CHRENEK | TOMAN | KOTRBA

Role právníka v oblasti kybernetické bezpečnosti: Řízení dodavatelů

Mgr. Šimon Toman

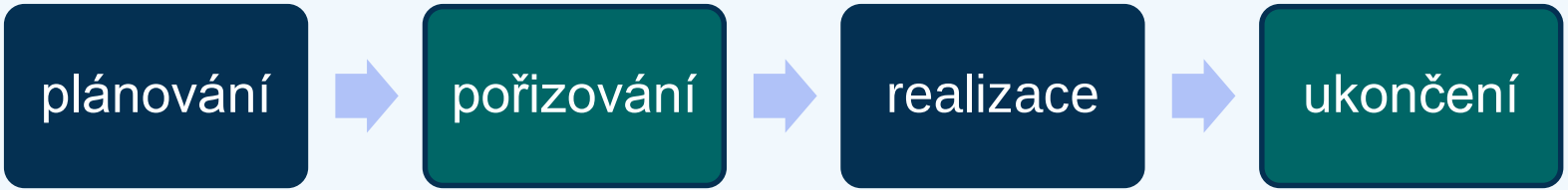
Bezpečnostní opatření: role právníka

Nastavení interních předpisů a metodik

Úprava smluvních vztahů

Řízení dodavatelů

- Zabývá se všemi aspekty výběru i spolupráce s dodavatelem v průběhu celého životního cyklu dodávky
- Týká se dodavatelů, jejichž činnosti přímo souvisejí anebo mohou mít vliv na **dostupnost, důvěrnost či integritu** informačního systému organizace
- Týká se jak případů akvizice, tak vývoje či údržby stávajících systémů.



Činnost organizace v rámci řízení dodavatelů

- Stanoví bezpečnostní **pravidla pro dodavatele**, seznamuje své dodavatele s těmito pravidly a **vyžaduje jejich plnění**
- **Řídí rizika** spojená s dodavateli – před kontraktační + průběžné
- Vede evidenci svých významných dodavatelů
- V souvislosti s řízením rizik spojených s významnými dodavateli zajistí, aby **smlouvy uzavírané s významnými dodavateli obsahovaly relevantní bezpečnostní ustanovení dle ZKB**.
- Pravidelně **přezkoumává plnění smluv a bezpečnostních opatření**

NIS 2 a problematika dodavatelů

- Směrnice NIS2 vyžaduje, aby povinné subjekty přijaly **technická, provozní a organizační opatření k řízení rizik**
- V této souvislosti směrnice NIS2 ukládá **základním a důležitým subjektům** nové povinnosti v oblasti kybernetické bezpečnosti např. ve vztahu k řízení rizik (včetně **řízení rizik dodavatelského řetězce**), hlášení kybernetických incidentů a sdílení informací.
- NIS 2 klade důraz i na **rizika spojená s osobou dodavatele**, ne jen na rizika spojená s konkrétním předmětem plnění či technologií
- V rámci transpozice Směrnice NIS2 jde slovenská právní úprava nad rámec stanovený touto úpravou a stanovila např. analýzu politického rizika dodavatele (implementace tzv. EU Toolboxu)

Řízení dodavatelů – žádná novinka

- **čl. 21 NIS2** – opatření k řízení kybernetických bezpečnostních rizik
  - součástí i opatření k zajištění bezpečnosti dodavatelského řetězce (čl. 21 odst. 2 písm. d) NIS2)
- ekvivalent v současné slovenské úpravě – bezpečnostní opatření dle **§19 odst. 2 a § 20 a násl. ZKB**
    - mj. analýza rizik pří výběru dodavatele + konkrétní bezpečnostní opatření v rámci smluv
- pravidla pro řízení dodavatelů blíže rozvinuta v **§ 8 Vyhlášky NBÚ**
  - vztahují se na povinné osoby => NIS2 rozšíří okruh povinných osob => povinnosti se vztáhnout i na nově povinné subjekty

Jak prakticky postupovat

1) **GAP analýza**
2) **Příprava interní dokumentace**
3) **Praktická implementace**

Politika řízení dodavatelů

Krok číslo 1

- ❑ Stanovení obecných pravidel bezpečnosti pro dodavatele (závazná dokumentace)

- Jednotlivá pravidla se na dodavatele vztahují přiměřeně s ohledem na **charakter dodávky nebo poskytovaných služeb** a s ohledem na zvláštní ustanovení v rámci smluvních ujednání.

- ❑ Stanovení obecných bezpečnostních opatření **pro všechny fáze řízení dodavatele!**

- ❑ Nastavení předem daných smluvních ujednání

Vytvoření katalogu hrozeb, zranitelností a rizik (živý dokument, který obsahuje konkrétní hrozby a rizika pro danou organizaci)

Příklady obecných pravidel pro dodavatele

- Dodavatel musí mít vytvořenou a schválenou bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně dodavatele při poskytování předmětu plnění.
- Dodavatel řídí vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.
- Dodavatel zavádí příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, a to v případě zjištění bezpečnostních rizik či identifikace bezpečnostních potřeb. Bezpečnostní opatření monitoruje a vyhodnocuje jejich účinnost.
- Dodavatel stanovuje a udržuje aktuální bezpečnostní opatření ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.
- **Pokud dodavatel využívá při poskytování předmětu plnění subdodavatele, musí zajistit adekvátní dodržování těchto bezpečnostních požadavků rovněž ve smluvních vztazích se svými subdodavateli.**
- Dodavatel zajišťuje neustálé vzdělávání svých zaměstnanců s cílem poskytovat předmět plnění dle aktuální legislativy, požadavků a nejnovějších technologií či trendů.
- **Dodavatel má zpracovanou politiku řešení incidentů a nenadálých událostí.**
- Dodavatel poskytuje součinnost při pravidelném monitoringu, který je u něj prováděn.
- Dodavatel jako zaměstnavatel při provádění prací při plnění předmětu plnění odpovídá za dodržování předpisů BOZP a PO svými zaměstnanci.

Nastavení metodiky výběru dodavatele

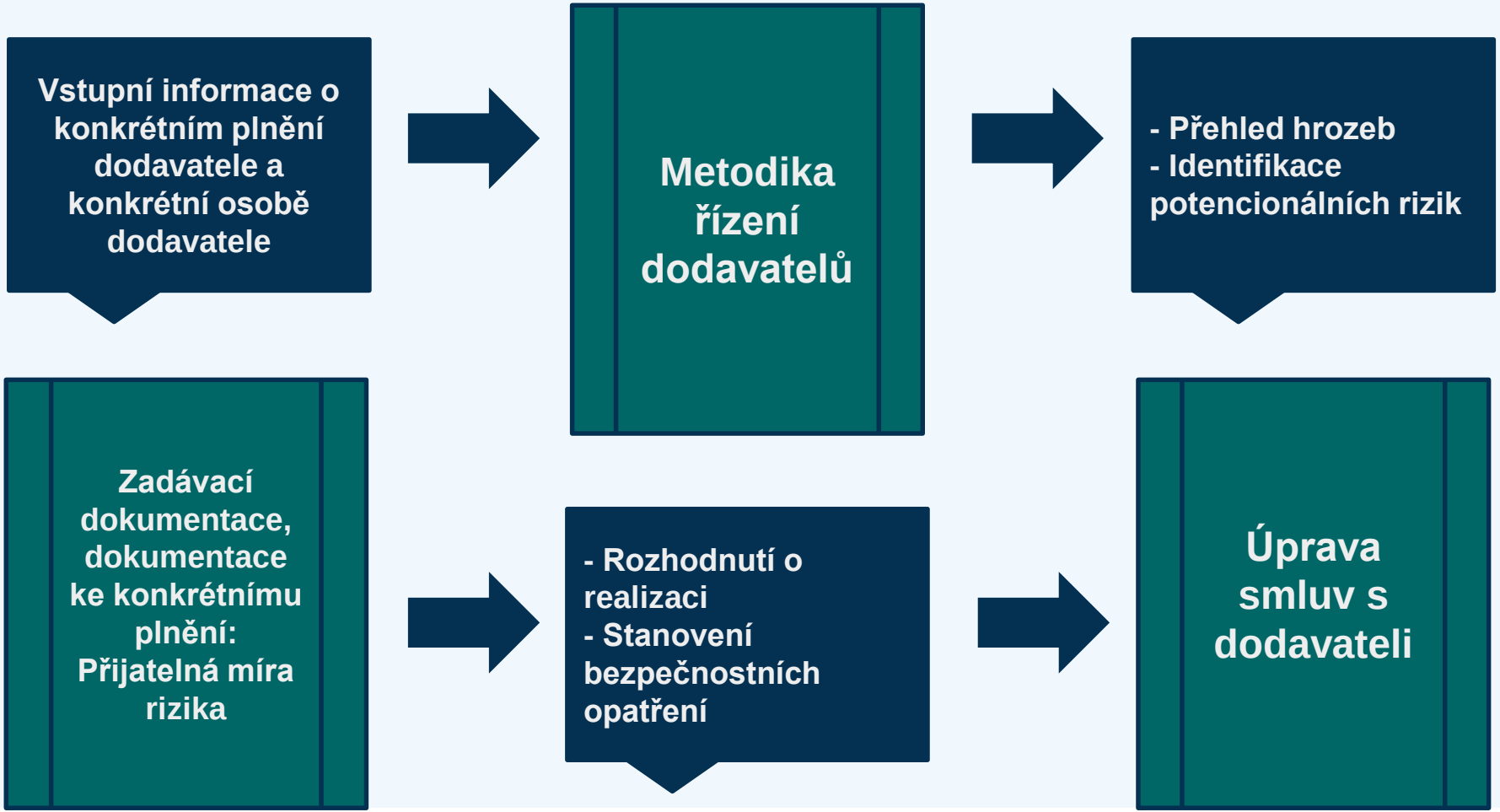
Krok číslo 2

- V rámci řízení dodavatelů se **před uzavřením smlouvy s třetí stranou** analyzují rizika dodavatelských služeb, akvizice, vývoje nebo údržby informačních systémů.
- Vychází se z **Bezpečnostní politiky, postupuje se dle Metodiky**
- **Metodika obsahuje:**

a) Pravidla a principy pro výběr dodavatele
b) Pravidla pro hodnocení rizik souvisejících s dodavateli
c) Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti
d) Pravidla pro provádění kontroly zavedení bezpečnostních opatření
e) Pravidla pro hodnocení dodavatelů

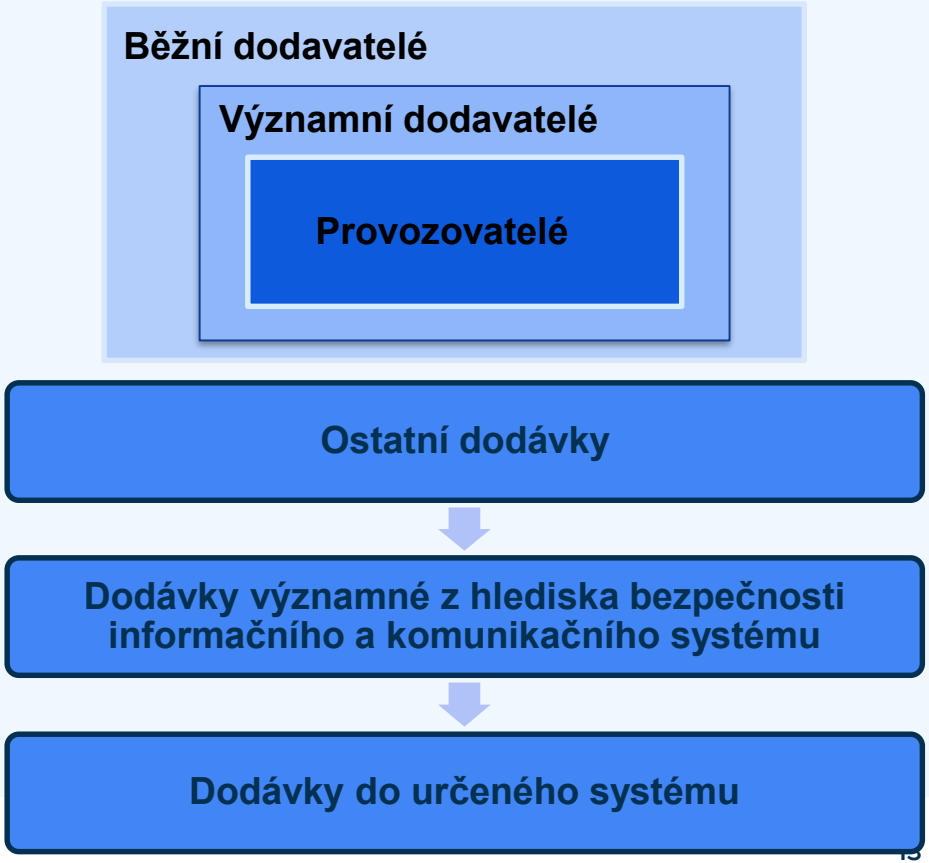
Veřejné zakázky

- Podmínky hodnocení rizik jsou zveřejněny v rámci **zadávací dokumentace** včetně základních kritérií přijatelnosti (rizikového skóre, po jehož překročení **není uzavření smlouvy s uchazečem pro Organizaci přijatelné**).


Vstupní informace o konkrétním plnění dodavatele a konkrétní osobě dodavatele
Metodika řízení dodavatelů
- Přehled hrozeb
- Identifikace potencionálních rizik
Zadávací dokumentace, dokumentace ke konkrétnímu plnění: Přijatelná míra rizika
- Rozhodnutí o realizaci
- Stanovení bezpečnostních opatření
Úprava smluv s dodavateli

Pravidla a principy pro výběr dodavatele

- Hodnocení rizik provádíme s ohledem na konkrétní předmět plnění smlouvy a **konkrétní osobu dodavatele (charakter systému. Dodavatele a plnění)**
- Identifikujeme aktiva, hrozby, konkrétní rizika a zranitelnosti.
- Následně provádíme hodnocení rizik a určujeme relevantní bezpečnostní opatření (řízení rizik)
- **Zvolená bezpečnostní opatření zohledňujeme ve smlouvě**



Seznam hrozeb + úroveň hrozby

Hrozba	Dopady do KII/VIS	Závažnost
Přístup k síti neoprávněnými osobami	Ohrožení důvěrnosti Ohrožení integrity	3
Porušení smluvních podmínek	Ohrožení dostupnosti	1
Kompromitace důvěrných informací	Ohrožení důvěrnosti	2
Způsobení škody třetí stranou	Ohrožení dostupnosti Ohrožení integrity	3
Poškození způsobená penetračními testy	Ohrožení dostupnosti Ohrožení integrity	3

Úroveň		Popis hrozby
1	Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
2	Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
3	Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
4	Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Stanovení rizikového skóre

- Přehled hrozeb zohledněných v rámci hodnocení rizik souvisejících s plněním předmětu výběrového řízení
- Pro vyhodnocení přijatelnosti míry rizika spojeného s plněním předmětu výběrového řízení bude jako vodítko použita následující škála:

Celkové rizikové skóre	Míra přijatelnosti rizika
0,00 .. 2,00	Přijatelné riziko, uzavření smlouvy s dodavatelem se doporučuje
2,01 .. 3,00	Zvýšené riziko, uzavření smlouvy s dodavatelem se doporučuje za předpokladu přijetí opatření směřujících ke snížení identifikovaných rizik
3,00 .. 3,50	Vysoké riziko, uzavření smlouvy s dodavatelem se výrazně nedoporučuje
3,51 .. 4,00	Nepřiměřeně vysoké riziko, uzavření smlouvy s dodavatelem není přípustné

Skutečnosti posuzované při hodnocení rizik

- Posuzujeme rizika související s **předmětem plněním**, ale i rizika spojená s **dodavatelem poptávaného řízení**
- Rozsah informací, ke kterým bude umožněn přístup
- Kritičnost aktiv, ke kterým bude umožněn přístup
- Typ přístupu: fyzický/logický
- Realizovaná bezpečnostní opatření
- Výběr osob, co se bude podílet na plnění závazků
- Jak máme řešeny postupy v případě bezpečnostních incidentů
- Zákonná, smluvní a další ujednání, co ovlivňují nebo mohou ovlivnit vztah s dodavatelem
- Bezpečnostní opatření vydaná úřadem: reaktivní nebo ochranná opatření, varování…

Politická rizika spojená s osobou dodavatele

Bezpečnostné opatrenia sa prijímajú a realizujú na základe analýzy rizík kybernetickej bezpečnosti, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti. Súčasťou analýzy rizík je aj analýza politického rizika tretej strany, pričom politické riziko sa posudzuje najmä vzhľadom na

- a) **plnenie záväzkov z medzinárodných zmlúv**, ktorými je Slovenská republika viazaná, a na jej členstvo v medzinárodných organizáciách,
- b) možnosť ovplyvňovania a zasahovania do činnosti tretej strany štátom, ktorý nie je členským štátom Európskej únie a Organizácie Severoatlantickej zmluvy (ďalej len „cudzí štát"),
- c) analýzu vlastníckej štruktúry a riadiacej štruktúry tretej strany vrátane vlastníckeho podielu cudzieho štátu a priamych zahraničných investícií do tretej strany,
- d) analýzu právnych predpisov a medzinárodných záväzkov cudzieho štátu v oblasti ochrany základných ľudských práv a slobôd, kybernetickej bezpečnosti, boja proti počítačovej kriminalite, ochrany osobných údajov a ochrany informácií,
- e) informácie špecifické pre cudzí štát a informácie spravodajskej služby o možných hrozbách pre záujmy Slovenskej republiky.

Posuzování dodavatele

- Historie a pověst dodavatele, kvalita technologie, výsledky auditů…
- Možnost bodování dodavatele dle dostupných informací
- Následné zařazení dodavatele do dané kategorie
- Zohlednění doporučení a metodik (např. Doporučení o důvěryhodnosti dodavatele)

Počet bodů	Kategorie	Bezpečnostní opatření
5-10	A	Standardní bezpečnostní pravidla
1-5	B	Vyšší míra bezpečnostních pravidel
-5-0	C	Potřeba nadstandardních bezpečnostních pravidel, zejména ve smyslu…
-10-5	D	Vysoce rizikový dodavatel, není doporučena spolupráce

Vyhodnocení rizik – určení bezpečnostních opatření

- Rizika identifikovaná v rámci úvodního hodnocení rizik souvisejících s plněním předmětu výběrového řízení jsou zavedena do celkového systému řízení rizik kybernetické bezpečnosti
- Na základě míry rizika identifikujeme konkrétní bezpečnostní opatření, která je nutná přijmout, abychom míru rizika snížili na přijatelnou úroveň
- Implementujeme konkrétní bezpečnostní opatření, např. zavedením do smluv s dodavateli

Povinné oblasti upravené bezpečnostními opatřeními ve smlouvě s třetími stranami (dodavateli)

- Oblast technických zranitelností systémů a zařízení
- Oblast řešení kybernetických a bezpečnostních incidentů,
- Oblast řízení bezpečnosti sítí a informačních systémů
- Oblast monitorování, testování bezpečnosti a bezpečnostních auditů
- Oblast řízení přístupů

Náležitosti smluv s třetími stranami (dodavateli) I.

- období trvání smlouvy;
- konkrétní rozsah činnosti třetí strany;
- ustanovení o povinnosti třetí strany chránit všechny jí poskytnuté informace;
- ustanovení o povinnosti třetí strany dodržovat bezpečnostní politiku provozovatele;
- ustanovení o povinnosti třetí strany dodržovat a přijímat bezpečnostní opatření (vč. jejich konkrétní specifikace, rozsahu a vyjádření souhlasu s těmito opatřeními ze strany provozovatele);
- ustanovení o povinnosti třetí strany informovat provozovatele o bezpečnostních incidentech a všech skutečnostech, které mají vliv na zabezpečení kybernetické bezpečnosti;
- seznam pracovních rolí třetí strany, které mají přístup k informacím a údajům provozovatele, vč. ustanovení povinnosti oznámit provozovateli každou změnu v personálním obsazení;

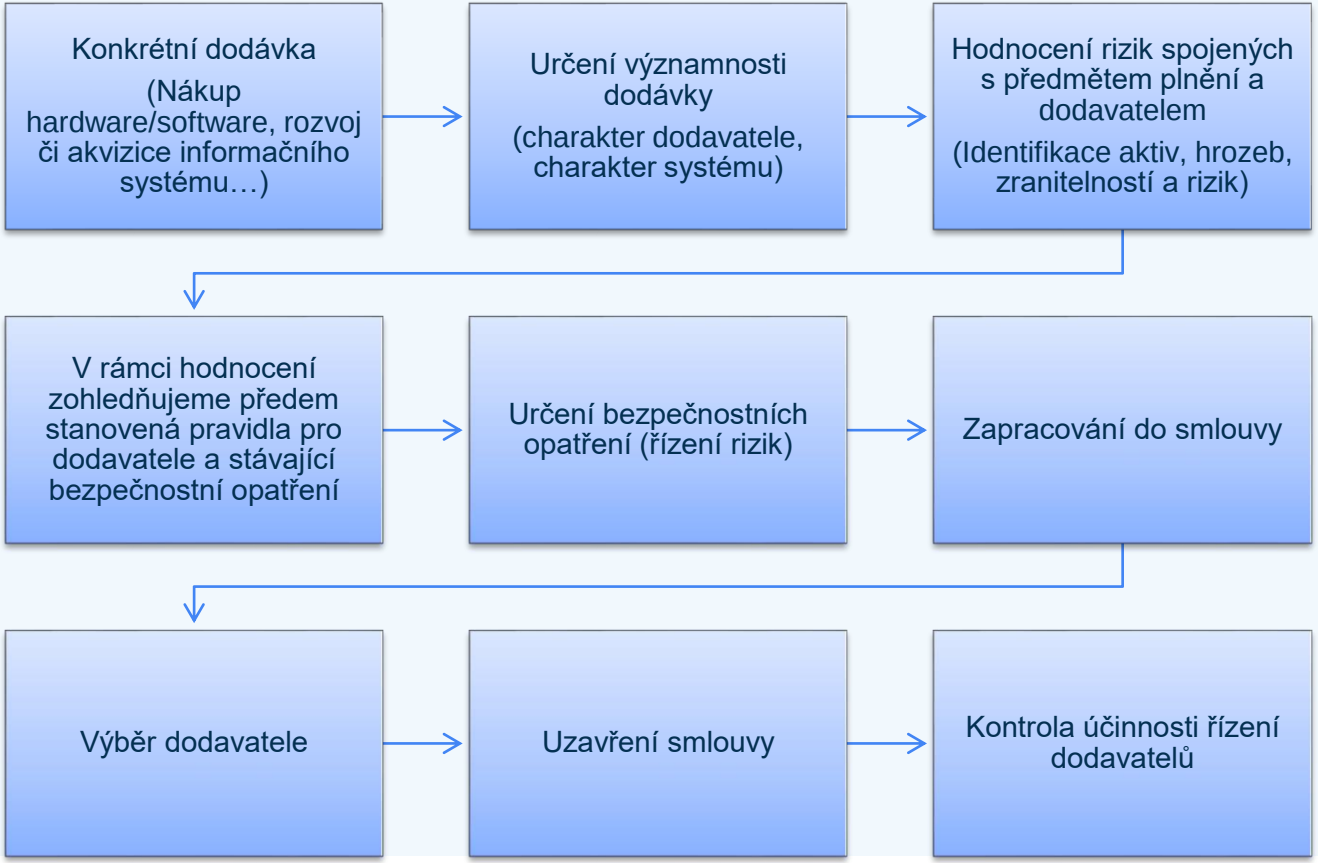
Náležitosti smluv s třetími stranami (dodavateli) II.

- ustanovení o rozsahu, způsobu a možnosti vykonávání kontrolních činností a auditu provozovatelem u třetí strany;
- vymezení podmínek a možnosti zapojení dalšího dodavatele;
- ustanovení o způsobu a formě hlášení dalších informací požadovaných provozovatelem na plnění jeho povinností vyplývajících ze zákona a jejich vymezení a všech informací majících vliv na smlouvu;
- ustanovení o sankčních mechanismech při porušení smlouvy;
- ustanovení o podmínkách a způsobu ukončení smlouvy;
- závazek třetí strany po ukončení smlouvy vrátit, převést, příp. zničit všechny informace, ke kterým měla přístup;
- závazek třetí strany po ukončení smlouvy udělit, poskytnout, převést nebo postoupit všechny potřebné licence, práva anebo souhlasy, které jsou nutné pro zabezpečení kontinuity.

Analýza politického rizika třetích stran (dodavatelů)

- schvaluje vláda Slovenské republiky na základě stanoviska Národního bezpečnostního úřadu (NBÚ)
- Stanovisko NBÚ se předkládá Radě bezpečnosti Slovenské republiky
- Politická rizika NBÚ zveřejňuje v jednotném informačním systému kybernetické bezpečnosti

- NBÚ v analýze politického rizika zohlední vyjádření Ministerstva zahraničních věcí a evropských záležitostí Slovenské republiky, Ministerstva hospodářství Slovenské republiky, Ministerstva vnitra Slovenské republiky, Slovenské informační služby a Ministerstva obrany Slovenské republiky z oblasti jejich působnosti


Konkrétní dodávka
(Nákup hardware/software, rozvoj či akvizice informačního systému…)
Určení významnosti dodávky
(charakter dodavatele, charakter systému)
Hodnocení rizik spojených s předmětem plnění a dodavatelem
(Identifikace aktiv, hrozeb, zranitelností a rizik)
V rámci hodnocení zohledňujeme předem stanovená pravidla pro dodavatele a stávající bezpečnostní opatření
Určení bezpečnostních opatření (řízení rizik)
Zapracování do smlouvy
Výběr dodavatele
Uzavření smlouvy
Kontrola účinnosti řízení dodavatelů

CHRENEK | TOMAN | KOTRBA

Chrenek, Toman, Kotrba advokátní kancelář spol. s r.o.
Těšnov 1/1059, Praha 1, PSČ 110 00,
Česká republika
IČO: 285 05 913
Tel.: (+420) 221 875 402-9
www.chrenektomankotrba.cz

POBOČKA Brno:
Smetanova 19, Brno, PSČ 602 00

POBOČKA Olomouc:
nábř. Přemyslovců 867/8, Olomouc, PSČ 779 00

POBOČKA Bratislava:
Palisády 56, Bratislava - mestská časť Staré Mesto, PSČ 811 06

Zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 146526

CHRENEK | TOMAN | KOTRBA

Děkuji za pozornost

Kontaktní osoba:

Mgr. Šimon Toman

E-mail: s.toman@chtk.cz
Tel.: (+420) 721 521 540