Nabídka - „Rozdílová analýza metodiky řízení kybernetických rizik a metodiky NUKIB (květen 2022)“ pro odbor KB

Správa železniční dopravní cesty, státní organizace

Praha 1, Nové Město, Dlážděná 1003/7, PSČ 110 00

„Dne 10.1.2023“

Aktualizace dne 10.02.2023

Aktualizace dne 2.5.2023

NETIA® s.r.o., Hliníky 259, 679 72 Kunštát

tel.: [redacted]

www.netia-it.cz

Obsah

1. Identifikační údaje uchazeče

Nabídku předkládá: NETIA® s.r.o.

Společnost NETIA® s.r.o. byla založena 24. ledna 2000, v souladu se zákony České republiky a je Vedená u Krajského soudu v Brně, oddíl C, vložka 36167.

Identifikační údaje dodavatele:
NETIA®, s.r.o.
Hliníky 259, 679 72 Kunštát
Telefon: [redacted]
E-mail: [redacted]
Česká Republika

IČO: **25588869**
DIČ: CZ **25588869**

Právní forma:
Společnost s ručením omezeným
Zapsáno: 24. ledna 2000

Jednatel:
Ing. [redacted]

Kontaktní osoby:
Kontaktní osoba pro věci obchodních:

[redacted]
Jednatel
Mobil: + [redacted]
E-mail: [redacted]

Kontaktní osoba pro věci technických:

[redacted]
Manažer realizace a konzultant
Mobil: + [redacted]
E-mail: [redacted]

Bankovní spojení:

FIO banka, číslo účtu: [redacted]

2. Účel dokumentu

Účel dokumentu je popsat a analyzovat stávající nastavení IS AURIS, které vychází ze stávající metodiky řízen aktiv a rizik a navrhnout úpravy nastavení tak aby odpovídalo obecné metodice NUKIB vydané v květnu 2022.

3. Výchozí předpoklady – stávající stav

Stávající metodika vychází z obdobných metodik řízení rizik a aktiv a odpovídá požadavkům Vyhlášky 82/2018 Sb. Vyhláška stanový požadavky velmi obecně a některé věci jsou řešeny poměrně složitě, více ve vazbě na ISO 27000. Nejvýraznější prvky metodiky jsou:

- Je definován složitý vztah mezi Zranitelností a Podpůrným aktivem.
- Pro výpočet hodnoty aktiva se provádí dvakrát, přičemž jeden z výpočtů se nepromítne do dalších výpočtů.
- Metodika není jednoznačná v řadě oblastí řízení aktiv a rizik, kdy v tomto případě byl zvolen přístup, který odpovídá vyhlášce 82/2018 Sb. Jedná se o oblasti.
    - Vazby mezi primárním a podpůrných aktivem a způsob dědění hodnocení
    - Způsob agregace rizik podpůrného aktiva
    - Práce s nápravným opatřením a jeho vztah k mitigaci rizika
    - Řízení rizik a jejich akceptace

3.1 Aktuální seznam šablon

Šablony

Aktivní | Smazané

Přidat | Upravit

Název	Verze	Popis	Status	Změnil
			Provozní	
KB | Agregovaná rizika	1	Agregovaná rizika podpůrných aktiv		Knapek Jiri
KB | Hromadná úprava NO	1	Hromadná úprava NO		Knapek Jiri
KB | Nápravná opatření	1	Nápravná opatření		Knapek Jiri
KB | Nová hrozba	1	Zadání a editace hrozby		Knapek Jiri
KB | Nová zranitelnost	1	Zadání a editace zranitelnosti		Knapek Jiri
KB | Podpůrná aktiva (v2)	1	Správa podpůrného aktiva		Knapek Jiri
KB | Primární aktiva	1	Správa primárního aktiva		Knapek Jiri
KB | Registr rizik	1	Registr rizik		Knapek Jiri
KB | Sdílené úložiště	1	Ukládání dokumentů		Knapek Jiri
KB | Vazby aktiv	1	Vazby mezi primárními a podpůrnými aktivy		Knapek Jiri
Import hrozeb	1			Knapek Jiri
Import podpurnych aktiv	1			Knapek Jiri
Import primarnich aktiv	1			Knapek Jiri
Import zranitelnosti	1			Knapek Jiri

4. Stručná charakteristika metodiky NUKIB

Metodika NUKIB byla zveřejněna na stránkách úřadu ke dni 20.5.2022. Nejedná se o metodický pokyn jako takový, ale o metodiku fiktivního úřadu „Ministerstva pro certifikaci senzorů“.

Metodika je popsána v níže uvedených materiálech a jeho přílohách.

- Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpenosti.pdf
- Podpurny_material_system_a_rozsah_ISMS_v1.0.pdf
- Příloha 9 - Vzorová zpráva o hodnocení rizik.pdf
- Příloha 8 - Vzorový plán zvládání rizik.xlsx
- Příloha 7 - Vzorové prohlášení o aplikovatelnosti.xlsx
- Příloha 6 - Vzorové hodnocen aktiv a rizik.xlsx
- Příloha 5 - Vzorová pravidla ochrany jednotlivých úrovní aktiv.pdf
- Příloha 4 - Struktura podpůrných aktiv.pdf
- Příloha 3 - Zjednodušená dopadová tabulka.pdf
- Příloha 2 - Vzorová metodika pro identifikaci a hodnocen aktiv a hodnocen rizik.pdf
- Příloha 14 - Zkratky a používané pojmy.pdf
- Příloha 13 - Vzorový plán zvládání rizik alternativního hodnocen.xlsx
- Příloha 12 - Vzorové alternativní hodnocen rizik u primárních aktiv.xlsx
- Příloha 11 - Vzorová zpráva o hodnocení rizik pro veřejnou zakázku.pdf
- Příloha 10 - Vzorové hodnocení rizik pro veřejnou zakázku.xlsx
- Příloha 1 - Vzorová politika systému řízení bezpečnosti informací.pdf

Metodika NUKIB vychází z příloh vyhlášky a 82/2018 Sb. a rozpracovává především hodnocení aktiv do většího detailu. Zavádí ovšem celou řadu pojmů a pravidel, která ve vyhlášce nejsou.

4.1.1 Základní změny a upřesnění

Z hlediska dopadů do řízení aktiv a rizika tím i do informačního systému AURIS jsou to především níže uvedené oblasti změn.

- Kategorizace primárních aktiv na aktiva typu služba a informace
- Vytvoření vazeb mezi primárními aktivy typu služba a informace.
- Číselník pro hodnocení primárních aktiv
- Způsob dědění vlastností podpůrného aktiva (metodika je v tomto shodná s nastavením systému)
- Zavedení parametru „váha vlivu“ pro hodnocení vazeb mezi primárním a podpůrným aktivem.

- Zavedení časového hodnocení dostupnosti, důvěrnosti a integrity, zavedení pojmu „ztráty dat“
- Zavedení nových pojmů, jako například gestora aktiva
- Je zaveden pojem typového podpůrného aktiva a jeho kategorizace
- Pracuje se dvěma metodami identifikace rizik
- Pro řízení rizik je jednoznačně definovaná matice kombinací hrozeb a zranitelností.
- Řízení rizik je zjednodušeno na způsob zvládání rizika
- Jsou zavedeny typové přílohy pro plán zvládání rizik a prohlášení o aplikovatelnosti
- Jsou upřesněna pravidla pro kategorizaci Hrozeb a Zranitelností
- Jsou jasně definovány pojmy karty (aktiva apod.) a katalogu (tyto pojmy v podstatě kopírují postupy použité v AURIS)
- Nápravná opatření se rozlišují podle typu identifikace

4.1.2 Nejasnosti nové metodiky

Přes velkou propracovanost návrhu jsou některé oblasti, které ve vlastní metodice bude třeba upřesnit, aby bylo možné přesně nastavit systém AURIS.
Tabulky metodiky bohužel neobsahují některé vzorce nebo jsou tyto buňky uzamčené, aby z nich bylo možné nepřímo odpovídající závislosti.

Níže uvedené oblasti bude vhodné upřesnit v rámci konkrétní metodiky SZ:

- V rámci stanovení vazeb mezi primárními aktivy typu služba informace není jasný způsob hodnocení, rozsah dědění hodnocení. Doporučujeme přístup, kdy se hodnocení bude dědit, podobně jako při vazbě primárního a podpůrného aktiva.
- V rámci stanovení vazeb mezi primárními aktivy typu služba informace není jasné, jestli Primární aktivum typu informace může být vázáno na více primárních aktiv typu služba (vazby n:n). V rámci zjednodušení řízení se přikláníme k přístupu, že primární aktivum typu informace bude mít vazbu jen na jedno nadřízení primární aktivum typu služba.
- Matice kombinací mezi Hrozbami a Zranitelnostmi se vytváří pevně nebo na základě daného scénáře. Aktuálně je systém nastaven tak, že se seznam vytváří pro každé podpůrné aktivum zvlášť na základě „filtrů“ a u Zranitelnosti musí být aktivum aktivně zadáno. Metodiky se přikláníme k řešení, že by „matice“ byla dále filtrována například na typ podpůrného aktiva, na které působí zranitelnost a tím se snížil počet kombinací pro hodnocení rizik a tím i samotná analýza. (Tento postup je pro nás složitější).

  Popis návrhu řešení Netia:

-

Komentář je ve vztahu k metodice NUKIB

Katalog hrozeb obsahuje to, jestli hrozba působí dostupnost, důvěrnost, integritu, neobsahuje na jaký typ aktiv působí, ale „vektor útoku".

Katalog zranitelností obsahuje kategorii (nejasně provázanou na kategorie podpůrných aktiv).

Z metodiky není jasné, jestli se tato data mají použít pro nějaké zafitrování do matice pro každé podpůrné aktivum, jestli tato matice platí pro všechna aktiva (cca 120 kombinací) Z kontextu dalších tabulek vyplývá, že se uplatňují jen vybrané kombinace – jednotky kombinací).

Technicky můžeme velmi snadno určit všechny kombinace pro každé podpůrné aktivum a nechat na uživateli, aby vybral platné. Na zpracování to ovšem bude velmi pracné (i když ne tolik, jako připravovat dat v MS Excelu).

Z našeho pohledu je ideální využít parametrů k filtrování relevantních kombinací dopředu.

- Metodika navrhuje fakticky dva způsoby hodnocení rizik a není jasné, do jaké míry lze oba přístupy kombinovat. Naším záměrem je podporovat oba způsoby hodnocení rizik, přičemž míru kombinace je nutné upřesnit metodicky.

  Popis návrhu řešení Netia:

  Metodiky jsou obsaženy v tabulkách:

  Příloha 12 - Vzorové alternativní hodnocen rizik u primárních aktiv.xlsx

  Příloha 6 - Vzorové hodnocení aktiv a rizik.xlsx

  Teoreticky můžeme i oba přístupy kombinovat a to i v rámci jedné analýzy (pokud budeme mít metodický podklad pro převod hodnocení rizik, kdy každá metoda používá jiné stupně.)

- Metodika zavádí pojem hodnocení rizik pro veřejné zakázky. Metodicky ovšem není toto hodnocení dostatečně upřesněno (fakticky se jedná o hodnocení dopadů – rizik projektu). Navrhujeme tato hodnocení evidovat odděleně.

  Popis návrhu řešení Netia:

Návrh předpokládá, že vytvoří „karta změny – veřejné zakázky“ která bude obsahovat popis změny stávajících a budoucích podpůrných aktiv a jejich vztah k primárním aktivům. Tak budeme schopni udělat analýzu rizik vztaženou k veřejné zakázce.

- Oblast řízení rizik (vyjma stanovení taktiky řízení rizika) je fakticky popsána jednou větou. Zde bude nutné stanovit vlastní metodiku. Především je nezbytné upřesnit způsob akceptace rizika, které by měl provádět výbor pro řízení rizik.
- Prohlášení o aplikovatelnosti je definováno obecně. Stávající nastavení předpokládá, že opatření je definováno pro každé podpůrné aktivum zvlášť (lze provázat i na primární aktivum), protože opatření různých systém mohou mít různou úroveň. Zjednodušení prohlášení je možné.

  Popis návrhu řešení Netia:

  V aplikaci je možné připravit podklady, data pro prohlášení o aplikovatelnosti
- Prohlášení o aplikovatelnosti v metodice popisuje vazbu na Zranitelnost, ale tto vazba není dostatečně zohledněna v příloze č. 7 – Prohlášení o aplikovatelnosti.

  Popis návrhu řešení Netia:

  Metodiku NUKIB lze odvodit z tabulky Příloha 7 - Vzorové prohlášení o aplikovatelnosti.xlsx

  U sloupců G-i není jasné, k čemu jsou vztaženy, pravděpodobně k aktivům, sloupce M-V odkazují na katalog zranitelností. V katalogu zranitelností není zřejmý parametr, díky kterému by bylo možné určit relevanci k opatření.
- Není jednoznačně popsána vazba mezi plánem zvládání rizik a jednotlivými opatřením. Doporučujeme opatření evidovat samostatně v souladu s jednoduchými pravidly projektového řízení nebo change managementu. Rozlišovat fáze přípravy na základě „statusu“ opatření.

  Popis návrhu řešení Netia:

  Opět vycházíme z tabulky Příloha 8 - Vzorový plán zvládání rizik.xlsx

  Plán kombinuje různé zdroje (sloupec D), je vázána na vybraná rizika – ale není zřejmé, jestli se do plánu zahrnují všechna opatření nebo jen vybraná, jaká je vazba opatření na konkrétní paragraf. Vyhlášky (jestli je například opatření na řádku 6 provázáno na prohlášení o aplikovatelnosti.

  Poznámka: z rizika lze jen nepřímo dovodit jakého se týká aktiva a zranitelnosti.

5. Rozsah změn při sjednocení metodiky

5.1 Úpravy globálního nastavení

5.1.1 Sjednocení názvosloví

Jde především o sjednocení pojmů dopadu hodnoty aktiv, názvy jednotlivých rolí (Odbor bezpečnosti, Gestor aktiv).

Pracnost je především v rovině analytické. O rámci systému e jedná pouze o změnu názvu proměnné.

5.1.2 Doplnění a přepracování dynamických tabulek (číselníků)

Rozsah pracnosti je podobný jako v předchozím bodě. Například rozšíření způsobu zvládání rizika o položky z metodiky, kategorizace podpůrných aktiv apod.

Číselníky, které již obsahují obdobnou kategorizaci, rozšíříme o nové položky (kategorizace podpůrných aktiv)

Stávající individuální číselníky SŽ navrhujeme zachovat.

5.1.3 Doplnění rolí při řízení ISMS

V rámci metodiky se pracuje s dalšími rolemi, se sterými stávající metodika nepočítala. Např. role pověřence pro ochranu osobních údajů.

Aktuální verze systému TAS umožňuje sloučit technické role do celků, které přesně odpovídají RACI matici v metodice. Odpovídající nastavení je tedy snadnější.

5.1.4 Přehledy (reporting)

Úpravy reportů (přehledů) v systému tak, aby odpovídaly metodice – tabulkám dle metodiky.

Až na výjimky budou tabulky odpovídat metodice. Výjimky, kdy bude nutné zvolit jiný způsob zobrazení jsou:

- Kombinace hrozeb a zranitelnosti. Jde o maticové uspořádání s proměnlivým počtem sloupců. Přehled bude mírně upraven.
- Vazby mezi aktivy. Jde opat o maticové uspořádání a proměnlivým počtem sloupců. Způsob zobrazení neumožní zobrazit další parametry vazby. Vazby budou zobrazeny řádkově, každá vazba na samostatný řádek.

5.2 Úpravy stávajících šablon

5.2.1 Primární aktiva

- Zapracování hodnocení dopadů primárního aktiva dle §2 odst. B. Aktuálně je hodnoceno jako volný text, nově bude hodnoceno číselníkem dle metodiky.
- Doplnění tabulek pro časové hodnocení dostupnosti, důvěrnosti, integrity a ztráty dat.
    - Zanesení určité logicky předepisování hodnot v tabulkách, aby nebylo nutné tabulky vyplňovat celé.
    - Modifikace výpočtů na nejvyšší hodnotu z tabulek
- Zrušení duplicitního výpočtu hodnoty a dopadu aktiva, který je specifický pro stávající metodiku.
- Rozšíření kategorizace primárních aktiv (číselníky)

5.2.2 Typová podpůrná aktiva

- Úprava číselníku členění podpůrných aktiv na typová aktiva (číselníky)
- Doplnění parametrů, které se dědí z primárních aktiv
    - Změna výpočtu korekce hodnoty s využitím parametru „váhy vlivu“. Aktuálně se zadává přímo výsledná hodnota.
    - Parametr Váha vlivu se zadává pro všechna hodnocení primárního aktiva.
- Úprava parametrů ve vazbě na „Prohlášení o aplikovatelnosti“
- Zavedení seznamu vázaných podpůrných aktiv
- Odstranění způsobu hodnocení rizik ve vazbě na podpůrné aktivum

5.2.3 Vazby aktiv

- Zavedení vazby mezi primárními aktivy a odpovídajícím děděním informací.
- Zavedení parametrů váhy vlivu včetně dvou souvisejících číselníků.
- Zjednodušení procesu schvalování a editace vazeb
- Rozšíření parametrů, které se dědí mezi primárním a podpůrným aktivem

5.2.4 Hrozby

- Doplnění číselníku vektor útoku
- Doplnění popisného pole „příklady“

5.2.5 Zranitelnosti

- Odstranění vytváření hodnocení přímo na podpůrná aktiva
- Doplnění vazby na typ podpůrného aktiva
- Doplnění popisného pole „příklady“

5.2.6 Agregovaná rizika (analýza rizik)

- Změna způsobu agregace rizika, kdy rizika mohou být analyzována (agregována), podle
  - A) matice hodnocení Zranitelností a hrozeb
  - B) podle jednotlivých scénářů.
- Bude zachována stávající vlastnost, že katalog obsahuje všechny kombinace hodnot podpůrného aktiva, hrozby a zranitelnosti.
- Způsob zvládání rizika se přesune přímo na riziko, nikoliv jeho agregovanou podobu.
- Přepracuje se způsob mitigace rizika s ohledem na přepracovaná nápravná opatření.
- Aktualizace analýzy rizika bude probíhat samostatným případem.

5.2.7 Registr rizik

- Rozšíření registru o nové položky rizika (zvládání rizika, hodnoty po zavedení opatření apod.)
- Zavedení nového typu registru podle „scénářů“
- Otevření některých položek registru k editaci.

5.2.8 Nápravná opatření

- Přepracování způsobu výběru dotčených rizik ve vazbě na změny v hodnocení rizik
- Doplnění proměnných z přílohy č. 8 metodiky
- Přepracování procesu – jeho zjednodušení na řízení „statusem“

5.3 Nové šablony

5.3.1 Scénáře

- Zavedení nové kategorie scénáře jako kombinace primárního aktiva, podpůrných aktiv, hrozby a zranitelnosti pro následné hodnocení rizik.

Poznámka: Jedná se sice o novou šablonu, ale princip už využívají některé instalace využívající TAS na úrovni pevného číselníku.

5.3.2 Plán zvládání rizik

- Zavedení proměnných pro samostatný plán dle metodiky
- Přiřazení nápravných opatření do plánu zvládání rizik (příloha č. 8)

5.3.3 Prohlášení o aplikovatelnosti

- Zavedení proměnných pro samostatné prohlášení dle metodiky
- Přiřazení opatření ve stanovené struktuře dle metodiky (příloha č. 7)

5.3.4 Analýza rizik pro veřejnou zakázku

- Modifikace případu analýzy rizik pro veřejné zakázky, nové projekty apod.
- Doplnění proměnných dle přílohy č. 10 metodiky
- Oddělení katalogů hodnocení rizik
- Vyloučení rizik z plánu zvládání rizik a nápravných opatření.

6. Harmonogram, pracnosti

Dílčí část díla	Pracnost (MD)	Ukončení do, termín předání	Součinnost
1. Úprav a testování šablony – Hrozby a Zranitelnosti	3	Do 20. 5.2023	
2. Úprav a testování šablony – Podpůrná aktiva	5	Do 20.5.2023	
3. Úprav a testování šablony – Primární aktiva a vazby	7	Do 30.5.2023	
4. Úprav a testování šablony – Agregovaná rizika a registr rizik	3	Do 10.6.2023	
5. Úprav a testování šablony – Nápravná opatření	2	Do 20.6.2023	
6. Vytvoření a testování šablony – Scénáře	5	Do 25.6.2023	
7. Vytvoření a testování šablony – Plán zvládání rizik	5	Do 30.6.2023	
8. Vytvoření a testování šablony – Prohlášení o aplikovatelnosti	5	Do 5.7.2023	
9. Vytvoření a testování šablony – Analýza rizik pro veřejnou zakázku	5	Do 15.7.2023	
10 Finální předání		Do 30.7.2023	
Provedení Díla	40 MD		

Pozn: Pokud by byly některé šablony upraveny, nebo vytvořeny dříve budou se předávat ihned po dokončení.

Odhad ceny vychází ze sazby za MD ze smlouvy o podpoře, nebo z rozvojové smlouvy. Sazba za MD je ve smlouvě 12.000,- Kč bez DPH.

Dle uvedené pracnosti 40 MD – je nabídková cena 480.000,- Kč bez DPH.. Termín dodání: do 30.7. 2023.

7. Závěr

Děkuji vám za prostudování naší nabídky. Naše nabídka plně pokrývá vámi zadané požadavky. Zakázku jsme připraveni realizovat certifikovanými konzultanty.

S pozdravem,

Ing. [redacted]

jednatel, Business development manager

NETIA® s.r.o.

Hliníky 259, 679 72 Kunštát

ICO: 25588869

DICO: CZ25588869

mob: [redacted]

mail: [redacted]

www.netia.cz