Kybernetické bezpečnost a veřejné zakázky

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Jan Hénik
Odbor regulace

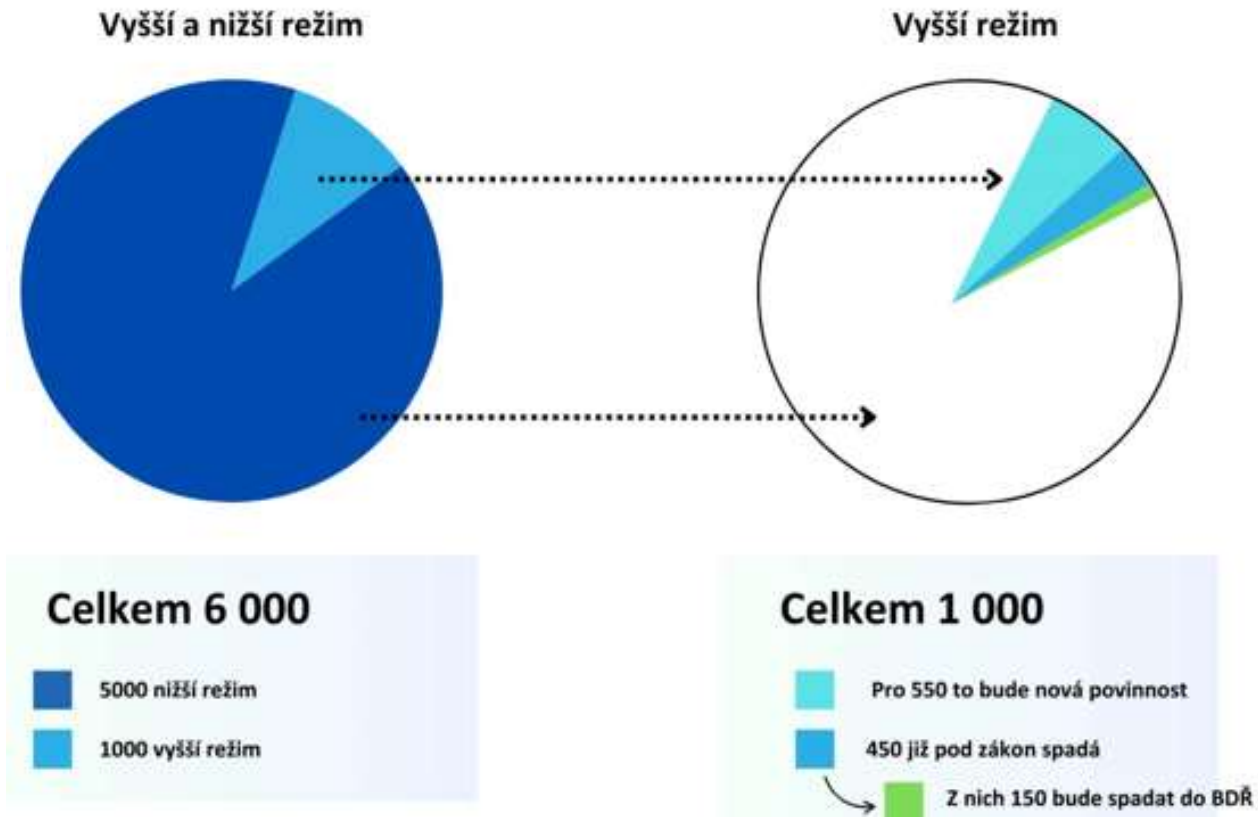
ISSS 2026
18. května 2026, Hradec Králové

Co požadovat a proč?

Zákon o kybernetické bezpečnosti

- **Veřejná správa**
- Energetika – Elektřina
- Energetika – Ropa a ropné produkty
- Energetika – Zemní plyn
- Energetika – Teplárenství
- Energetika – Vodík
- Výrobní průmysl
- Potravinářský průmysl
- Chemický průmysl
- Vodní hospodářství
- Odpadové hospodářství
- Letecká doprava
- Drážní doprava
- Vodní doprava
- Silniční doprava
- Digitální infrastruktura a služby
- Finanční trh
- Zdravotnictví
- Věda, výzkum a vzdělávání
- Poštovní a kurýrní služby
- Obranný průmysl
- Vesmírný průmysl

Kategorie podniku	Počet zaměst-nanců: roční pracovní jednotka (RPJ)	Roční obrat	nebo	Bilanční suma roční rozvahy
Střední podnik	< 250	≤ 50 milionů EUR	nebo	≤ 43 milionů EUR
Malý podnik	< 50	≤ 10 milionů EUR	nebo	≤ 10 milionů EUR
Mikropodnik	< 10	≤ 2 miliony EUR	nebo	≤ 2 miliony EUR



Bezpečnostní opatření = proč to celé existuje

Základní důvod existence zákona.

Podstatou je:

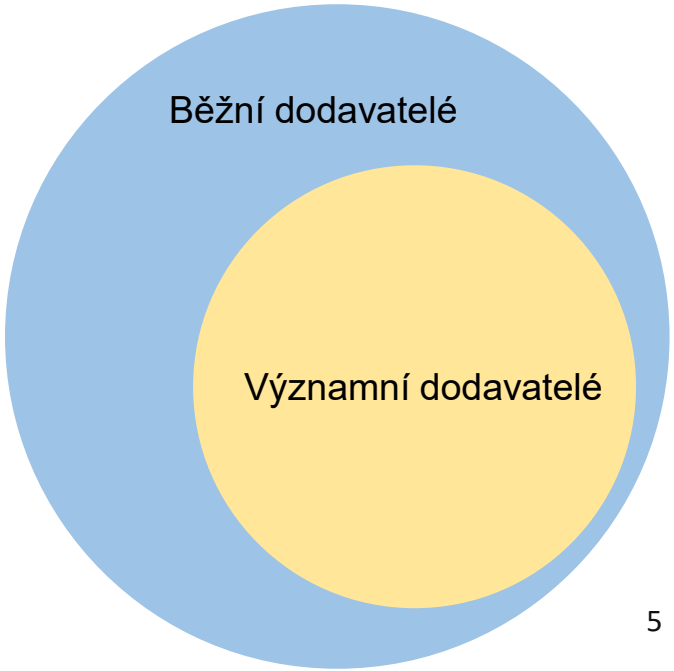
- **zvolit a zavést v organizaci takové procesy a kroky, které pomohou zodolnit organizaci tak, že její služba bude i zítra fungovat tak, jako fungovala včera**

Řízení dodavatelů

Stěžejní povinnosti:

- Stanovení pravidel pro dodavatele
- Vedení evidence významných dodavatelů
- Řízení rizik spojených s dodavateli
- Minimální obsah smluv (příloha + stanovení úrovně a způsobů realizace bezpečnostních opatření)
- Pravidelné přezkoumávání smluv s významnými dodavateli
- Hodnocení rizik spojených s významnými dodavateli

Významný dodavatel:
= ten, kdo poskytovateli regulované služby poskytuje plnění, které je významné z hlediska kybernetické bezpečnosti



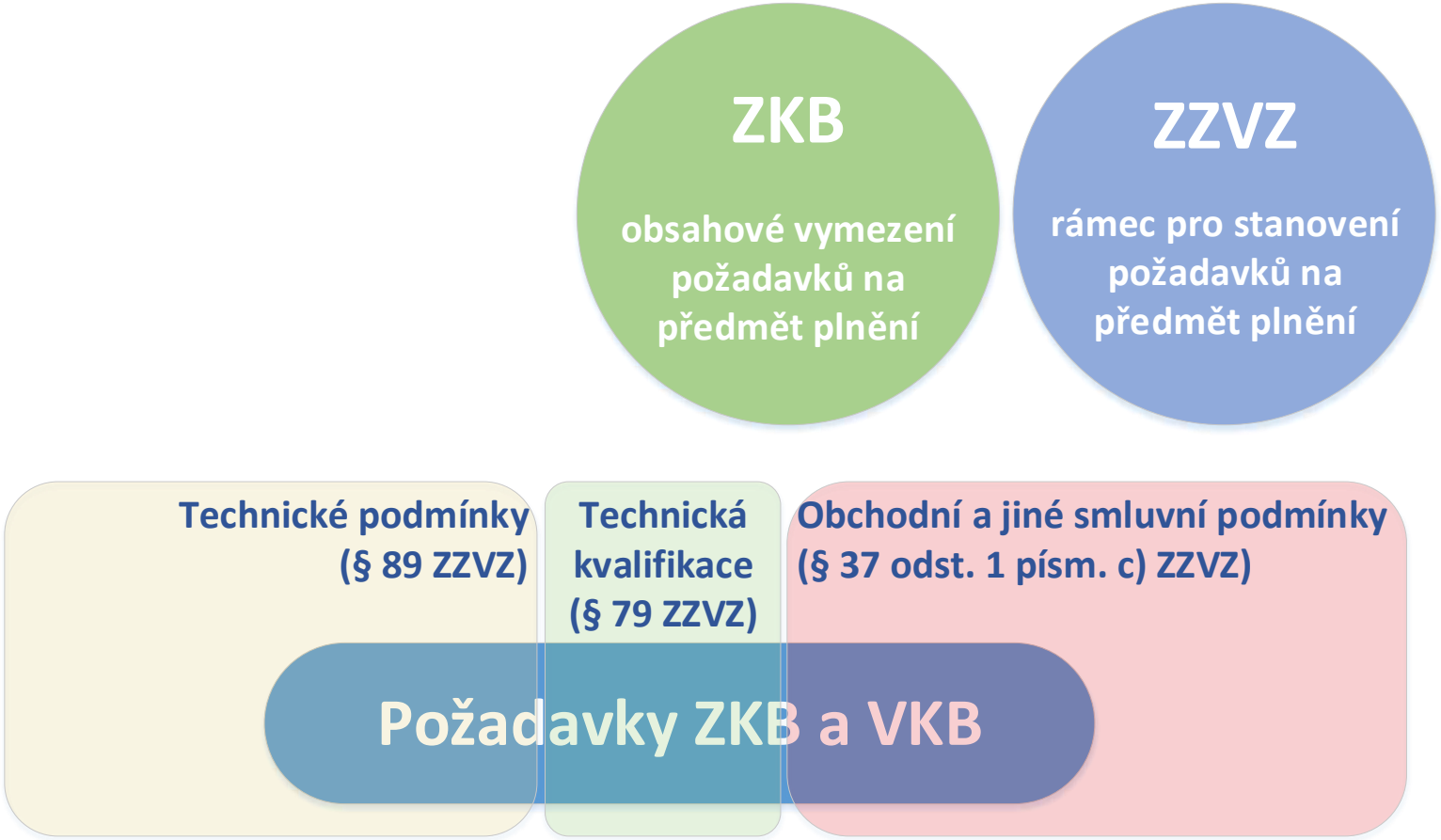
Proč nás dodavatelé bolí

- mají přístupy
- mají data
- provozují systémy
- incident u dodavatele = váš problém

Nejde jen o cenu

Jak pracovat s požadavky na KB ve VZ?

Jak spolu mluví ZKB a ZZVZ



Přípustné omezení hospodářské soutěže

Starý ZKB

- *„**zohlednění požadavků** vyplývajících z bezpečnostní politiky, bezpečnostních pravidel, bezpečnostních opatření a dalších podmínek sjednaných ve smlouvě podle odstavce 5, **které jsou nezbytné pro splnění povinností podle tohoto zákona, nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži**“*

ZKB

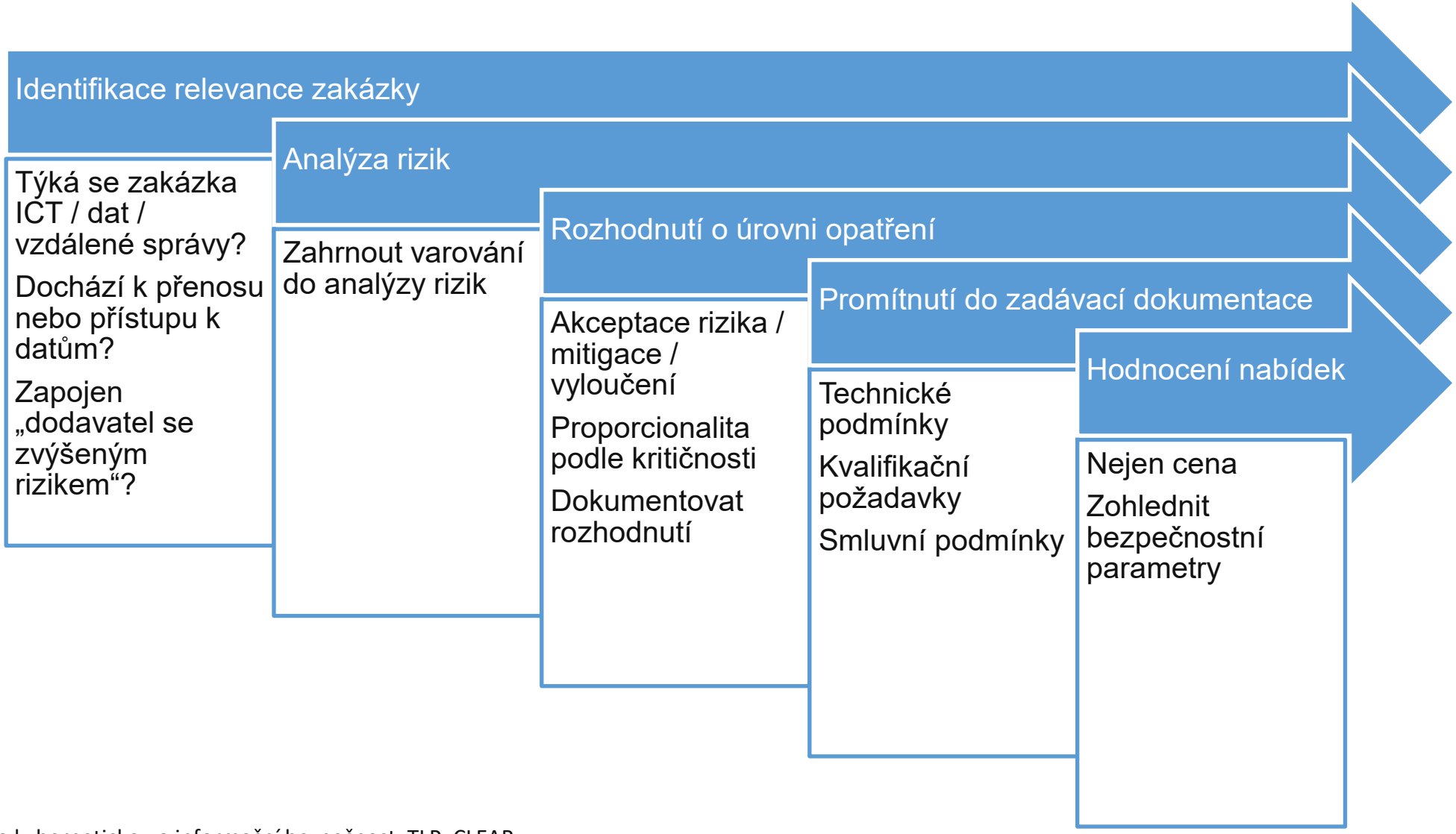
- Obdobné ustanovení chybí, protože bylo nadbytečné
- Uvedené umožňuje už § 36 odst. 1 ZZVZ
- Kybernetická bezpečnost je legitimní potřebou zadavatele a tudíž se nejedná o bezdůvodnou překážku hospodářské soutěže

Přípustné omezení hospodářské soutěže

6 As 338/2021: *„…Rovněž argumentace zákonem o kybernetické bezpečnosti nemůže bez dalšího odůvodnit výlučný požadavek na potvrzení výrobce. … Uvedený zákon nedává zadavatelům „bianco šek“ na nedodržování ZZVZ…**překážku hospodářské soutěže podle tohoto zákona nepředstavují pouze bezpečnostní opatření činěná v míře nezbytné**. Tuto nezbytnou míru však osoba zúčastněná na řízení jako zadavatel ve správním řízení přezkoumatelně neobjasnila ani nedoložila.“*

ZKB nedává zadavatelům bianco šek

Doporučení NÚKIB pro řízení dodavatelů



Vyloučení/omezení rizikových dodavatelů

Využití kvalifikačních předpokladů

- Zkušenosti, certifikace, organizační opatření
- Striktně regulované, musí souviset s předmětem zakázky

Vyloučení účastníka zadávacího řízení pro nezpůsobilost

- Relevantní důvody (bezpečnostní riziko, profesní pochybení)
- Opřené o zákonné důvody a řádně zdůvodněné

Vyloučení/omezení rizikových technologií

Správné vymezení požadavků v rámci stanovení technických podmínek

- Bezpečnostní požadavky lze nastavit jako **technické podmínky plnění** (např. zákaz konkrétních technologií), pokud jsou **odůvodněné a nediskriminační**
- Musí být formulovány **jednoznačně a přiměřeně**

Bezpečnost jako kritérium kvality stanovené zadavatelem pro hodnocení nabídek

- Bezpečnost lze zahrnout do kritérií hodnocení (kvality), nikoli jen jako tvrdý požadavek
- Umožňuje to **preferovat bezpečnější řešení**, aniž by byli ostatní dodavatelé automaticky vyloučeni

Co musí zadavatel umět obhájit

- Jaké riziko řeším?
- Proč nestačí mírnější opatření?
- Proč je omezení přiměřené?
- Jak to doložím při kontrole?

Bez dokumentace není obhajitelnost

Co potvrzuje rozhodovací praxe ÚOHS

- Bezpečnostní požadavky mohou omezit hospodářskou soutěž
  → pokud jsou přiměřené a odůvodněné
- Klíčová je analýza rizik
  → zadavatel musí své požadavky doložit
- Samotný odkaz na kyberbezpečnost nestačí
  → požadavky musí být přezkoumatelné a dokumentované

S0262/2019, S0358/2019, S0196/2022

Varování NÚKIB ve VZ

Co je to varování?

- NÚKIB jej vydává v případě **existence hrozby v oblasti kybernetické bezpečnosti**
- **závazné pro regulované subjekty**, neregulované subjekty mohou varování zohlednit dobrovolně
  - Poskytovatel regulované služby ve **vyšším režimu** povinností se musí hrozbou zabývat ve své **analýze rizik**
  - Poskytovatel regulované služby v **nižším režimu** povinností by měl varování **zohlednit přiměřeně**
- **nejedná se o automatický zákaz,** ale povinnost pracovat s hrozbou

Jak postupovat po vydání varování?

Před zahájením VZ

Úprava zadávacích podmínek
→ možnost omezení/vyloučení

Během zadávacího řízení

Změna zadávací dokumentace
→ prodloužení lhůt

Po podání nabídek

Možné zrušení zadávacího řízení

Po uzavření smlouvy

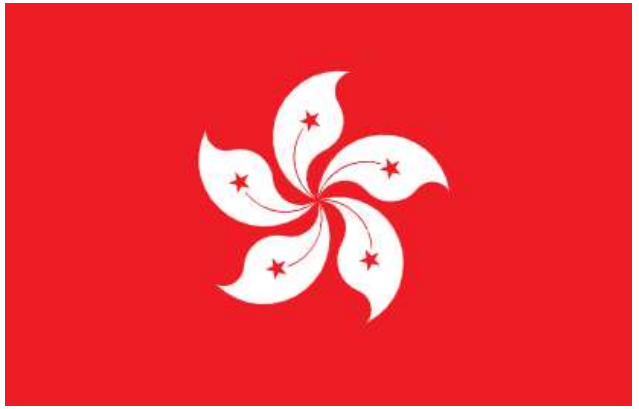
Mitigace/výměna/změna smlouvy

Konkrétní postup závisí na fázi zadávacího řízení
(vždy na základě výsledků analýzy rizik)

Vybraná varování NÚKIB

Varování proti předávání dat a vzdálené správě z ČLR

- Varování se týká:
  - **předávání systémových a uživatelských dat do Čínské lidové republiky**,
  - **vzdálené správy technických aktiv vykonávané z území Čínské lidové republiky.**
- Úřad hrozbu hodnotí na úrovni **Vysoká** – Hrozba je **pravděpodobná až velmi pravděpodobná**.



Příklady technologií, které varování zahrnuje

Telefony, notebooky, tablety

Připojená vozidla

Zdravotnické přístroje

Solární střídače

Smartmetery

deepseek

Software

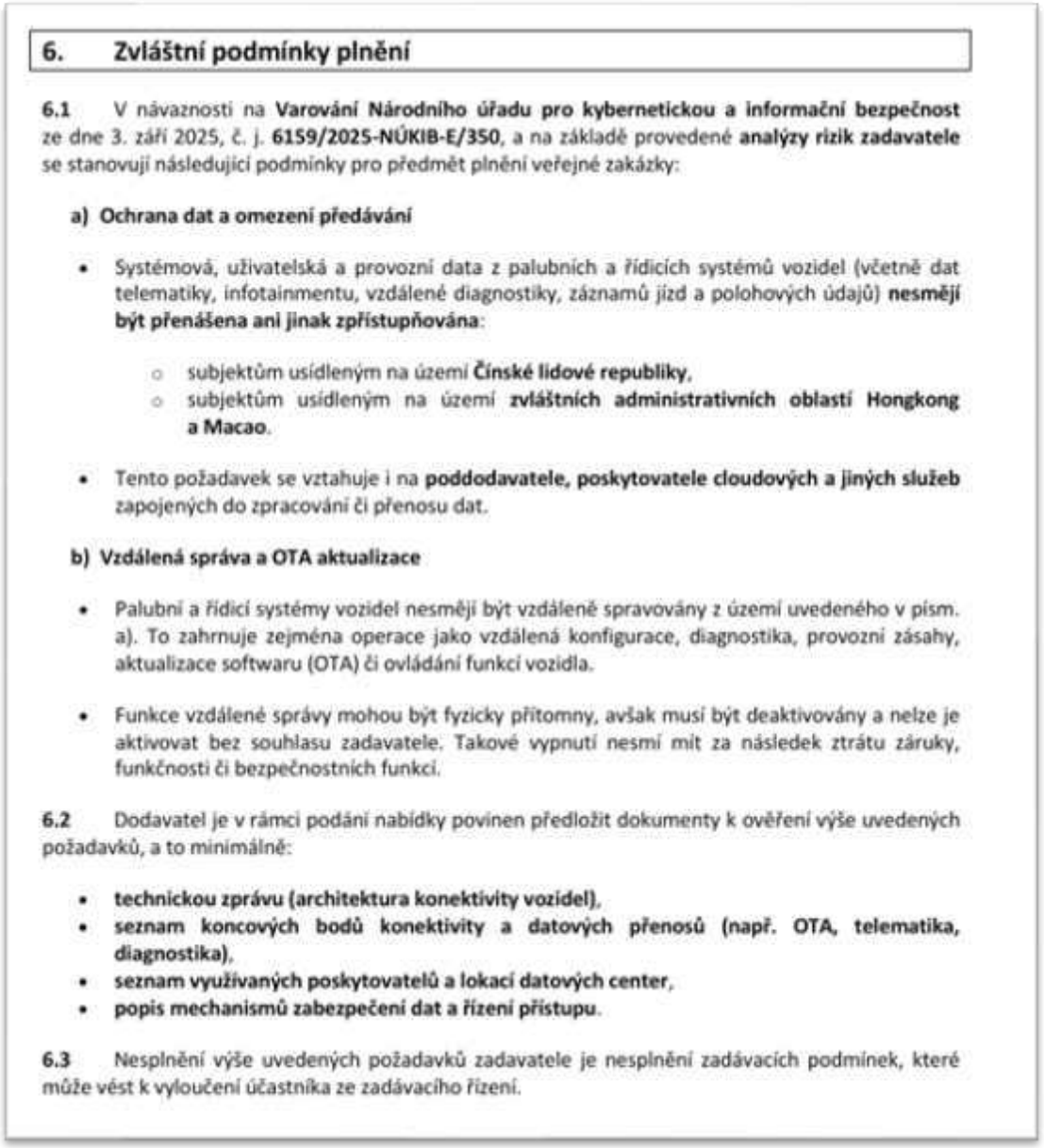
IP kamery

Drony

Případová studie NÚKIB: Operativní leasing služebních osobních vozidel

- Posouzení relevance varování pro předmět plnění
- Provedena analýza rizik podle interních metodik NÚKIB
- Promítnutí výsledků do zadávacích podmínek
- Analýza rizik jako podklad pro odůvodnění zadávacích podmínek
- **Analýza rizik je neveřejná, ale je archivována** pro účely kontroly a přezkumu

S0262/2019 *„kompletní analýza rizik nemusí být součástí zadávací dokumentace“*



6. Zvláštní podmínky plnění

6.1 V návaznosti na **Varování Národního úřadu pro kybernetickou a informační bezpečnost** ze dne 3. září 2025, č. j. **6159/2025-NÚKIB-E/350**, a na základě provedené **analýzy rizik zadavatele** se stanovují následující podmínky pro předmět plnění veřejné zakázky:

a) Ochrana dat a omezení předávání

- Systémová, uživatelská a provozní data z palubních a řídicích systémů vozidel (včetně dat telematiky, infotainmentu, vzdálené diagnostiky, záznamů jízd a polohových údajů) **nesmějí být přenášena ani jinak zpřístupňována**:
  - subjektům usídleným na území **Čínské lidové republiky**,
  - subjektům usídleným na území **zvláštních administrativních oblastí Hongkong a Macao**.
- Tento požadavek se vztahuje i na **poddodavatele, poskytovatele cloudových a jiných služeb** zapojených do zpracování či přenosu dat.

b) Vzdálená správa a OTA aktualizace

- Palubní a řídicí systémy vozidel nesmějí být vzdáleně spravovány z území uvedeného v písm. a). To zahrnuje zejména operace jako vzdálená konfigurace, diagnostika, provozní zásahy, aktualizace softwaru (OTA) či ovládání funkcí vozidla.
- Funkce vzdálené správy mohou být fyzicky přítomny, avšak musí být deaktivovány a nelze je aktivovat bez souhlasu zadavatele. Takové vypnutí nesmí mít za následek ztrátu záruky, funkčnosti či bezpečnostních funkcí.

6.2 Dodavatel je v rámci podání nabídky povinen předložit dokumenty k ověření výše uvedených požadavků, a to minimálně:

- **technickou zprávu (architektura konektivity vozidel)**,
- **seznam koncových bodů konektivity a datových přenosů (např. OTA, telematika, diagnostika)**,
- **seznam využívaných poskytovatelů a lokací datových center**,
- **popis mechanismů zabezpečení dat a řízení přístupu**.

6.3 Nesplnění výše uvedených požadavků zadavatele je nesplnění zadávacích podmínek, které může vést k vyloučení účastníka ze zadávacího řízení.

Co se chystá?

Metodika zadávání VZ v oblasti ICT a KB

Metodika by měla zadavatelům pomoct:

- převést analýzu rizik do konkrétních zadávacích podmínek
- promítnout varování a protiopatření NÚKIB do veřejných zakázek
- nastavit bezpečnostní požadavky přiměřeně a obhajitelně
- sladit požadavky kybernetické bezpečnosti se zásadami hospodářské soutěže
- pracovat s dodavatelským řetězcem

Metodika vznikla ve spolupráci NÚKIB, ÚOHS a AVZ.

Mgr. Jan Hénik

NÚKIB
Email: jan.henik@nukib.gov.cz
Telefon: +420 720 026 645