečnost a ochranu kritických informačních infrastruktur č. CZ.02.1.01/0.0/0.0/16_019/0000822“