Řízení dodavatelů v oblasti kybernetické bezpečnosti a zkušenosti z kontrol

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

18. října 2023, Brno
TLP: CLEAR

Alena Rybáková
Odbor kontroly

Obsah

- **NEJČASTĚJŠÍ NEDOSTATKY**
- **BEZPEČNOSTNÍ OPATŘENÍ Z VYHLÁŠKY O KYBERNETICKÉ BEZPEČNOSTI**
- **NOVELA ZKB**

Nejčastější nedostatky

ve spojení s dodavateli

Nejčastější nedostatky

Organizační část VKB I:

- Nevhodně stanovený rozsah systému řízení bezpečnosti informací
- Nedostatečné zapojení garantů aktiv do procesu řízení bezpečnosti informací
- Řízení rizik není prováděno v dostatečném rozsahu ani míře detailu

Nejčastější nedostatky

Organizační část VKB II:

- Nedostatečná podpora ze strany top managementu
- Chybějící jednotná pravidla pro řízení dodavatelů v oblasti KB
- Neurčování významných dodavatelů/provozovatelů

Nejčastější nedostatky

Technická část VKB I:

- „Blackbox“ zařízení v síti bez relevantních opatření
- Nedostatečný dohled nad přístupem dodavatelů
- Používání zastaralého HW a SW

Nejčastější nedostatky

Technická část VKB II:

- Nedostatečné sbírání a uchovávání logů
- Využívání sdílených účtů
- Nedostatečné zálohování

Bezpečnostní opatření z vyhlášky o kybernetické bezpečnosti

Vyhláška č. 82/2018 Sb., vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

Typy dodavatelů

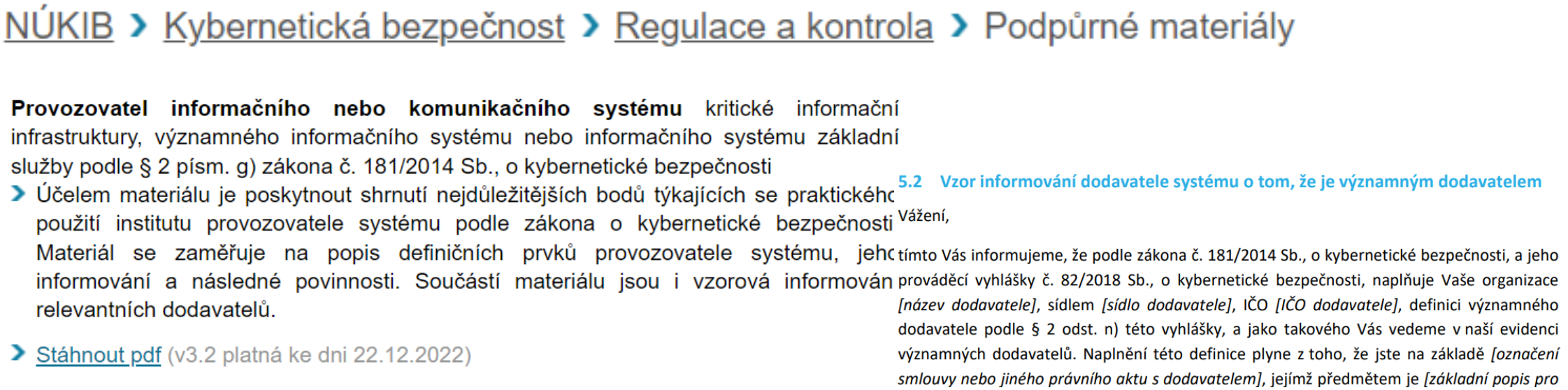
3 typy dodavatelů:

- **„Dodavatel“**
- **Významný**
  - *„provozovatel a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému“ (VKB)*
- **Provozovatel**
  - *„orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém“ (ZKB)*
  - Povinná osoba ze ZKB

Provozovatel

- Zajišťování funkčnosti technických a programových prostředků může zajišťovat i více provozovatelů
- S nZKB zanikne

Podpůrný materiál



NÚKIB › Kybernetická bezpečnost › Regulace a kontrola › Podpůrné materiály

Provozovatel informačního nebo komunikačního systému kritické informační infrastruktury, významného informačního systému nebo informačního systému základní služby podle § 2 písm. g) zákona č. 181/2014 Sb., o kybernetické bezpečnosti

› Účelem materiálu je poskytnout shrnutí nejdůležitějších bodů týkajících se praktického použití institutu provozovatele systému podle zákona o kybernetické bezpečnosti. Materiál se zaměřuje na popis definičních prvků provozovatele systému, jeho informování a následné povinnosti. Součástí materiálu jsou i vzorová informován relevantních dodavatelů.

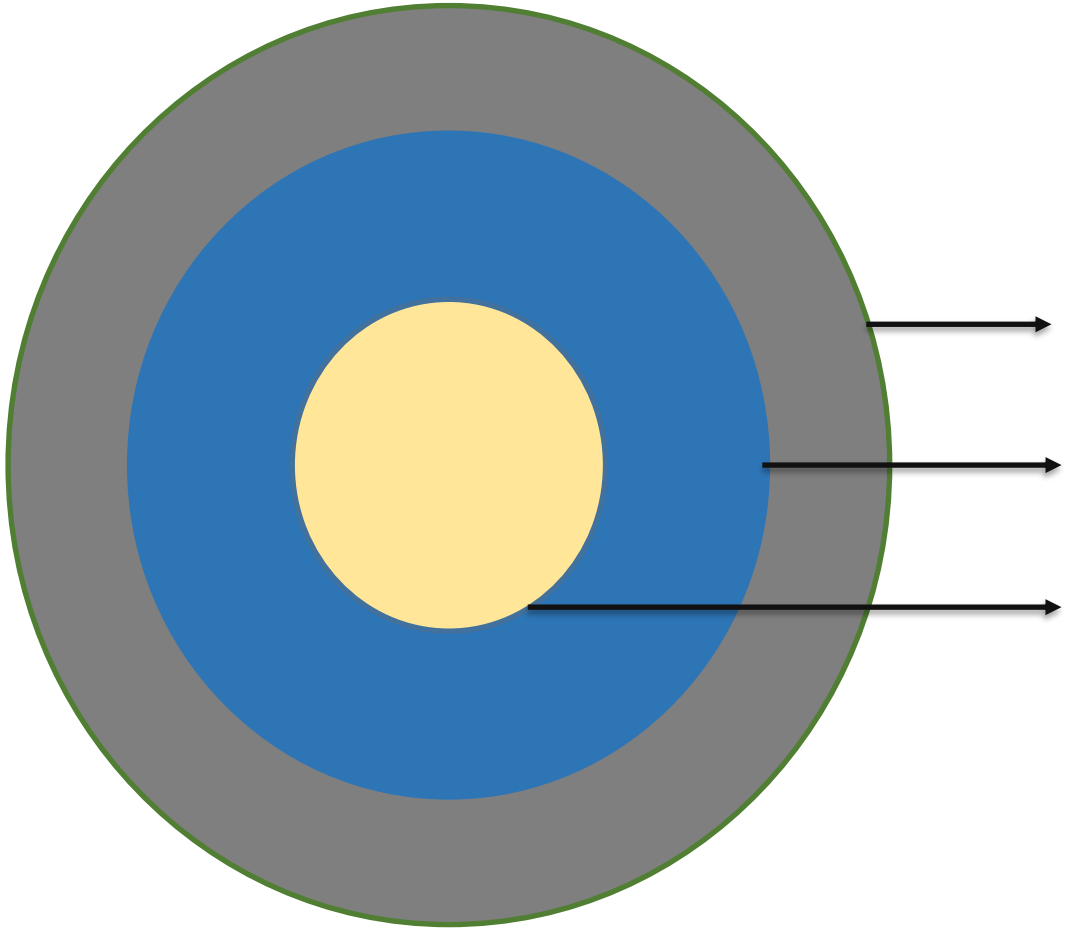
› Stáhnout pdf (v3.2 platná ke dni 22.12.2022)

5.2 Vzor informování dodavatele systému o tom, že je významným dodavatelem

Vážení,

tímto Vás informujeme, že podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcí vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, naplňuje Vaše organizace *[název dodavatele]*, sídlem *[sídlo dodavatele]*, IČO *[IČO dodavatele]*, definici významného dodavatele podle § 2 odst. n) této vyhlášky, a jako takového Vás vedeme v naší evidenci významných dodavatelů. Naplnění této definice plyne z toho, že jste na základě *[označení smlouvy nebo jiného právního aktu s dodavatelem]*, jejímž předmětem je *[základní popis pro*

Typy dodavatelů



Všichni dodavatelé = běžní, významní, provozovatelé

Významní dodavatelé (vč. provozovatelů)

Provozovatelé

§ 8 VKB – řízení dodavatelů

Povinná osoba

- stanoví **pravidla** pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací,
  - **seznamuje** své dodavatele s pravidly podle písmene a) a vyžaduje plnění těchto pravidel,
- vede **evidenci** svých významných dodavatelů,
  - prokazatelně písemně informuje své významné dodavatele o jejich evidenci,
    - ➢ vzor viz podpůrný materiál Provozovatel

§ 8 VKB – řízení dodavatelů

Povinná osoba

- **řídí rizika** spojená s dodavateli,
- v souvislosti s řízením rizik spojených s významnými dodavateli zajistí, aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní oblasti uvedené v příloze č. 7 k této vyhlášce, a
- pravidelně přezkoumává plnění smluv s významnými dodavateli z hlediska systému řízení bezpečnosti informací.

§ 8 VKB – řízení dodavatelů

Povinná osoba **u významných dodavatelů** dále

- v rámci výběrového řízení a před uzavřením smlouvy provádí **hodnocení rizik** souvisejících s plněním **předmětu výběrového řízení** přiměřeně podle přílohy č. 2 k této vyhlášce,
- v rámci uzavíraných smluvních vztahů **stanoví způsoby a úrovně realizace bezpečnostních opatření** a určí obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření,

§ 8 VKB – řízení dodavatelů

Povinná osoba **u významných dodavatelů** dále

- provádí pravidelné hodnocení rizik a pravidelnou **kontrolu** zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany a
- v reakci na rizika a zjištěné nedostatky zajistí jejich řešení.

§ 8 VKB – řízení dodavatelů - příloha č. 7 VKB

Příklad:

- ustanovení o povinnosti dodavatele informovat povinnou osobu o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
- specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,
- pravidla pro likvidaci dat.

Podpůrný materiál:

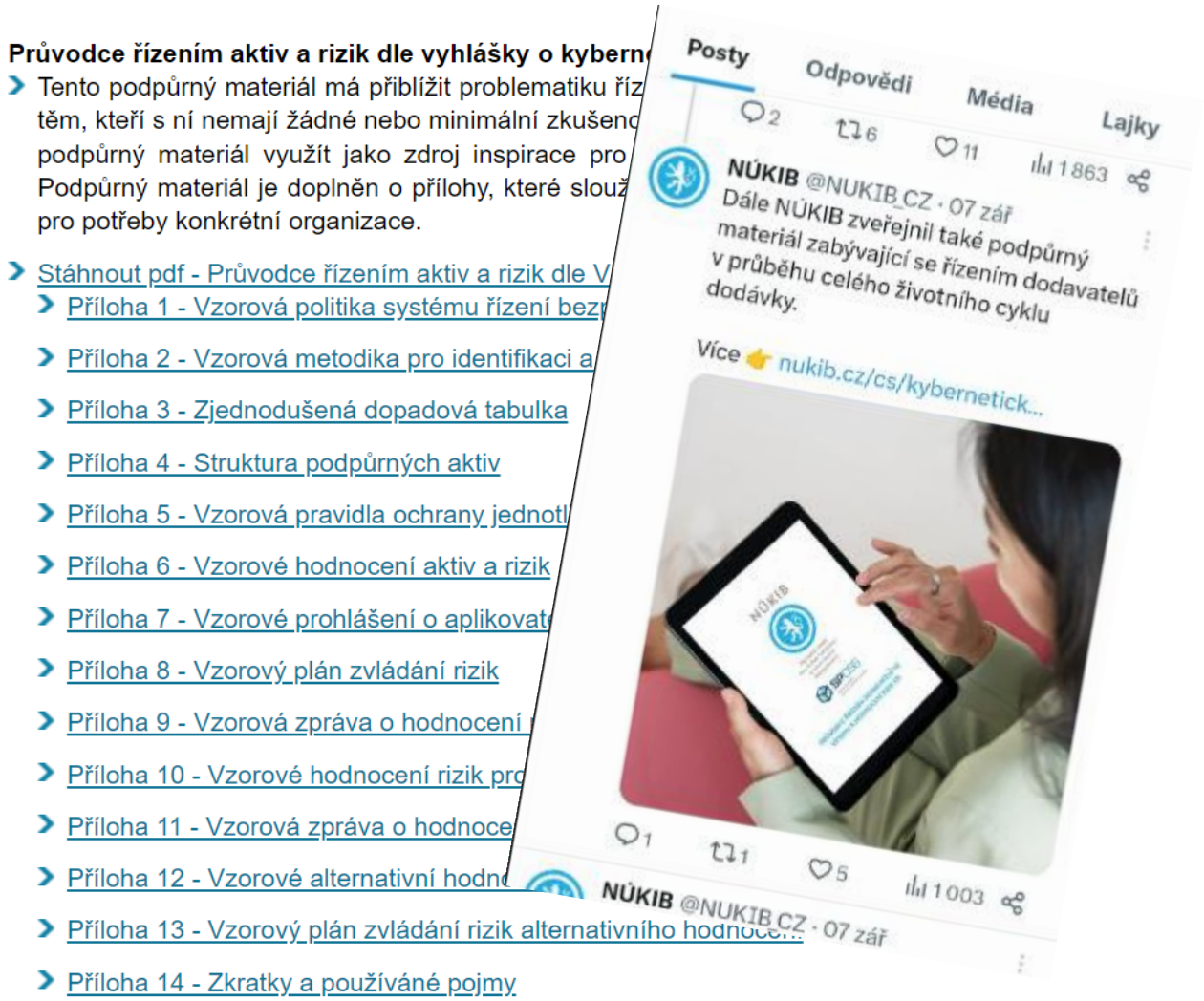
- **Požadavky na smlouvy s dodavateli**
- https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-akontrola/podpurne-materialy/

Řízení rizik nejen ve vztahu k dodavatelům

Podpůrný materiál:

- **Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti**
- **Průvodce řízením dodavatelů ve vztahu k hodnoceni rizik KB**

https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/



Řízení rizik v souvislosti s výběrovým řízením

ZKB § 4

- **(4)** Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. **Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.**

Řízení rizik v souvislosti s výběrovým řízením

- https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-19165.html

ČÍSLO JEDNACÍ: **28082/2023/500**
SPISOVÁ ZNAČKA: **S0172/2023**

Instance	I.
Věc	FN Motol – Dodávky PC sestav pro FN Motol v období 2022 – 2026
Účastníci	1. Fakultní nemocnice v Motole
Typ správního řízení	Veřejná zakázka
Typ rozhodnutí	§ 257 písm. f) zákona č. 134/2016 Sb.
Rok	2023
Datum nabytí právní moci	11. 8. 2023
Dokumenty	dokument ke stažení 471 KB

„Předinstalované programové vybavení (image na disku) – musí být plně kompatibilní s OS používaném na stávajících PC ve vlastnictví zadavatele – OEM MS Windows 10 Professional CZ 64 bit“, přičemž, jak uvedl ve Vysvětlení zadávací dokumentace ze dne 13. 6. 2022, uvedený požadavek plní pouze OEM licence poskytnutá výrobcem zařízení**, a tím vytvořil bezdůvodnou překážku hospodářské soutěže,** a znemožnil tak účast v soutěži dodavatelům, kteří dodávají licence jiného typu než OEM a byli by objektivně schopni předmět plnění realizovat a dne 26. 8. 2022 uzavřel rámcovou dohodu, **se podle § 257 písm. f) citovaného zákona zastavuje, neboť v řízení zahájeném z moci úřední nebyly zjištěny důvody pro uložení sankce podle § 268 citovaného zákona.**

Řízení rizik v souvislosti s výběrovým řízením

ZÁVĚRY ÚŘADU

39. Úřad přezkoumal na základě ustanovení § 248 a následujících ustanovení zákona případ ve všech vzájemných souvislostech a po zhodnocení všech podkladů, na základě vlastních zjištění, tj. zejména při zohlednění závěrů uvedených ve stanovisku NÚKIB konstatuje, že správní řízení vedené ve věci možného spáchání přestupku obviněným podle § 268 odst. 1 písm. b) zákona uvedeného ve výroku tohoto usnesení se podle § 257 písm. f) zastavuje, neboť v řízení zahájeném z moci úřední nebyly zjištěny důvody pro uložení sankce podle § 268 zákona.

Řízení rizik musí probíhat v souladu s §5 VKB!

Relevantní varování vydaná NÚKIB

Varování před použitím technických nebo programových prostředků společností Huawei Technologies Co., Ltd., a ZTE Corporation

- https://www.nukib.cz/download/uredni_deska/Varovani_NUKIB_2018-122-17.pdf

Podpůrné materiály:

- **Metodika k varování ze dne 17. prosince 2018**
- **Zohlednění varování ze dne 17. prosince 2018 v zadávacím řízení**
- https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

Řízení dodavatelů – další podpůrné materiály

Podpůrné materiály:

- **Metodika řízení dodavatelů**
- **Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost**
- https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

Novela ZKB

Krátké shrnutí

Novela ZKB - shrnutí

- Na základě NIS 2
- Předpokládaná platnost říjen 2024

- Aktuálně v legislativním procesu, stále mohou nastat změny

- Více informací:
  - https://osveta.nukib.cz/course/view.php?id=145
  - regulace@nukib.cz

Vítejte na webových stránkách věnovaných blížící se regulaci kybernetické bezpečnosti v České republice – směrnici Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, tzv. směrnice NIS2 a změnám, které tato směrnice pro kybernetickou bezpečnost v České republice přinese. Tyto změny nastanou až s účinností nového zákona o kybernetické bezpečnosti (podle plánu v druhé polovině roku 2024).

Novela ZKB - shrnutí

- Nově jedna povinná osoba:
  - **Poskytovatel regulované služby**
    - V nižším režimu
    - Ve vyšším režimu
- Povinnost samourčení

Novela ZKB – vyhláška o regulovaných službách

Vyhláška o regulovaných službách:

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby a jeho režim pro tuto službu
Poskytování zdravotní péče	Poskytovatel zdravotní péče podle zákona o zdravotních službách je I. poskytovatel regulované služby **v režimu vyšších povinností**, v případě, že a) je velkým podnikem, nebo b) disponuje počtem lůžek akutní péče nejméně 270, II. poskytovatel regulované služby v režimu **nižších povinností**, v případě, že je středním podnikem.
Poskytování zdravotnické záchranné služby	Zdravotnická záchranná služba podle zákona o zdravotních službách je poskytovatel regulované služby v režimu **nižších povinností**, v případě, že je velkým nebo středním podnikem.

nVKB – nižší režim

- Identifikace aktiv a stanovení rozsahu systému řízení bezpečnosti informací v nZKB

Řízení dodavatelů:

- Pouze náležitosti smlouvy, celkem 13 bodů
  - Obdoba aktuální přílohy č. 7 VKB

Povinnosti dále upravené vyhláškou:

1. povinnosti vrcholového vedení
2. bezpečnost lidských zdrojů
3. řízení kontinuity činností
4. řízení přístupu
5. řízení identit a jejich oprávnění
6. detekce a zaznamenávání kybernetických bezpečnostních událostí
7. řešení kybernetických bezpečnostních incidentů
8. bezpečnost komunikačních sítí
9. aplikační bezpečnost
10. kryptografické algoritmy

nVKB – vyšší režim

- **Obdoba aktuální VKB**
  - Nově stanovení rozsahu systému řízení bezpečnosti informací a identifikace aktiv již v nZKB

- **Řízení dodavatelů**
  - Bez zásadní změny

Souhrn zdrojů

KONZULTACE ZKB
regulace@nukib.cz

PODPŮRNÉ MATERIÁLY
https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

NIS 2
https://osveta.nukib.cz/course/view.php?id=145

VZDĚLÁVÁNÍ
https://osveta.nukib.cz/ - vzdělávací portál NÚKIB
https://www.nukib.cz/cs/kyberneticka-bezpecnost/vzdelavani/

SLUŽBY VLÁDNÍHO CERT
https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/poskytovane-sluzby/
cert@nukib.cz

Alena Rybáková

ředitelka odboru kontroly

Email: alena.rybakova@nukib.cz
Telefon: +420 720 966 957