



Národní úřad
pro kybernetickou
a informační bezpečnost

Dodavatel v zákoně o kybernetické bezpečnosti

Martin Švéda



Povinnosti poskytovatele regulované služby

Podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti

- Cílem je zajistit bezpečný provoz regulované služby a minimalizovat dopady kybernetických incidentů.
- K zajištění cíle je zejména potřeba zavádět bezpečnostní opatření a hlásit kybernetické bezpečnostní incidenty.
- **Významnou součástí zajištění kybernetické bezpečnosti je zavádění bezpečnostních opatření nejen u mě, ale i u mých dodavatelů.**



Tři různé dodavatele podle ZKB

Různé způsoby nahlížení na dodavatele podle zákona

Dodavatel

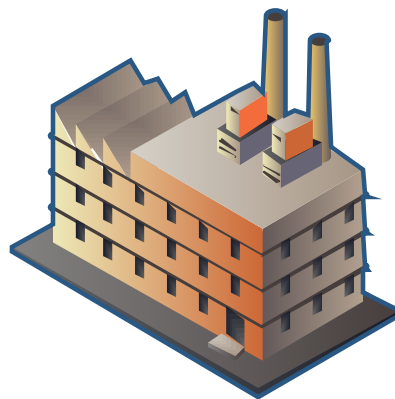
- každý jakýkoliv dodavatel
- vyšší i nižší režim
- minimální interakce

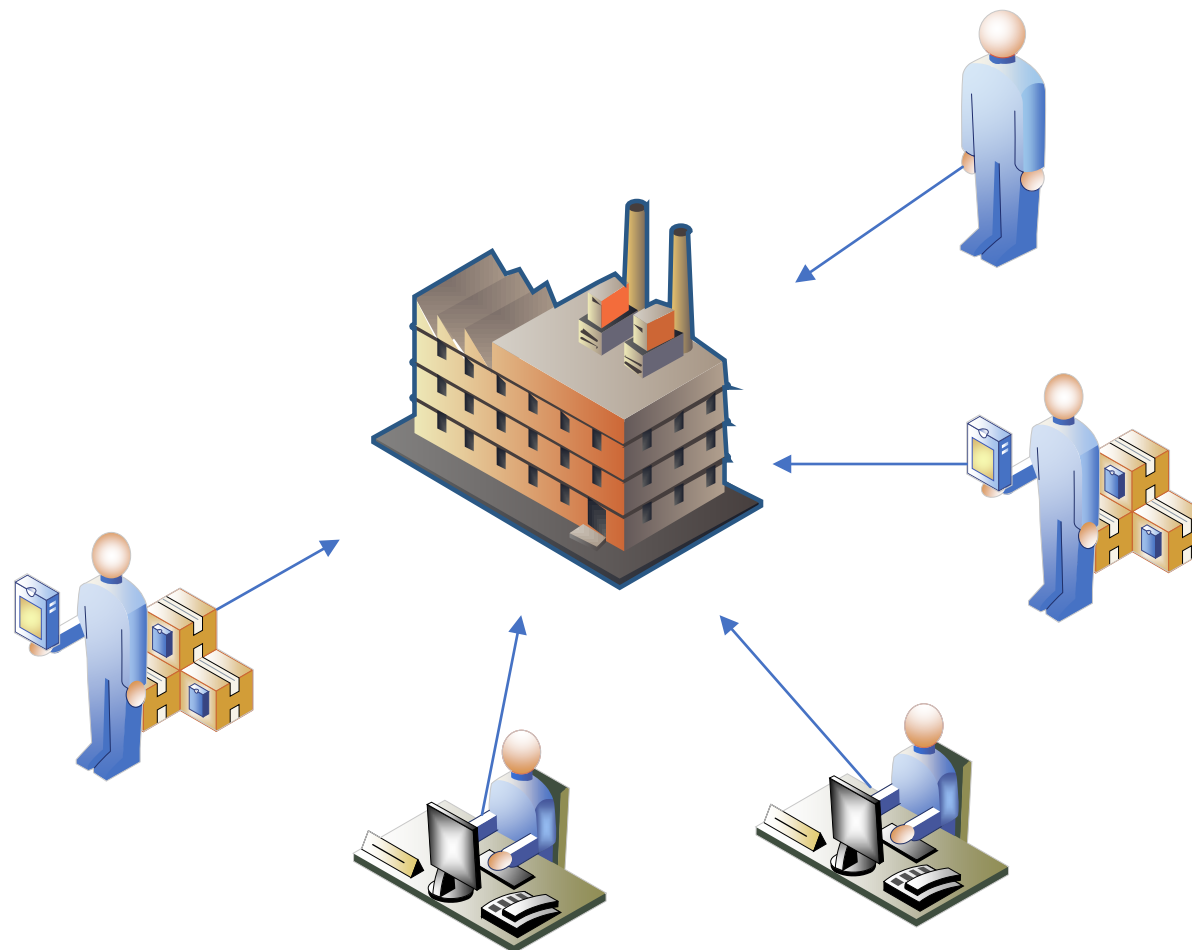
Významný dodavatel

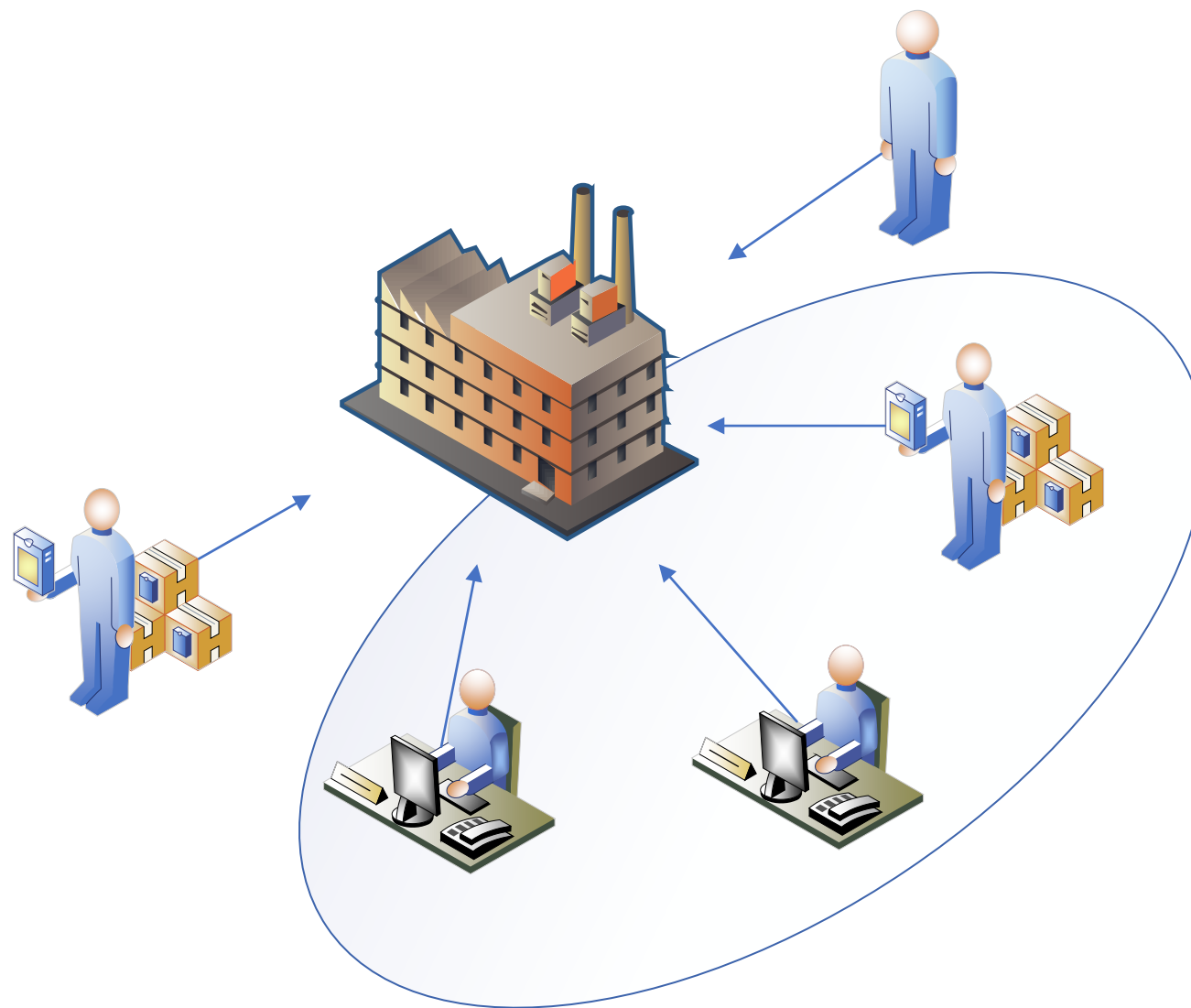
- „kvalifikovaný“ dodavatel
- jen vyšší režim
- *„Ten (každý), kdo povinné osobě poskytuje plnění, které je významné z hlediska zajištění kybernetické bezpečnosti regulované služby“*
(§ 2 písm. h) vyhlášky BO-VR)
- určité požadavky

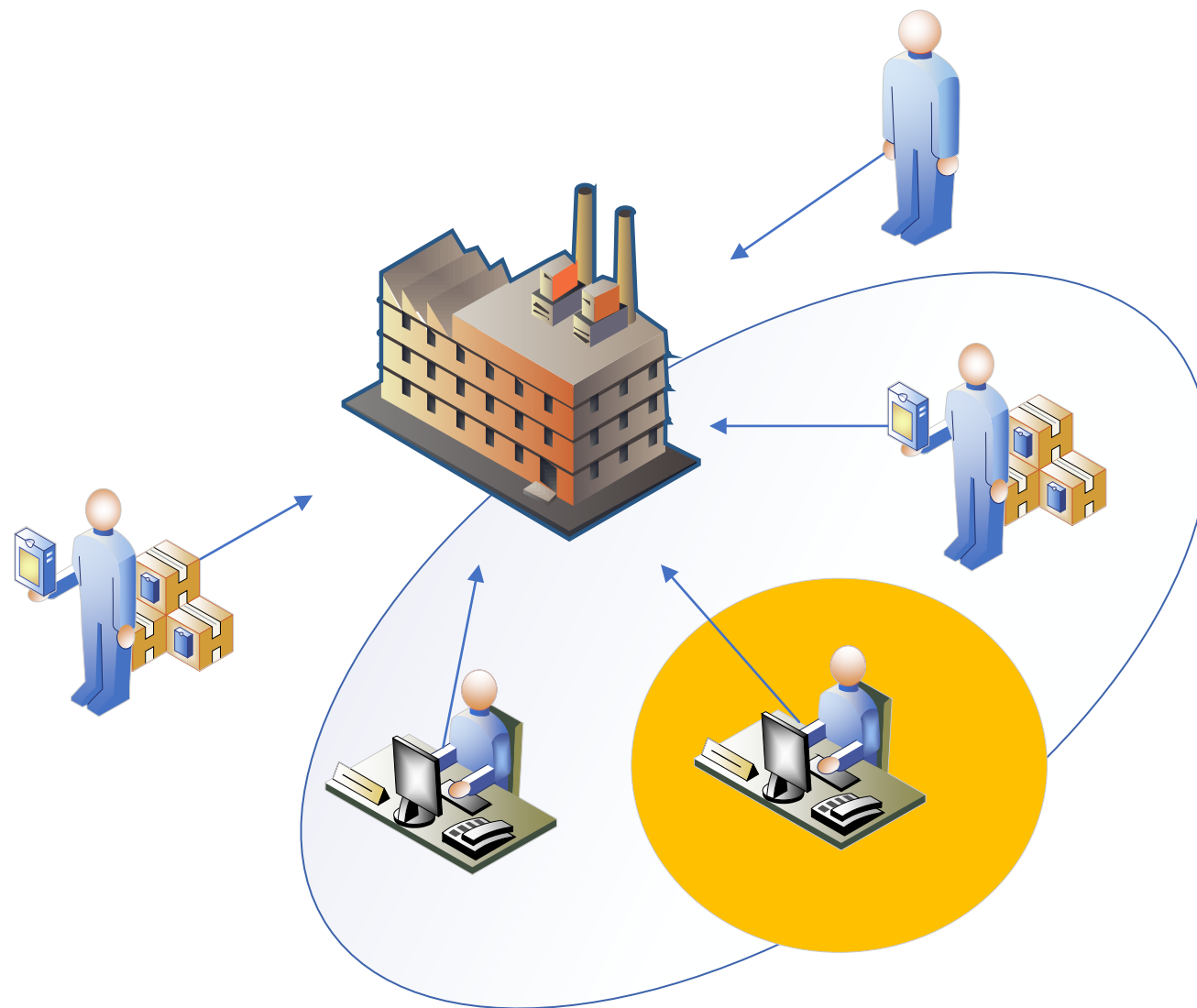
Poskytovatel řízené (bezpečnostní) služby

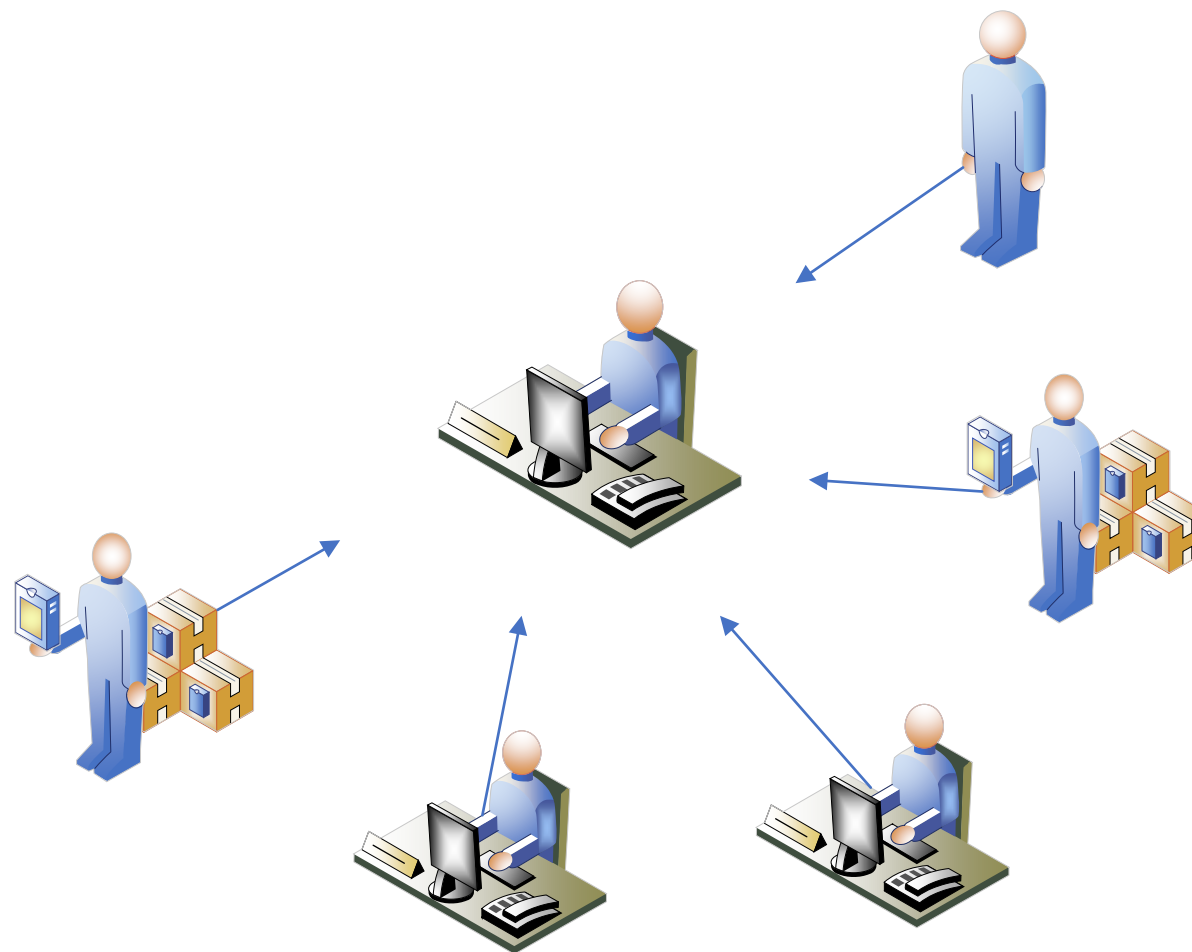
- dodavatel splňující samostatně kritéria pro určení jako povinná osoba
- plné požadavky povinné osoby (a své vlastní řízení dodavatelů)













Vyšší režim povinností

Poskytovatel regulované služby je povinen v rámci stanoveného rozsahu zavádět a provádět bezpečnostní opatření v míře nezbytné pro zajištění kybernetické bezpečnosti regulované služby.

- Každý dodavatel je podpůrným aktivem (§ 2 odst. 1 písm. e) zákona).
- Významný dodavatel je ten, kdo povinné osobě poskytuje plnění, které je významné z hlediska zajištění kybernetické bezpečnosti regulované služby (§ 2 písm. h) vyhlášky)
- Dodavatele musíme vybírat v souladu s požadavky vyplývajícími z bezpečnostního opatření a **zahrnovat tyto požadavky do smluv** (§ 13 odst. 5 zákona).
- V rámci ISMS **zajistit mlčenlivost dodavatelů** (§ 4 odst. 1 písm. m vyhlášky).
- Řízení dodavatelů podle § 9 vyhlášky:
 - Dodavatele **seznamovat s pravidly** pro dodavatele v souladu s ISMS
 - Identifikovat, evidovat a informovat významné dodavatele
 - Relevantní ustanovení přílohy č. 5 do smluv s významnými dodavateli
 - V rámci veřejné zakázky a před uzavřením smlouvy u významných dodavatelů **hodnocení rizik**
 - Stanovit způsoby, úrovně realizace, odpovědnosti a kontrolu zavedení bezpečnostních opatření
- Smluvně zajistit **hlášení podezřelého chování aktiv u dodavatelů** (§ 14 vyhlášky).



Nižší režim povinností

Poskytovatel regulované služby je povinen v rámci stanoveného rozsahu zavádět a provádět bezpečnostní opatření v míře nezbytné pro zajištění kybernetické bezpečnosti regulované služby.

- **Každý dodavatel je podpůrným aktivem (§ 2 odst. 1 písm. e) zákona).**
- **Povinná osoba při uzavírání smlouvy s dodavatelem do stanoveného rozsahu zohlední hrozby a zranitelnosti spojené s tímto dodavatelem, celkovou kvalitu produktů a postupů v oblasti kybernetické bezpečnosti tohoto dodavatele, včetně postupů bezpečného vývoje a na základě toho zajistí, aby smlouvy s tímto dodavatelem obsahovaly relevantní požadavky na smluvní ujednání uvedené v příloze k této vyhlášce (§ 3 odst. 5 vyhlášky).**
- **Povinná osoba uzavírá pouze takové smlouvy, které stanoví způsoby realizace bezpečnostních opatření a určují obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.**



Relevantní smluvní ustanovení

- a) ustanovení o bezpečnosti informací z pohledu důvěrnosti (včetně ustanovení o mlčenlivosti), integrity a dostupnosti,
- b) ustanovení o oprávnění užívat data,
- c) ustanovení o autorství programového kódu, popřípadě o programových licencích,
- d) ustanovení o kontrole zavedených bezpečnostních opatření (pravidla zákaznického auditu),
- e) ustanovení upravující řetězení dodavatelů, **přičemž musí být zajištěno, že subdodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele,**
- f) ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele (nebo odsouhlasení pro dodavatelský vztah relevantních částí bezpečnostních politik) povinnou osobou,
- g) ustanovení o řízení změn,
- h) ustanovení o souladu smluv s obecně závaznými právními předpisy,**
- i) ustanovení o povinnosti dodavatele informovat povinnou osobu (...)**
- j) specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy, tzv. exit strategie (...),
- k) specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli,
- l) specifikace náležitosti smlouvy o úrovni služeb (SLA) a způsobu a úrovni realizace bezpečnostních opatření.
- m) ustanovení o dodržování pravidel bezpečného vývoje,
- n) specifikace podmínek pro formát předání dat a informací po vyžádání povinnou osobou,**
- o) pravidla pro likvidaci dat,**
- p) ustanovení o právu jednostranně odstoupit od smlouvy nebo smlouvu vypovědět bez výpovědní doby v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy,**
- q) ustanovení o sankcích za porušení povinností a
- r) ustanovení o zpřístupnění nebo předání dat na základě žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu**
 - 1. až po provedení přezkoumání zákonnosti žádosti,**
 - 2. až po vynaložení úsilí o zabránění zpřístupnění nebo předání dat v rámci možností daných právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána,**
 - 3. pouze v nezbytném rozsahu.**



Další relevantní ustanovení o dodavateli

Poskytovatel regulované služby je povinen v rámci stanoveného rozsahu zavádět a provádět bezpečnostní opatření v míře nezbytné pro zajištění kybernetické bezpečnosti regulované služby.

- Speciální úprava předání informací a dat od dodavatele (§ 24 zákona)
- Mechanismus prověřování bezpečnosti dodavatelského řetězce (§ 27 - § 32 zákona)



Národní úřad
pro kybernetickou
a informační bezpečnost

**Děkuji
za pozornost**

Martin Švéda

martin.sveda@nukib.gov.cz