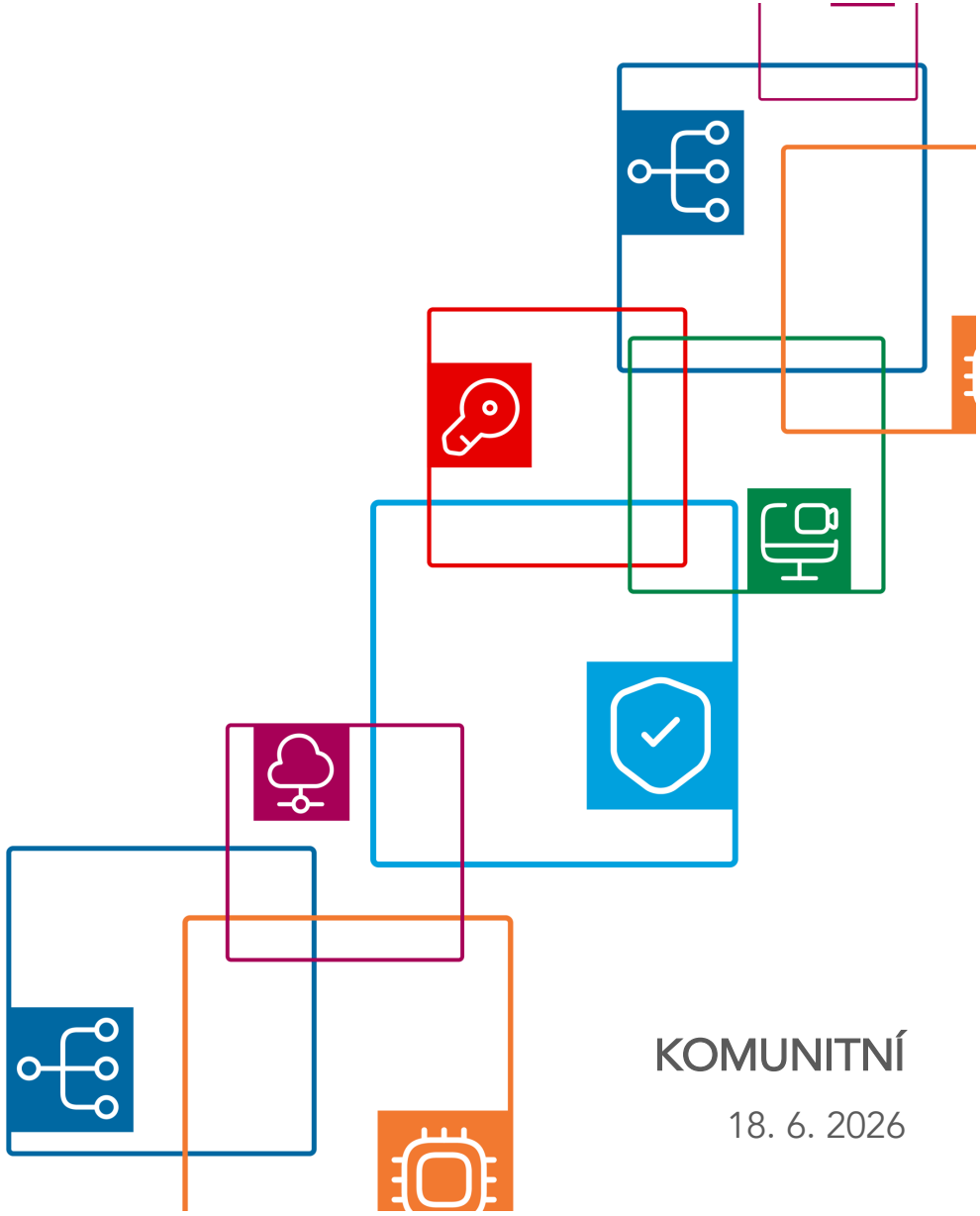
cesnet

TaPnZKB: Analýza rizik

A. Kropáčová, M. Pospíšilová



KOMUNITNÍ

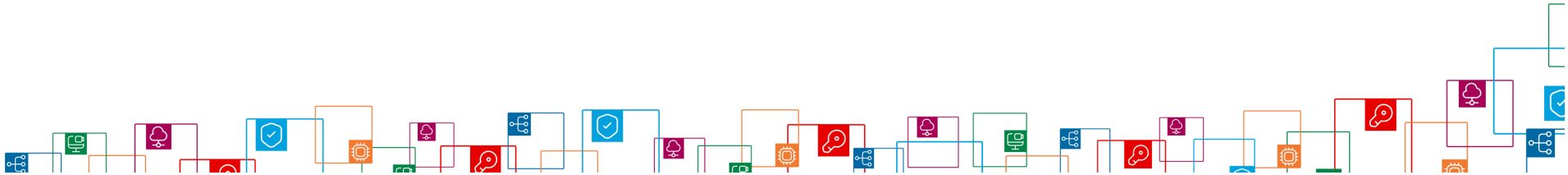
18. 6. 2026

cesnet

Teorie – vyhláška č. 409/2025 Sb.

- řízení rizik
  - proces zahrnující **hodnocení rizik**, zavádění bezpečnostních opatření ke zvládání rizik a komunikaci rizik

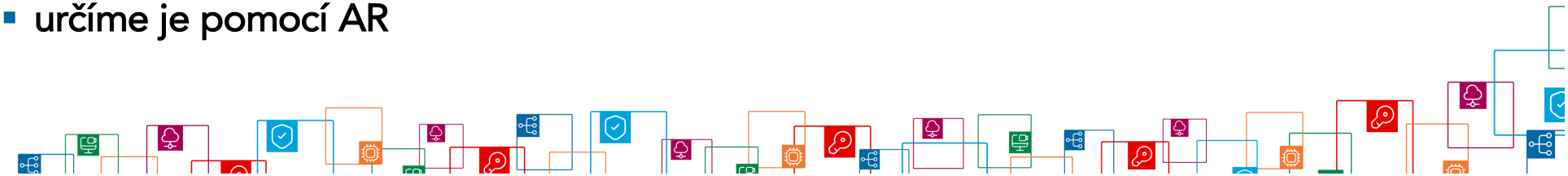
- hodnocení rizik
  - hodnocením rizik proces určování, **analýzy** a vyhodnocení rizik



cesnet

AR = chybějící článek

- CO CHRÁNÍME? aktiva = cokoliv, co má pro organizaci nějakou hodnotu
  - bez čeho by organizace nemohla provádět svoji činnost
  - základní stavební prvek ISMS (co děláte a co k tomu potřebujete)
- JAK TO CHRÁNÍME? zaváděním bezpečnostních opatření = opatření pro zajištění bezpečnosti aktiv ☺
  1. organizační
  2. technická
- **PŘED ČÍM? před riziky...**
  - **před těmi neakceptovatelnými**
  - **určíme je pomocí AR**

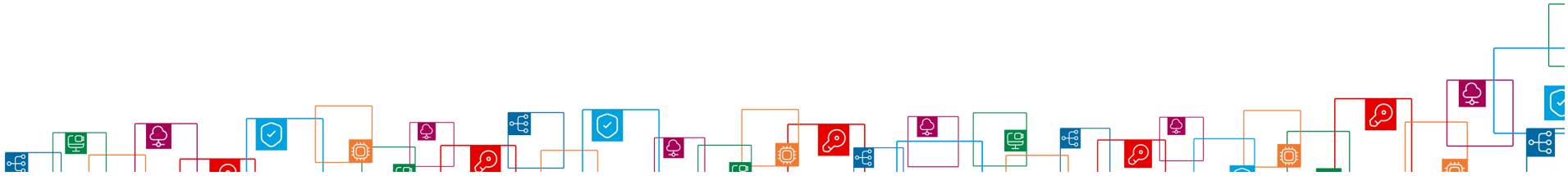


cesnet

Opravdu musím?

- § 8 vyhlášky
  - alespoň 1x ročně + při významných změnách
  - alespoň v rozsahu dle vyhlášky
  - se zprávou o hodnocení rizik a s plánem zvládání rizik se musí seznámit vrcholné vedení

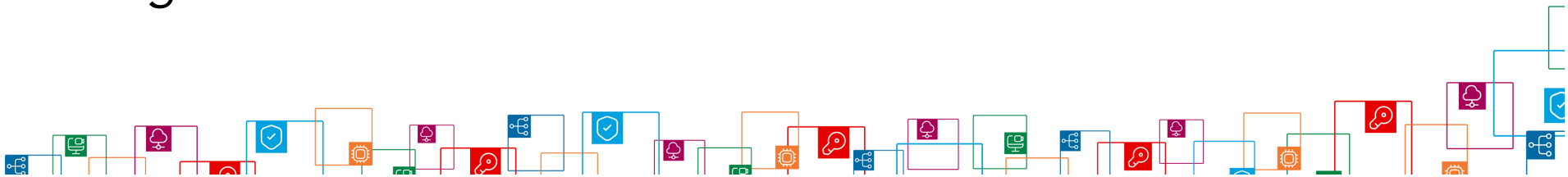
- je to prerekvizita
  - viz dále



cesnet

Teorie – vyhláška č. 409/2025 Sb. i č. 410/2025 Sb.

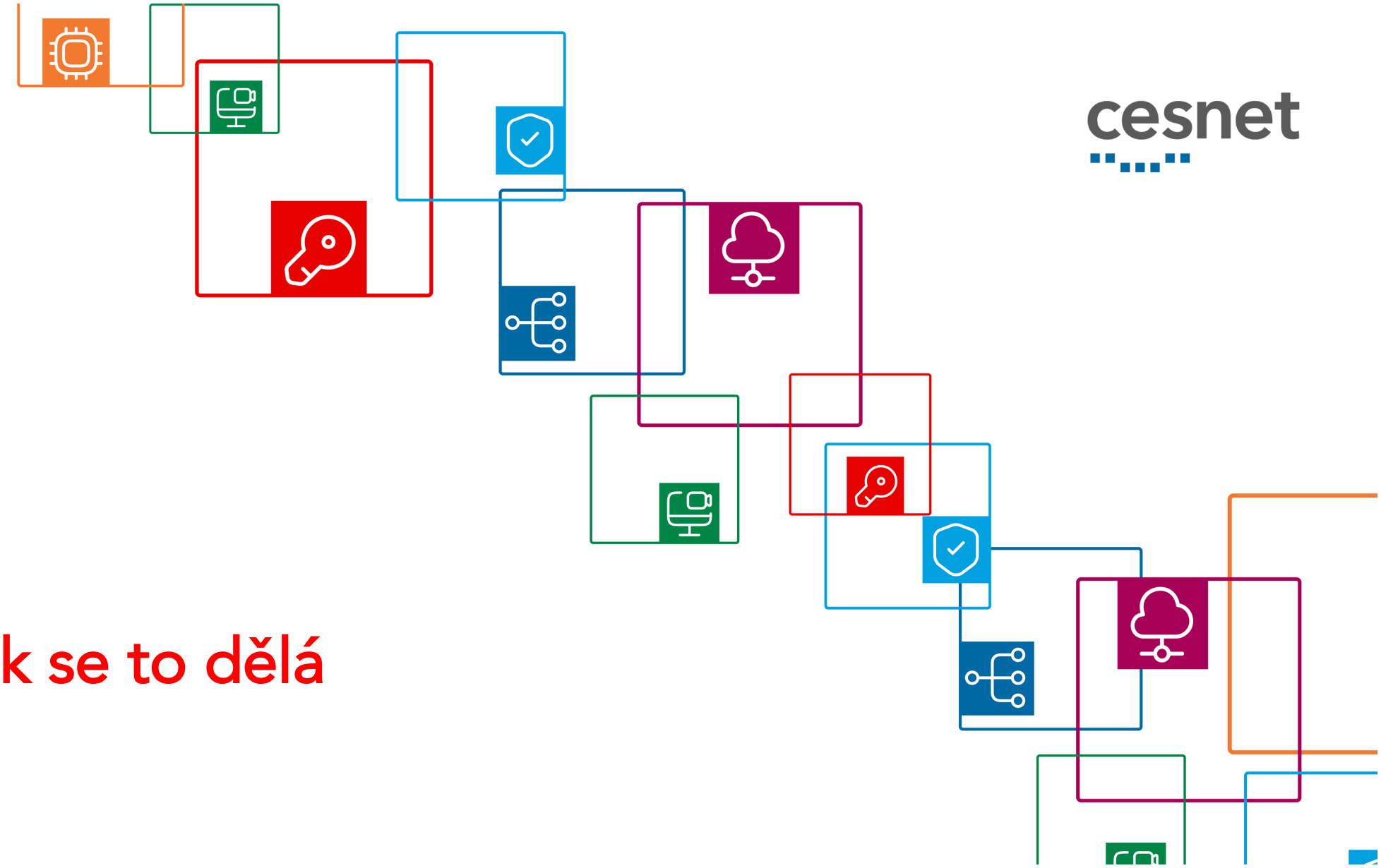
- bezpečnostní potřeby
  - definice: ?
  - *„Hlavní bezpečnostní potřeby sdružení CESNET jsou:*
    - *a) zajistit funkční systém řízení kybernetické bezpečnosti,*
    - *b) zajistit výkon potřebných bezpečnostních rolí,*
    - *c) řádně a včas zavádět bezpečnostní opatření a reagovat na bezpečnostní události a incidenty,*
    - *d) stanovit bezpečnostní politiky a zvyšovat bezpečnostní povědomí adresátů těchto politik,*
    - *e) vést řádné záznamy a dokumentaci a na jejich základě soustavně zlepšovat úroveň kybernetické bezpečnosti organizace."*



cesnet

Help...

- vyhláška 409 – § 8 + její přílohy ...už chápete?
- NÚKIB – nové podpůrné materiály
  - *https://portal.nukib.gov.cz/informacni-servis/podpurne-materialy*
  - *poslední z 6/2026*
  - přiměřenost pro nižší režim: https://portal.nukib.gov.cz/storage/uploads/2026/03/31/podpurny-material_primerenost-v-1-1_uid_69cbcfc2926be.pdf
- NÚKIB – staré podpůrné materiály
  - jen malá změna oproti starému nZKB
  - https://nukib.gov.cz/download/publikace/podpurne_materialy/Prvodce%20zenm%20aktiv%20a%20rizik%20dle%20vyhlky%20o%20kybernetick%20bezpenosti.pdf



cesnet

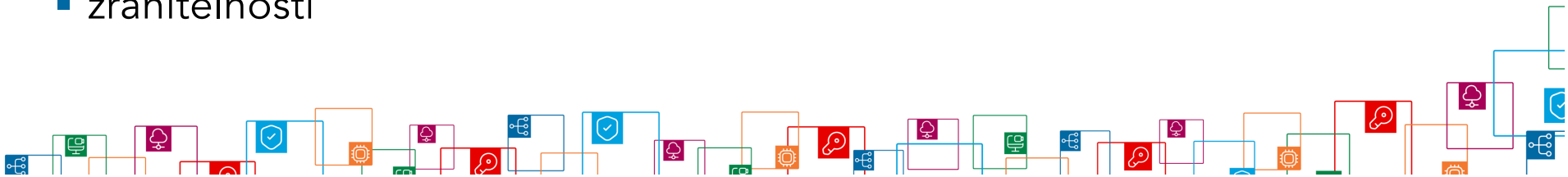
Jak se to dělá

cesnet

Metodika pro určování a hodnocení rizik

Jak vypadá metodika CESNET (1. část)

- úvod
  - proč metodiku vydáváme, jaké jsou její cíle
    - stanovit jasný postup, zajistit opakovatelnost
    - při pochybnostech o správnosti provedené AR nutno předložit (např. u výběrových řízení)
- východiska
  - odkaz na rámce, ze kterých vychází (např. ZKB, ISMS,...)
  - co zohledňujeme
    - dopady
    - hrozby
    - zranitelnosti



cesnet

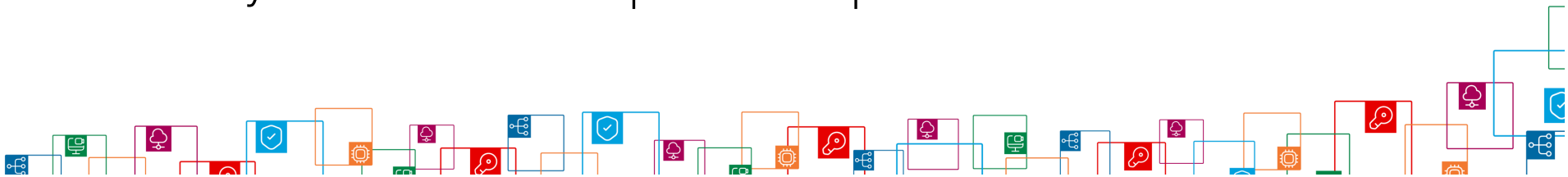
Jak vypadá metodika CESNET (2. část)

- jak hodnotit dopady
  - odvozena od hodnoty aktiv
  - stupnice pro určení hodnoty dopadů
- jak hodnotit hrozby
  - máme katalog hrozeb, vybíráme ty relevantní
  - stupnice pro hodnocení hrozeb
  - vycházíme z pravděpodobnosti jejího uplatnění
- jak hodnotit zranitelnosti
  - stupnice pro hodnocení zranitelností
  - vycházíme z pravděpodobnosti její úspěšnosti

Jak vypadá metodika CESNET (3. část)

- jak hodnotit rizika
  - vzorec
    - dopad X hrozba X zranitelnost
  - stupnice jako podklad pro určení akceptovatelnosti

- kritéria pro akceptovatelnost rizik
  - tj. určení akceptační meze
    - nízká – budeme sledovat, jinak bez opatření
    - střední - vybereme (MKB + garant), která lze akceptovat a která vyžadují bezpečnostní opatření
    - vysoká – zavedeme bezpečnostní opatření
    - kritická rychle zavedeme bezpečnostní opatření



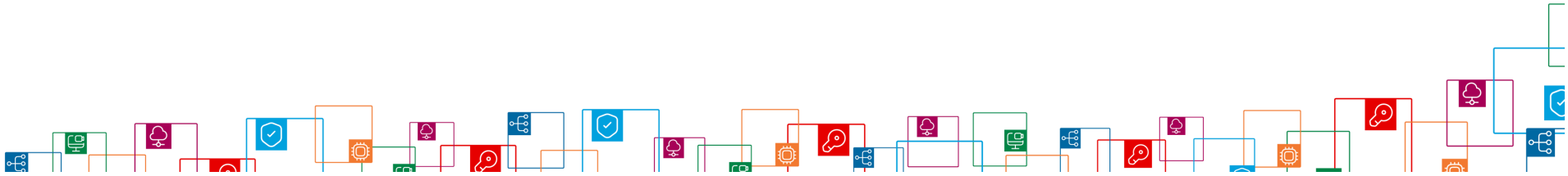
cesnet

Analýza rizik jako prerekvizita

cesnet

Jak to má teoreticky fungovat

1. mám aktiva
2. na aktiva působí hrozby a zranitelnosti
3. vyhodnotím, jaká rizika jim hrozí a jak jsou velká
4. stanovím bezpečnostní opatření pro jejich eliminaci či snížení



K čemu je AR potřeba? (1. část)

- stanovení bezpečnostní politiky
  - soubor zásad a pravidel, která určují způsob zajištění ochrany aktiv
  - základ viz náš vzor z podzimu 2025

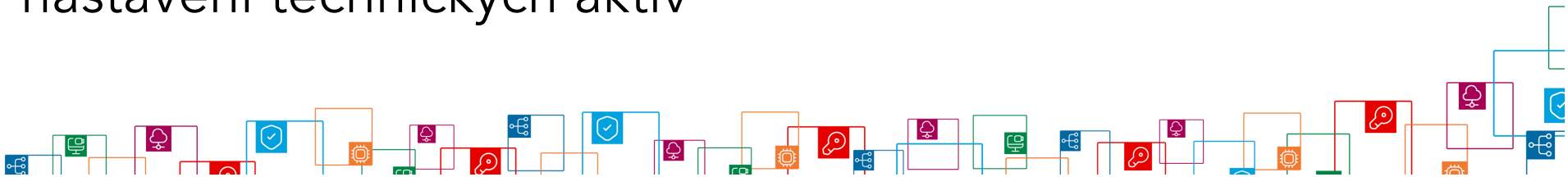
- PoA
  - přehled všech bezpečnostních opatření stanovená vyhláškou
  - která byla aplikována + jakým způsobe,
  - která nebyla aplikována + proč + náhradní opatření
    - **neaplikovat lze pouze na základě provedené AR**

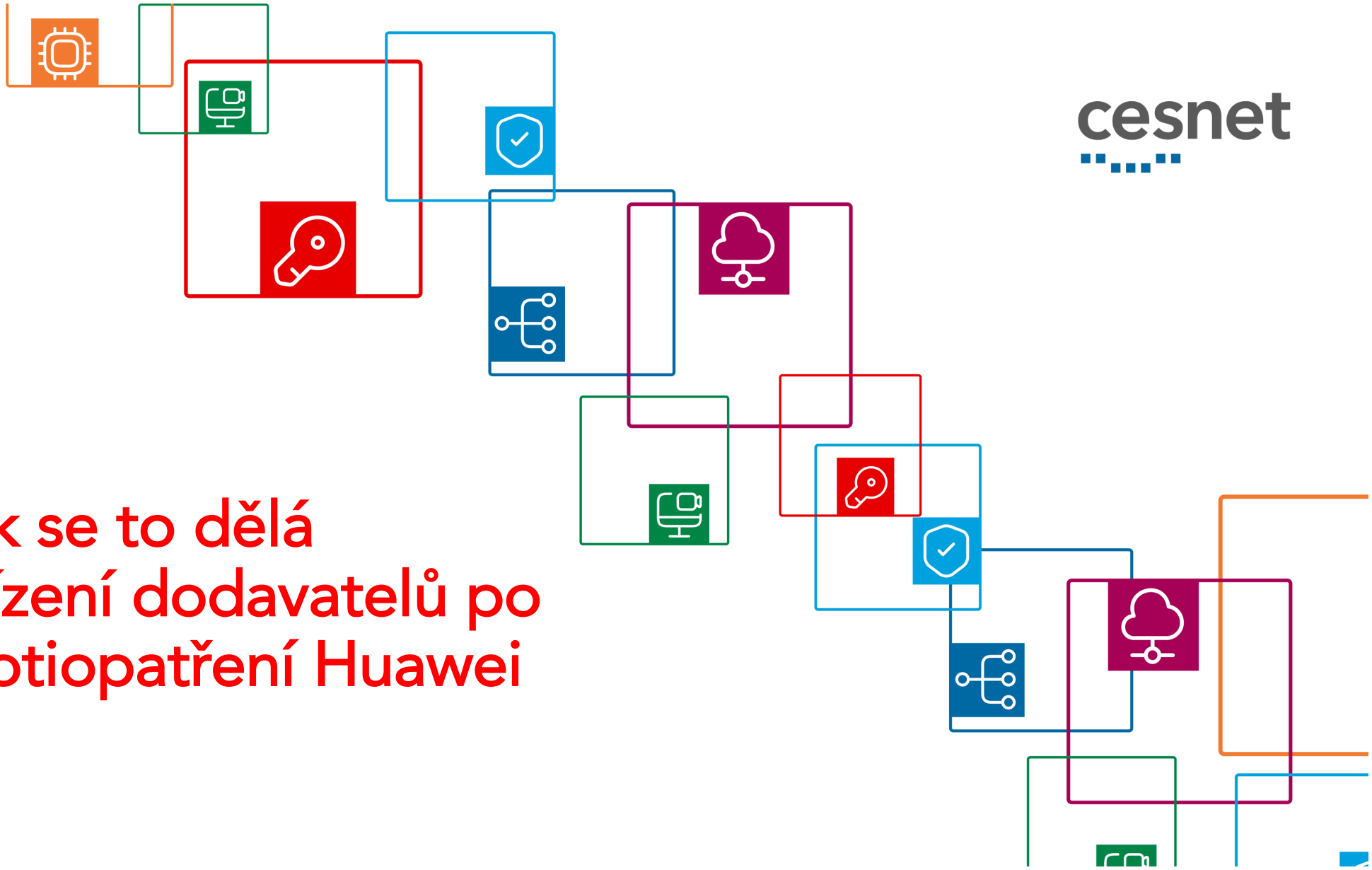
- řízení dodavatelů
  - povinně u významných
  - při výběrovém řízení či před uzavřením smlouvy
  - průběžně – pravidelně + bezodkladně na rizika reaguje

cesnet

K čemu je AR potřeba? (2. část)

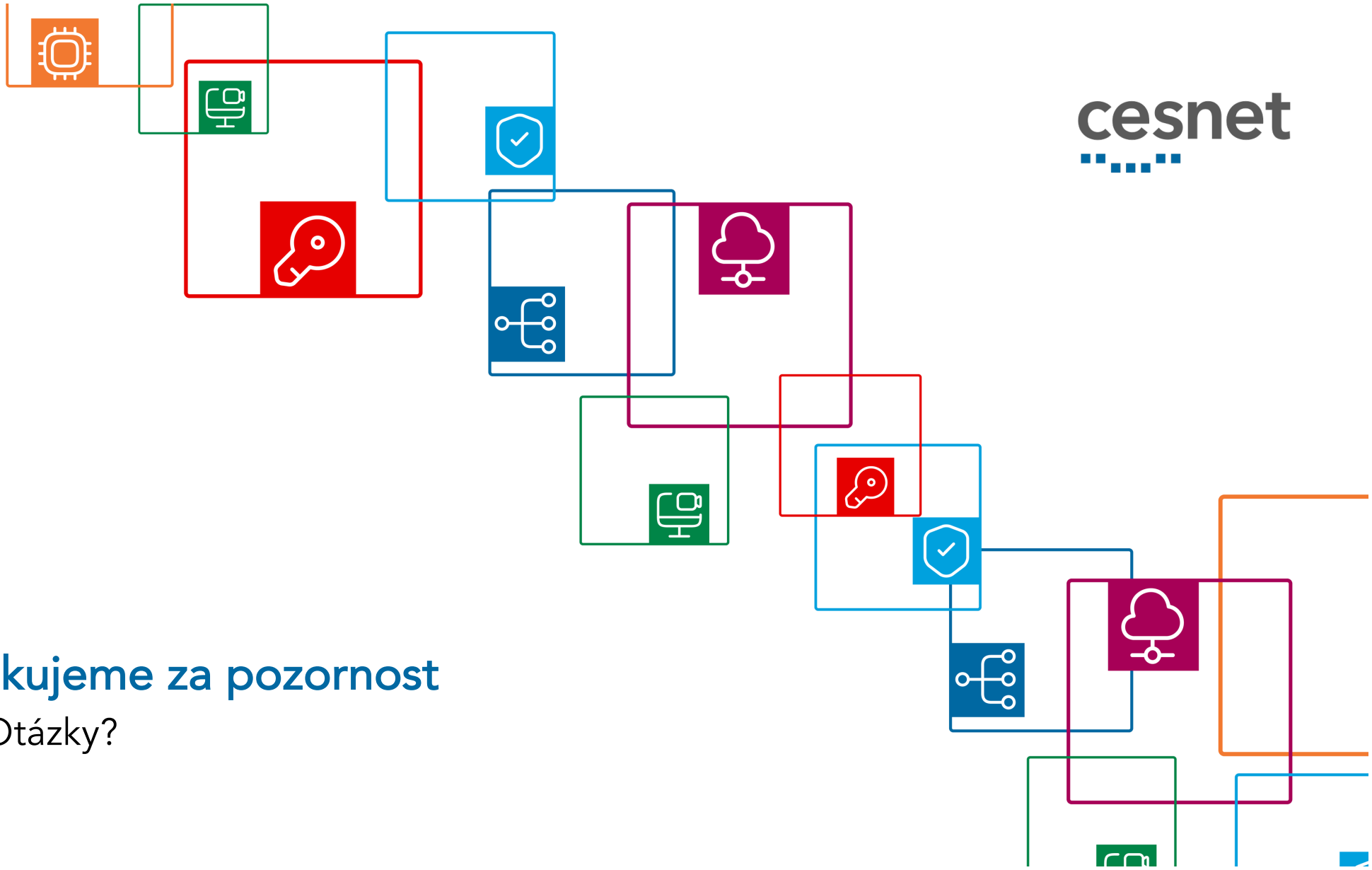
- řízení kontinuity činností
  - zohlednit při stanovování cílů řízení kontinuity činností
- penetrační testování
  - zohlednit při stanovování kdy a co testovat
  - zpětně zohlednit při AR
- zajišťování dostupnosti regulované služby
  - podklad pro stanovení požadavků na konfiguraci a nastavení technických aktiv





cesnet

Jak se to dělá
- řízení dodavatelů po protiopatření Huawei



cesnet

Děkujeme za pozornost

... Otázky?