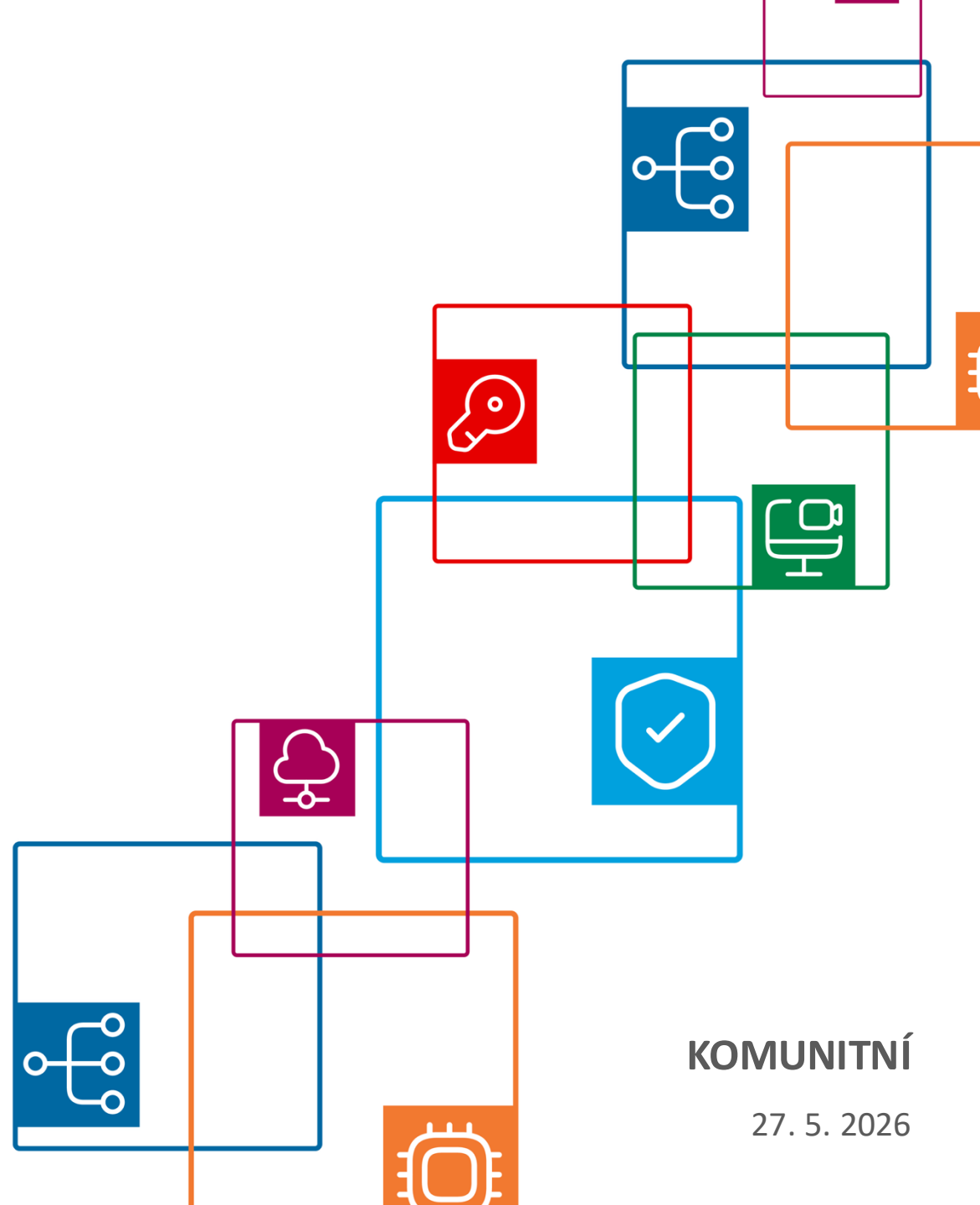




TaPnZKB: Aktiva

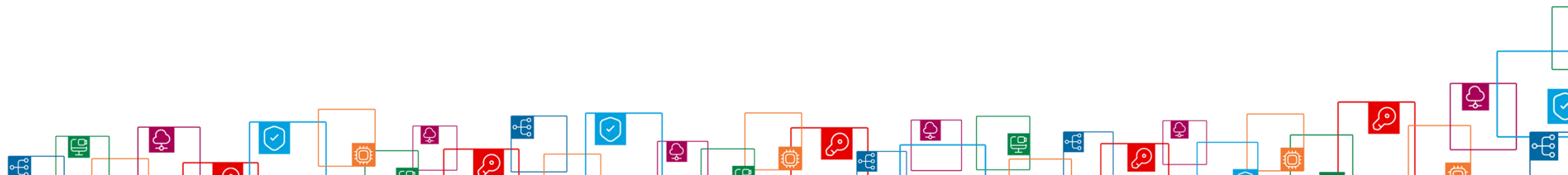
A. Kropáčová, J. Bořík, M. Pospíšilová



KOMUNITNÍ

27. 5. 2026

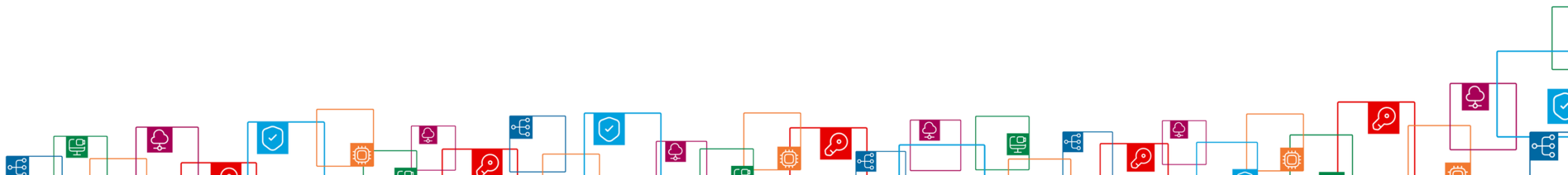
- ptejte se!
- pošlete na mkb@cesnet.cz, co je potřeba vysvětlit podrobněji či znovu a lépe (na dalších WS)



1. Máme splněné administrativní povinnosti dle nZKB	▪ na NUKIB jsme ohlásili regulované služby a další požadované údaje
2. Víme, co máme chránit	▪ máme evidenci aktiv ▪ máme dle potřeby zmapované vazby mezi aktivy (primární – podpůrná, aktiva – podaktiva, ...) ▪ víme, která aktiva tvoří regulované služby
3. Zavedli jsme proces pro sledování a plnění protiopatření NUKIB	▪ někdo sleduje vývěsní desku a zpracovává DZ, které NUKIB posílá ▪ někdo to zanalyzuje a vyvodí z toho důsledky pro organizaci (= stanoví potřebná bezpečnostní opatření) ▪ někdo kolem toho vyřeší administrativu (mj. pošle info na NUKIB, jak bylo vypořádáno)
4. Zavedli jsme proces pro identifikaci a zvládání KBI, jehož součástí je komunikace s NUKIB	▪ máme nastavená pravidla pro sledování a vyhodnocování KBU ▪ existují krizové scénáře pro zvládání KBI ▪ je určená osoba, která zajistí ohlášení NUKIB a spolupráci s nimi
5. Máme gap analýzu plnění bezpečnostních opatření a dál s ní pracujeme	▪ víme, nakolik plníme požadovaná technická a organizační opatření podle vyhlášky ▪ máme plán opatření pro zajištění souladu (vč. odpovědných osob a harmonogramu)
6. Máme zavedený systém řízení kybernetické bezpečnosti	▪ řízeně analyzujeme a hodnotíme rizika, přijímáme bezpečnostní opatření, kontrolujeme jejich plnění, hodnotíme účinnost, zlepšujeme celý systém ▪ o všem vedeme záznamy ▪ o všem informujeme vedení organizace



- zákonná povinnost
 - § 12 nZKB, § 7 vyhlášky
- prerequisite pro další činnosti
 - provádění analýzy rizik
 - zavádění bezpečnostních opatření
 - plnění protiopatření NÚKIB
 - řízení dodavatelů



■ aktivum

- fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováváním informací a dat v elektronické podobě

■ primární aktivum

- aktivum v podobě zpracovávané informace nebo poskytované služby

■ podpůrné aktivum

- aktivum zajišťující fungování primárních aktiv, zejména zaměstnanec, dodavatel, technické aktivum, budova a jiný ohraničený prostor, ve kterém se nachází aktivum regulované služby

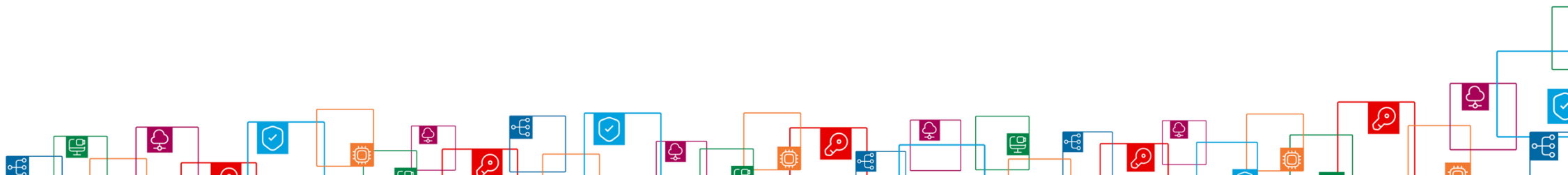
■ technické aktivum

- technickým aktivem technický nebo programový prostředek anebo vybavení

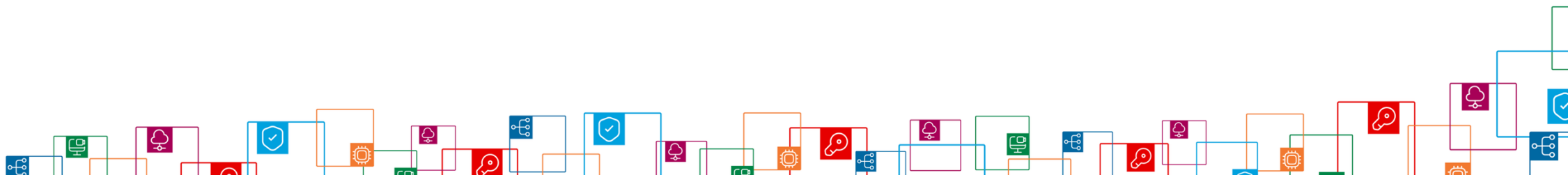


- aktivum = cokoliv, co má pro organizaci nějakou hodnotu
 - bez čeho by organizace nemohla provádět svoji činnost
 - základní stavební prvek ISMS

- pomocné otázky
 1. co vaše organizace dělá?
 2. co k tomu potřebuje?



- do rozsahu ISMS **zahrnout** aktiva související s regulovanou službou
- určit, která aktiva jsou primární a podpůrná
- pokud neurčíme, která aktiva souvisí s regulovanou službou, patří tam všechna



- stanovit metodiku (=postup) pro
 - určování aktiv
 - hodnocení aktiv (viz příloha k vyhlášce)
- evidovat garanty aktiv
 - tj. osoba odpovědná za bezpečnost aktiva
- identifikovat vazby mezi aktivy
- stanovovat pro aktiva bezpečnostní opatření



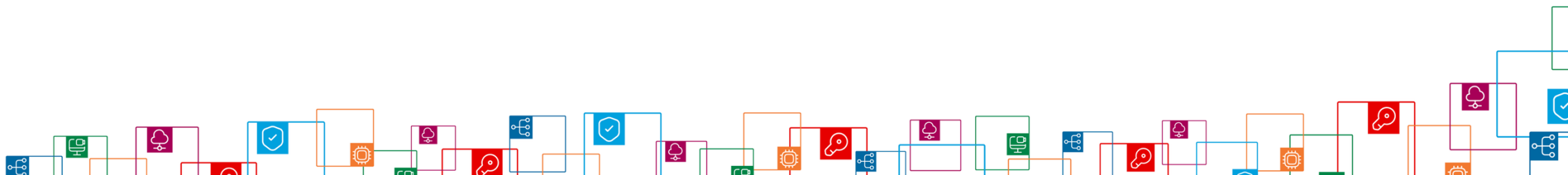
Určování aktiv na ZČÚ



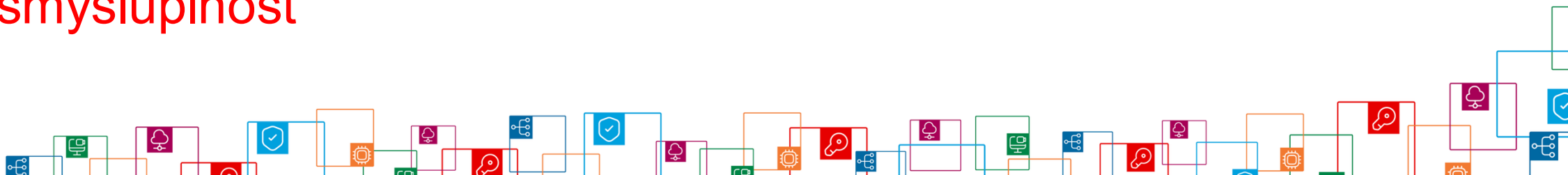
Určování aktiv jako prerekvizita



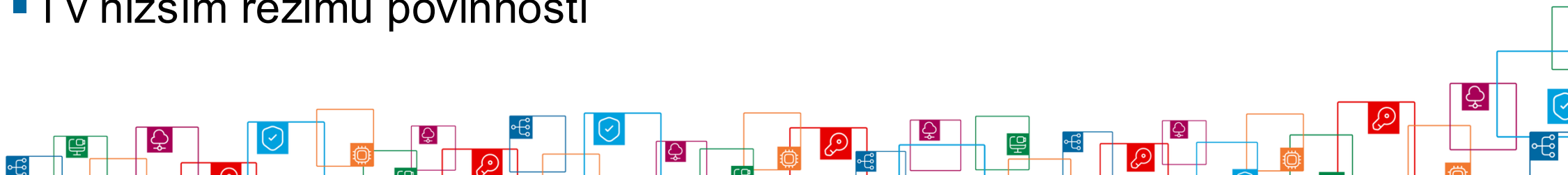
- analýzu rizik děláme nad databází aktiv
- při hodnocení rizik vycházíme z hodnocení aktiv
- pro hodnocení rizik potřebujeme určit hrozby relevantní pro aktiva
- při hodnocení rizik vycházíme z hodnocení aktiv

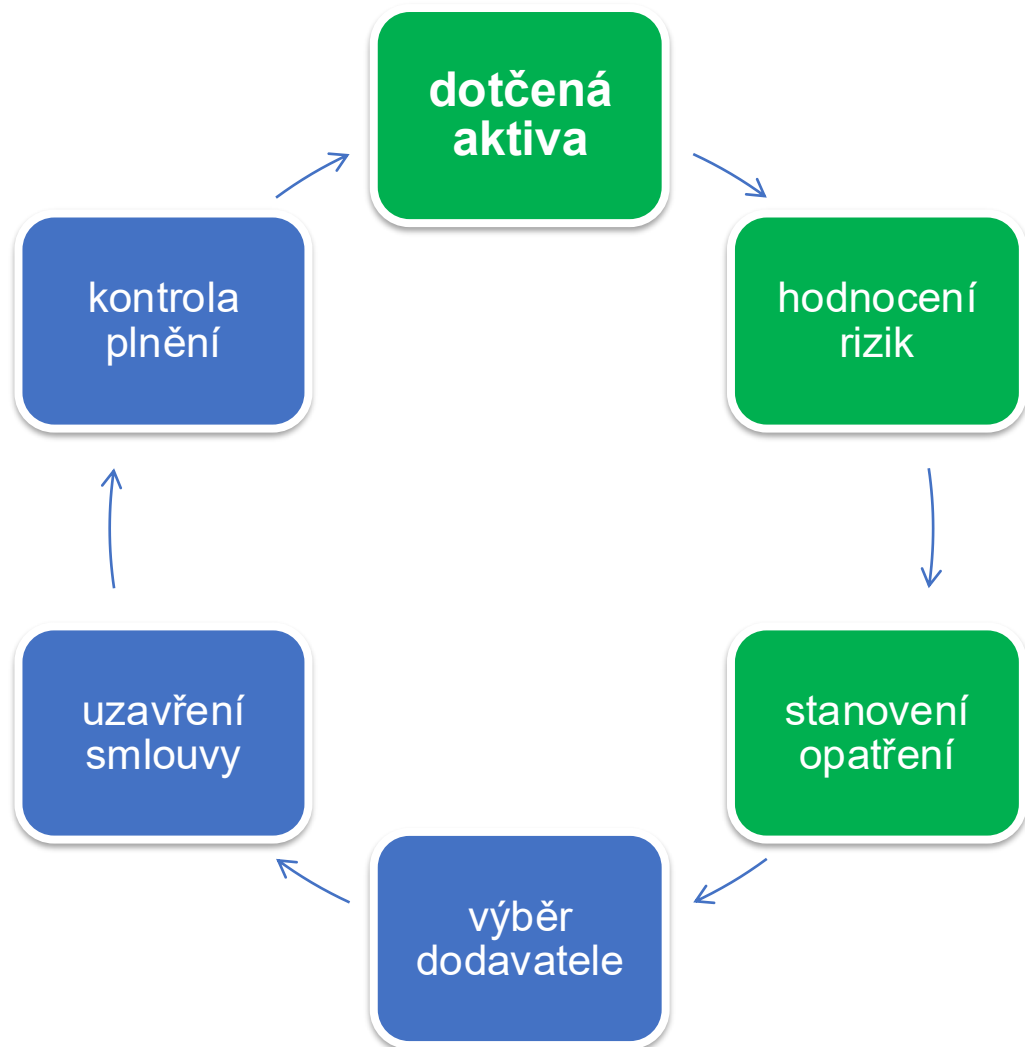


- § 13 nZKB, § 3 vyhlášek
- musím splňovat všechno?
 - zavést opatření, která jsou **relevantní** pro daná aktiva
 - zavést je **v takové míře**, která je přiměřená s ohledem na kontext organizace, stanovení cíle ISMS, bezpečnostní potřeby a řízení rizik
- obecně sledovat proporcionalitu, ekonomičnost a smysluplnost



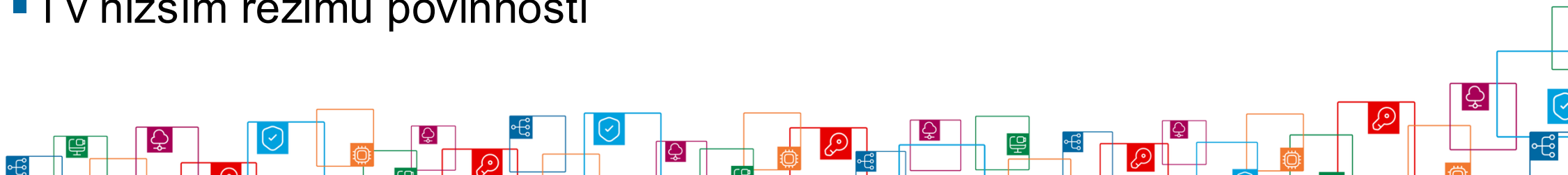
- Řízení dodavatelů = stanovení pravidel pro řízení bezpečnostních rizik souvisejících s dodávkou zboží a služeb
- Cíle řízení dodavatelů
 - zmírnit rizika spojená s přístupem dodavatele k aktivům organizace
 - zajistit bezpečnost aktiv při spolupráci s dodavateli v souladu s požadavky bezpečnostních politik
- Pozn.: Nutno řídit všechny dodavatele
 - i ty méně významné
 - i ty vybrané před účinností nZKB
 - i v nižším režimu povinností





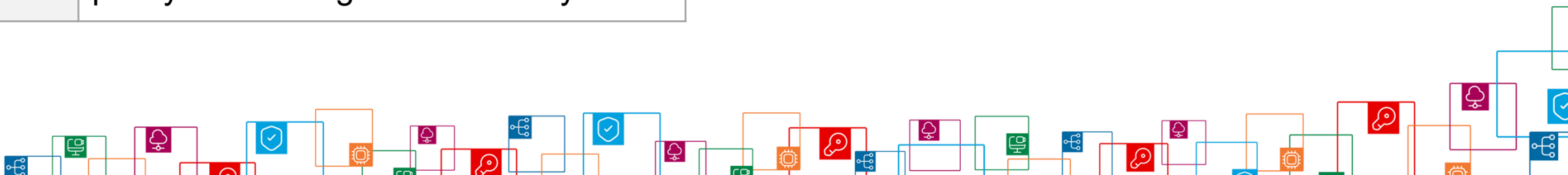
- vhodné vycházet z „životního cyklu dodavatele“
 - od definice předmětu plnění po exit strategii
- hlavní kroky:
 - identifikace dotčených aktiv
 - hodnocení rizik
 - stanovení opatření (smluvní zajištění!)

- Řízení dodavatelů = stanovení pravidel pro řízení bezpečnostních rizik souvisejících s dodávkou zboží a služeb
- Cíle řízení dodavatelů
 - zmírnit rizika spojená s přístupem dodavatele k aktivům organizace
 - zajistit bezpečnost aktiv při spolupráci s dodavateli v souladu s požadavky bezpečnostních politik
- Pozn.: Nutno řídit všechny dodavatele
 - i ty méně významné
 - i ty vybrané před účinností nZKB
 - i v nižším režimu povinností

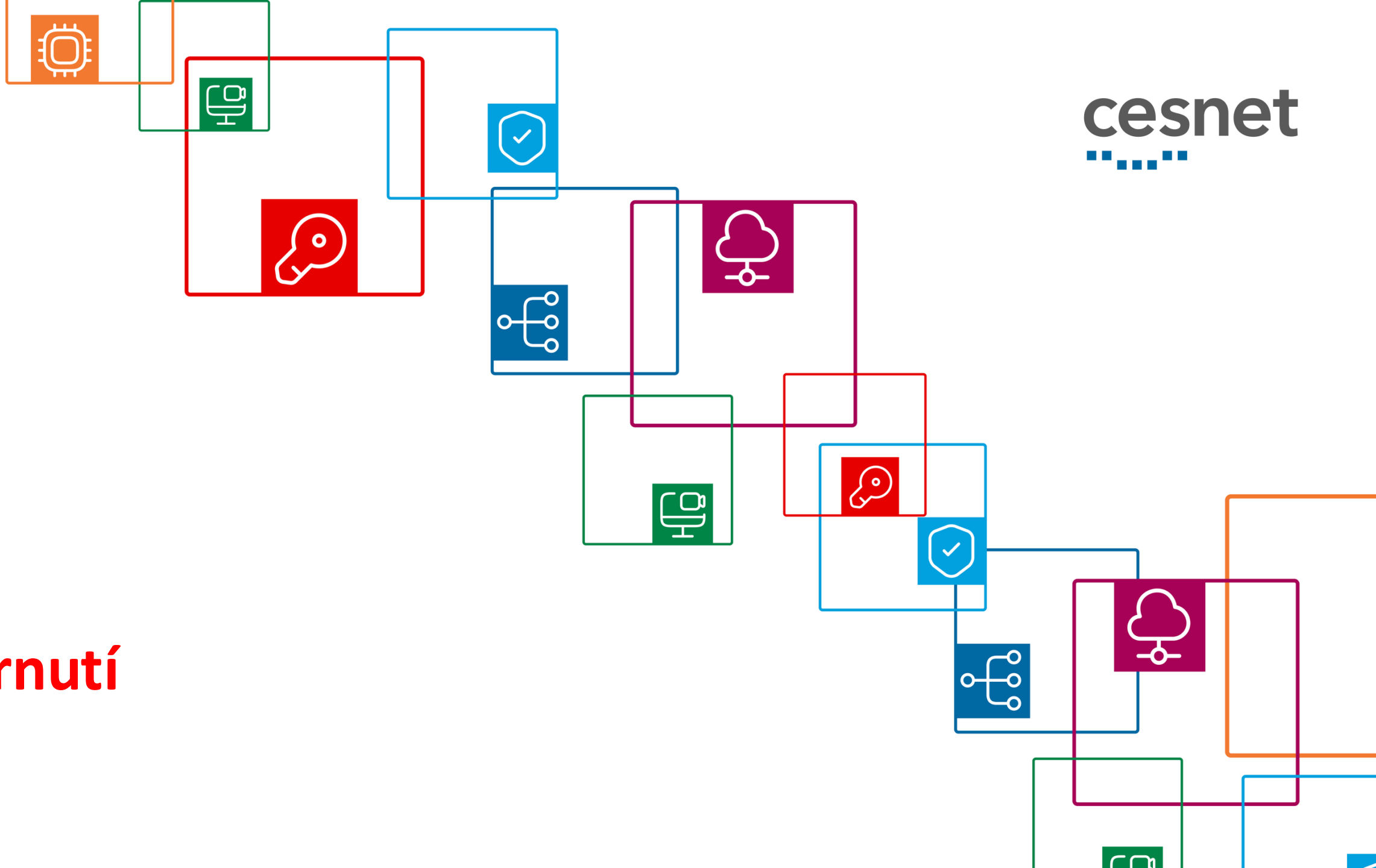


sZKB	nZKB
opatření	protiopatření
(§ 11)	(§ 20)
varování	varování = info o nové hrozbě či zranitelnosti
reaktivní opatření	reaktivní protiopatření = stanovení povinností za účelem zajištění bezpečnosti
ochranné opatření	
---	výstraha = info o KBI / porušování ZKB poskytovatele regulované služby

- viz Úřední deska NÚKIB
 - textace protiopatření + metodiky
 - platí pro všechny do odvolání, i ty dříve vydané
- **postup:**
 - **určím dotčená aktiva**
 - **provedu AR**
 - **stanovím bezpečnostní opatření**



Shrnutí



Děkujeme za pozornost
... Otázky?

