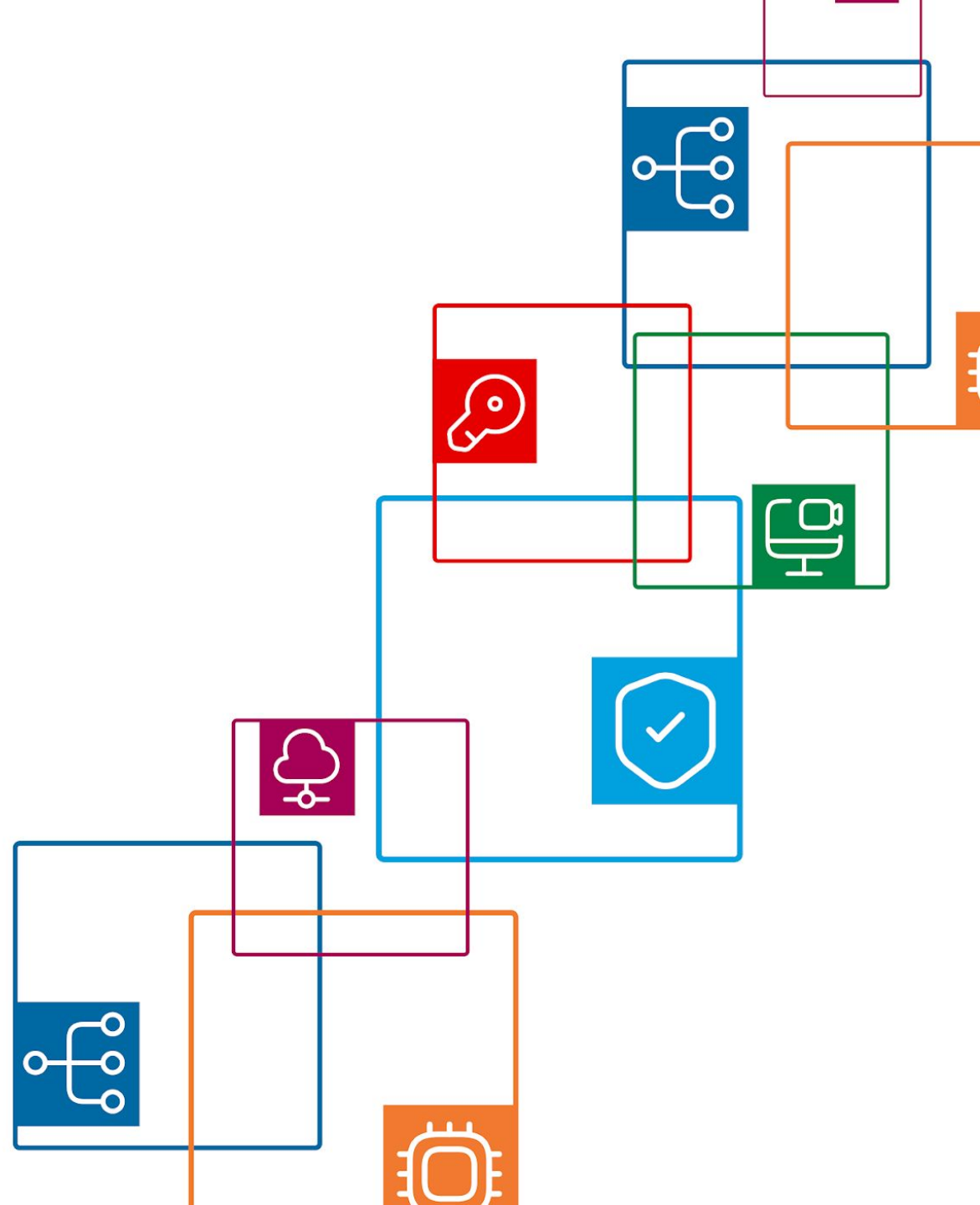




Teorie a praxe nového zákona o kybernetické bezpečnosti

Určení aktiv a jejich garantů

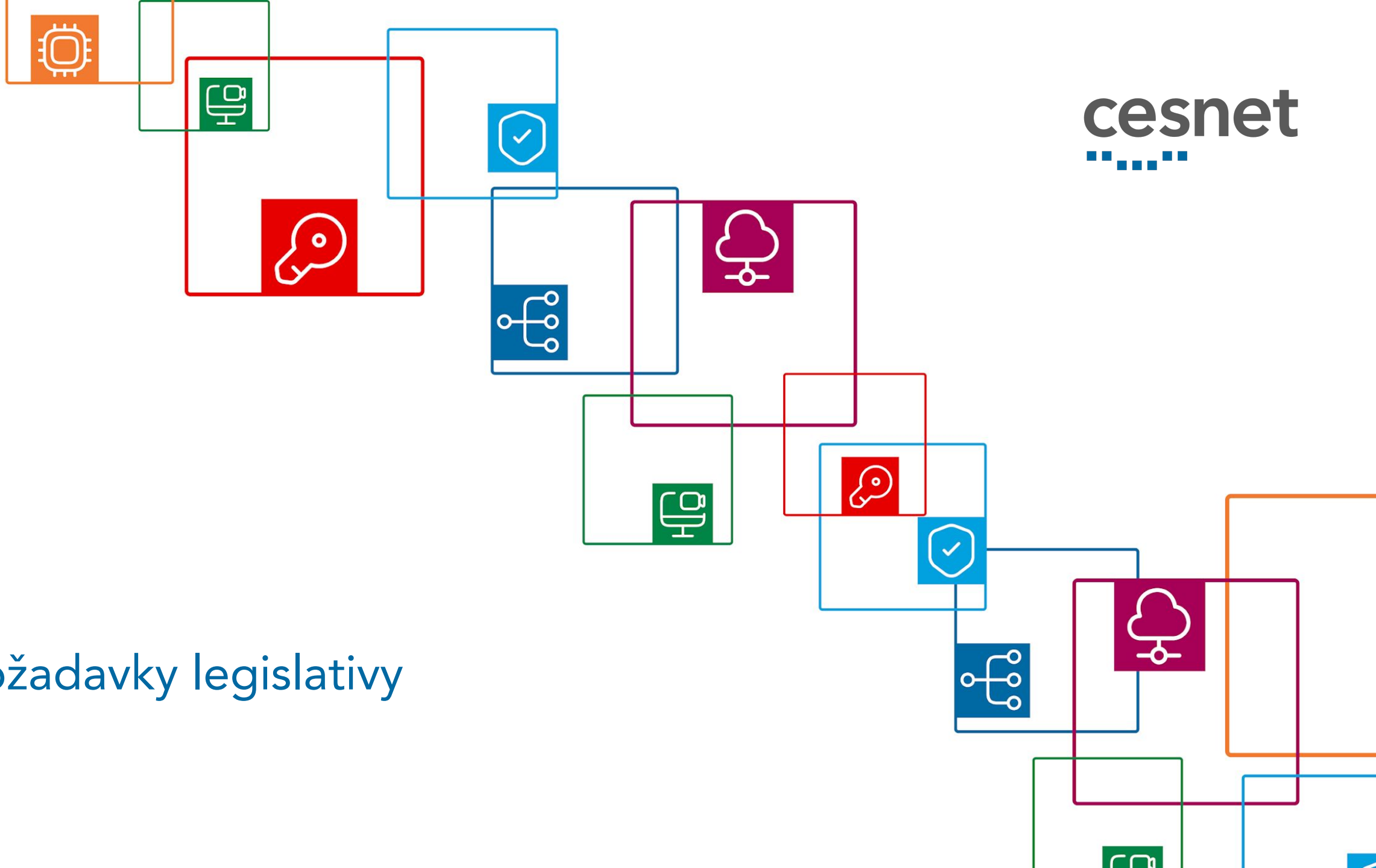
Jiří Bořík, 27. května 2026



- Zákonné povinnosti
- Předpoklady pro určování aktiv
- Určení aktiv a jejich garantů
- Garant a jeho povinnosti
- Příklad řešení na univerzitě
- Shrnutí



Požadavky legislativy



zákon 264/2025 Zákon o kybernetické bezpečnosti

§ 2 Vymezení pojmů

- (1) Pro účely tohoto zákona se rozumí
- ... c) aktivem fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováváním informací a dat v elektronické podobě,

§ 12 Stanovení rozsahu řízení kybernetické bezpečnosti

- ... Součástí rozsahu řízení kybernetické bezpečnosti (dále jen „stanovený rozsah“) jsou aktiva související s poskytováním regulované služby.
- ... Poskytovatel regulované služby eviduje ... primární aktiva, která byla ze stanoveného rozsahu vyjmuta, včetně důvodů jejich vyjmutí.
- ... Stanovený rozsah je poskytovatel regulované služby povinen pravidelně přezkoumávat a aktualizovat.

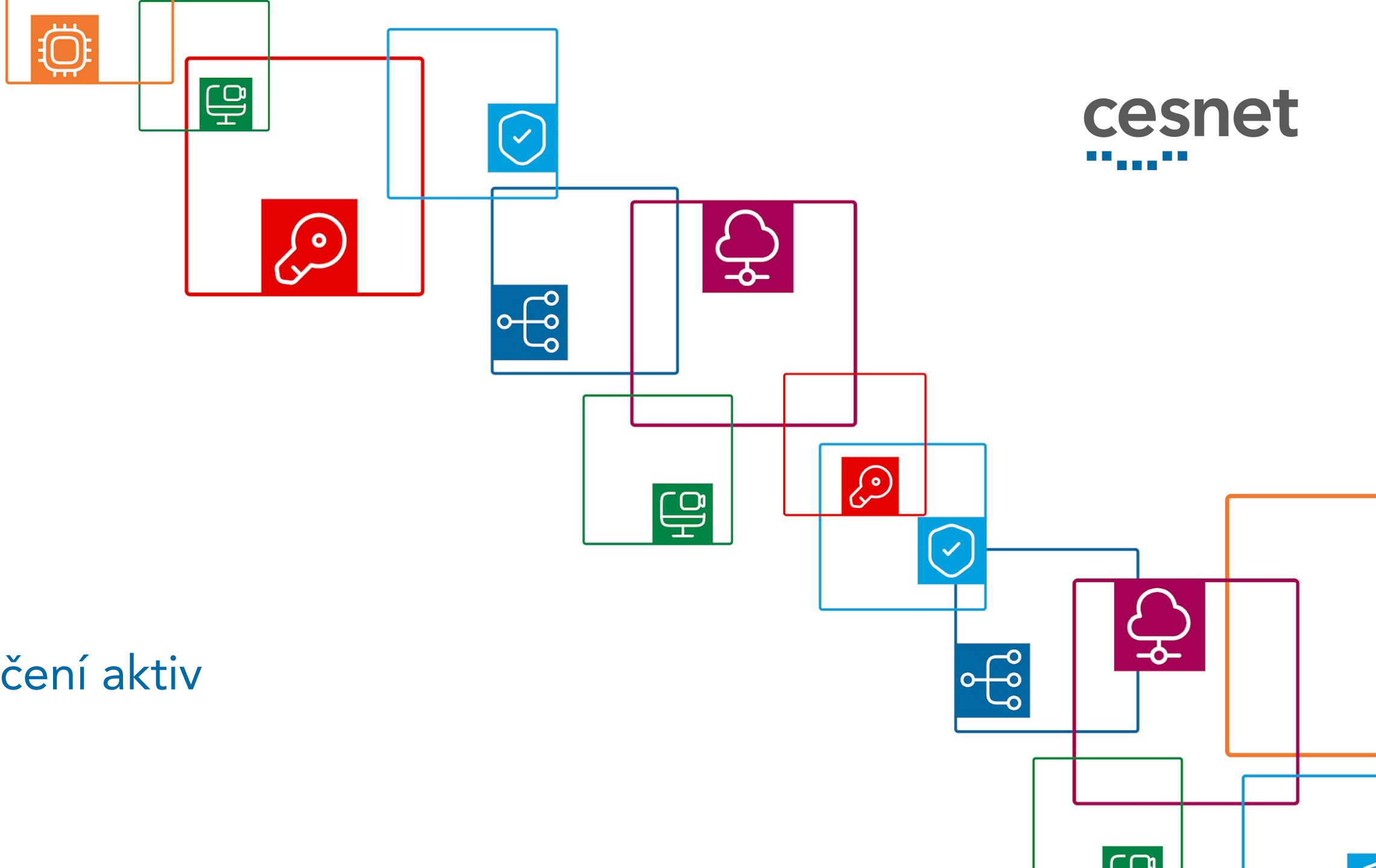


409/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

- § 4 ...vrcholné vedení ... určí ... c) garanta aktiva ...
- § 5 ... (3) Garant aktiva je pověřen k zajištění rozvoje, použití a bezpečnost aktiva.
- § 7 ... Povinná osoba ... stanoví metodiku určování aktiv ... eviduje garanty ... hodnotí aktiva ... stanovuje pravidla ochrany aktiv ...
- příloha číslo 1 Hodnocení aktiv



Určení aktiv



- Registrované regulované služby
 - výsledky samoidentifikace (podklady pro hlášení RS)
 - oznámení NÚKIB o registraci RS
- Interní zdroje informací o aktivech
 - Katalog služeb
 - Evidence informačních systémů
 - Řízení rizik organizace
 - Mapa procesů organizace
 - Smluvní partneři a předměty smluv
 - ... další vhodné zdroje



- **Technický pohled**
 - aktivum je technologická jednotka (např. diskové pole)
 - vede na velký počet aktiv (velké desítky nebo stovky)
- **Manažerský pohled**
 - aktivum je logická jednotka (hlavní proces, velká množina dat) k zajištění reg. služby
 - vede na technicky nesourodá (nejednotná) aktiva, ale v menším počtu (malé desítky)
- **Pracnost evidence aktiv**
 - potřebné kroky pro každé aktivum (úvodní i periodické!)
 - evidence aktiva (základní údaje, kategorizace minimálně dle vyhlášky...), garanti aktiv, správci,
 - analýza rizik (rizika a jejich vlastníci), nápravná opatření (a jejich zodpovědné osoby), kontrola řešení
 - analýza dopadů, plán kontinuity, plán obnovy...
 - formální dokumentace a její projednání
 - školení garantů aktiv a dalších rolí
 - plocha pracnosti - počet aktiv x potřeby řízení jednoho aktiva
- **Společné zdroje pro provoz všech aktiv (peníze, lidé, čas...)**
 - kolize priorit, souboj o zdroje,
 - kritická rozhodnutí se stejně eskalují k vrcholným manažerům



- Evidence samotných aktiv (minimum dle ZoKB)
 - název, popis
 - typ aktiva podle ZoKB § 2 (1)
 - stupnice pro hodnocení důvěrnosti, integrity a dostupnosti podle vyhl. 409/2025, příloha 1, Tab. č. 1-3
 - oblasti hodnocení primárních aktiv podle vyhl. 409/2025, příloha 1, Tab. č. 4
 - u podpůrných aktiv vazba na primární aktiva dle vyhl. 409/2025, příloha 1
 - garant aktiva
- Analýza rizik aktiva
 - rizika aktiva, vlastník rizika
 - ošetření rizika, nápravné opatření, stav realizace opatření
- Analýza dopadů
- Plán kontinuity (např. priority obnovy aktiva vůči ostatním)
- ... další navazující agendy
- a vše periodicky aktualizovat a vylepšovat v PDCA cyklu



- Rozběhnutí správy aktiv - jde většinou o nové činnosti:
 - vytvoření politiky a pracovních postupů,
 - konsolidace datové základny, napojení na ostatní datové zdroje,
 - nastavení komunikace s garanty aktiv,
 - vysvětlení nových pojmů a procesů, osobní konzultace,
 - první určení aktiv, první analýza rizik,
 - postupné přidávání činností a rozšiřování datové základny.

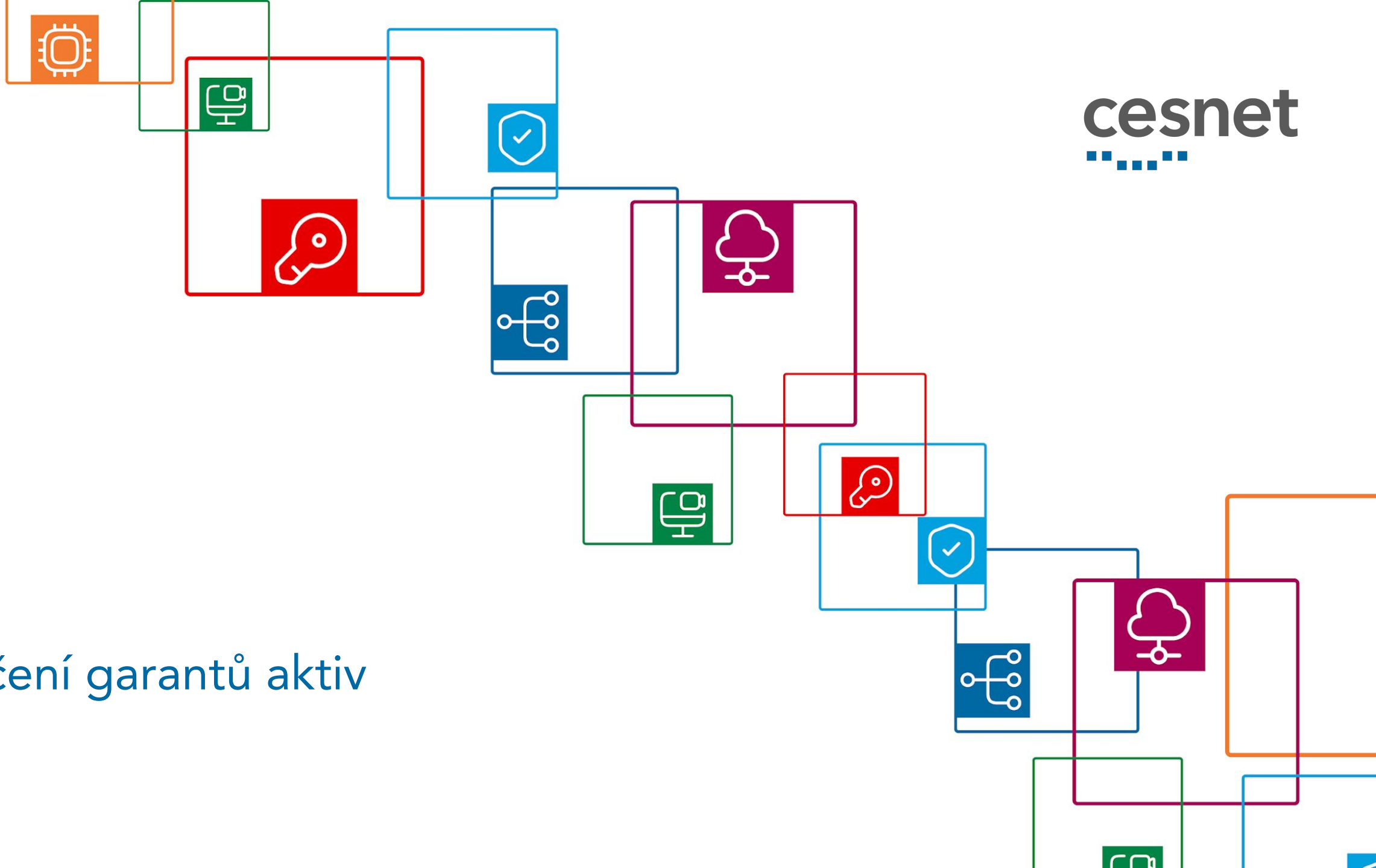
Nejpružnější je v úvodní fázi použít běžné kancelářské nástroje (textový editor a tabulkový procesor).

Pro zaběhnutý systém a metodiku pak vybrat aplikaci, která vyhovuje zjištěným potřebám.

- Výhody aplikace:
 - snazší správa, jednotný formát dat, číselníky,
 - přístup garantů a dalších rolí přímo k datům pomocí aplikace (máme už zaběhnutý proces, nutná znalost používání ze strany garantů),
 - snadné dokumentační výstupy,
 - automatická auditní stopa.



Učení garantů aktiv



- Zná aktivum,
 - ví proč aktivum organizace potřebuje a používá (proces, služba)
 - má představu o budoucím využití (životní cyklus aktiva)
 - návaznost na dlouhodobou strategii organizace (rozvoj a útlum služeb)
- Dokáže ovlivnit zdroje na provoz a rozvoj aktiva,
 - aktivum konzumuje finance, lidské zdroje
 - návaznost na finanční plánování a projekty
- Dokáže posuzovat rizika spojená s aktivem,
 - rizika, analýza dopadů, proces řešení incidentů, plán kontinuity...
 - znalost technických řešení, provádění bezpečnostních opatření
 - návaznost na operativu a provoz aktiva



- Požadavky na garanta aktiva jsou široké,
 - většinou nenajdeme osobu pokrývající všechny oblasti
 - klíčová je strategie a schopnost ovlivnit zdroje
- Pomocná role: technický správce aktiva
 - většinou jde o administrátora dotčených systémů
 - navázat komunikaci garant - tech. správce
 - někde už přirozeně vazba existuje
 - všechny určené osoby proškolit, vysvětlit novou terminologii, proces, PDCA



- **Garant aktiva**
 - strategický pohled na aktivum
 - manažerské zdroje a prostředky
- **Technický správce aktiva**
 - provozní pohled nad aktivem
 - technické a provozní znalosti aktiva
- **Manažer kybernetické bezpečnosti**
 - procesní pohled na všechna aktiva
 - řízení správy aktiv, analýzy rizik, sledování nápravných opatření...



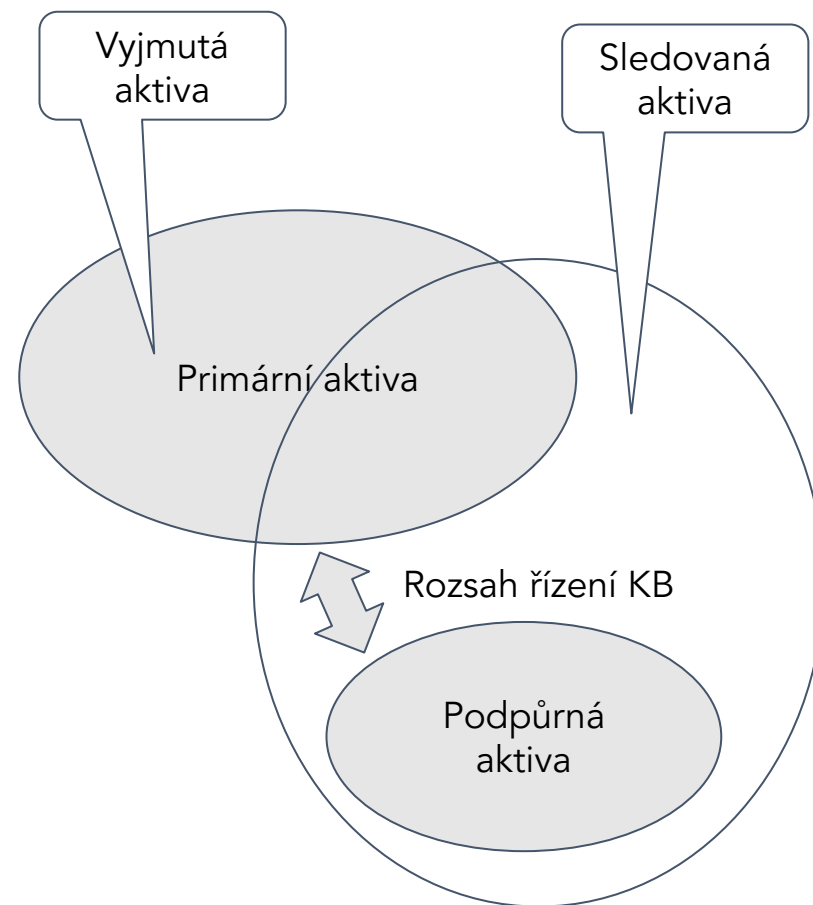
Příklad - Západočeská univerzita v Plzni

- ZČU má 9 fakult (z toho 3 technické) a jedno samostatné výzkumné centrum
- centrální správa ICT infrastruktury a služeb
 - poměrně málo fakultních a katedrálních IT složek
- implementace povinností ZKB
 - netvoříme nový úřad, přibyl jen MKB
 - nezbytně nutný minimální rozsah, rozšíření dle zkušeností později
 - návaznost na stávající struktury a role, nezačínáme od nuly
 - výbor řízení rizik univerzity
 - provozní oddělení IT bezpečnosti CIV
 - prorektor pro vědu a jeho kolegium (fakultní proděkaní pro vědu)
 - lokální IT správci na fakultách



minimalistická varianta:

- Dle ZKB: rozsah řízení KB obsahuje primární aktiva potřebná pro zajištění registrovaných regulovaných služeb.
- Ostatní primární aktiva jsou z rozsahu vyjmuta
 - z důvodu nerelevantnosti pro zajištění registrovaných regulovaných služeb.
- Podpurná aktiva
 - jsou společná pro všechna identifikovaná aktiva (společná infrastruktura)
 - vyjmutá aktiva jsou tedy stejně pod působením bezpečnostních opatření.
- Granularita všech evidovaných aktiv je velmi hrubá
 - co největší celky, kde lze nalézt společného garanta
 - do budoucna - rozdělení na menší aktiva jen tam, kde to bude z hlediska evidence dávat smysl



- Reg. služba 1 Výkon svěřených pravomocí VŠ
 - studijní agenda (služba a informace)
 - garantem aktiva je prorektor pro studium
 - spisová služba (služba a informace)
 - komunikační systémy (služba)
 - garantem těchto aktiv je kvestorka
- Reg. služby 16 Digitální služby
 - poskytování hostingu v rámci akademické spolupráce (služba)
- Reg. služba 19 Výzkum a vývoj
 - úložiště výzkumných dat (informace)



- Úložiště vědeckovýzkumných dat a jednotlivá aktiva
 - Centrálně spravovaná úložiště
 - 1 logické aktivum - vlastní úložiště ZČU, cloudy, DÚ CESNET
 - garantem aktiva je prorektor pro vědu
 - technickým správcem je vedoucí odboru infrastruktury
 - Úložiště ve správě fakult nebo center
 - 4 samostatná aktiva, různé varianty (celá serverovna, diskové úložiště, několik dílčích úložišť kateder, cloudy)
 - garantem aktiva je proděkan pro vědu nebo podobný vedoucí pracovník
 - technický správce - odpovědný IT pracovník fakulty nebo katedry
 - Úložiště v osobní správě výzkumníka
 - všechny ostatní varianty (server pod stolem, notebook, flashdisk...)
 - tlak na přesun do centrálně řízených úložišť, zbytkový rozsah zůstane stále
 - garant aktiva - prorektor pro vědu
 - technický správce - MKB (pravidla, pravidelná školení, metodická pomoc při migraci...)



- Podpůrná aktiva - ICT infrastruktura v hrubé granularitě
 - síť,
 - serverovny,
 - HW,
 - SW serverů a stanic,
 - lidské zdroje (IT pracovníci)
 - samostatně i kyberbezpečnost (nástroje a procesy)
- Garant všech podpůrných aktiv
 - ředitelka CIV
 - zodpovídá za zdroje pro infrastrukturu (finance na techniku a personál)
- Techničtí správci
 - vedoucí odpovídajících oddělení
 - zodpovídají za provoz a technický rozvoj aktiv



vyhl. 409/2025				ZoKB § 2 (1)	vyhl. 409/2025 příloha 1 Tab. č. 1:				Tab. č. 4 Oblasti hodnocení primárních aktiv			
Aktivum	reg. služba popis aktiva	garant aktiva	technický správce	typ aktiva	Stupnice pro hodnocení důvěrnosti	Stupnice pro hodnocení integrity	Stupnice pro hodnocení dostupnosti		a) rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů	b) rozsah dotčených právních povinností nebo jiných závazků nebo obchodního tajemství	c) rozsah narušení vnitřních řídicích a kontrolních činností	d) poškození veřejných obchodních nebo ekonomických zájmů a možné finanční ztráty
Primární aktiva												
1.1 Výkon svěřených pravomocí												
studijní agenda - aplikace a proces	zajištění dostupnosti služeb a souvisejících aplikací	PR-P		služba	vysoká	vysoká	střední				chybný výkon administrace studia	
studijní agenda - data	studijní agenda - kvalita a zabezpečení uchovávaných dat	PR-P		informace	vysoká	vysoká	střední		osobní data studentů			pokuta ÚOOÚ
spisová služba - aplikace a proces	spisová služba - zajištění dostupnosti služeb	kvestorka		služba	vysoká	vysoká	střední			499/2004 Sb. Zákon o archivnictví a spisové službě	backoffice organizace	
spisová služba - data	spisová služba - kvalita uchovávaných dat	kvestorka		informace	vysoká	vysoká	střední		osobní data komunikujících subjektů	499/2004 Sb. Zákon o archivnictví a spisové službě		
elektronická pošta	dostupnost a bezpečnost základní komunikační platformy	kvestorka		služba	vysoká	střední	střední				backoffice organizace	
16.8 Poskytování služby cloud computingu												
Aplikační hosting	poskytování hostingu pro menší školy			služba	vysoká	vysoká	střední					nedodržení smluvních parametrů
16.9 Poskytování služby datového centra												
Serverový hosting	poskytování hostingu na serverovnách ZČU jiným subjektům			služba	střední	střední	střední					nedodržení smluvních parametrů
16.14 Poskytování řízené bezpečnostní služby												
KIVS/CMS pro IS/STAG	komunikace se státní infrastrukturou pro			služba	vysoká	vysoká	střední					nedodržení smluvních parametrů
19.1 Výzkum a vývoj												
výzkumná data v centrální správě	zpracování a uložení výzkumných dat v centrální správě	PR-V		informace	střední	vysoká	střední			dle typu výzkumu a partnerů		smluvní výzkum - pokuty
výzkumná data	zpracování a uložení výzkumných dat ve správě součástí			informace	střední	vysoká	střední			dle typu výzkumu a partnerů		
výzkumná data	zpracování a uložení výzkumných dat ve správě součástí			informace	střední	vysoká	střední			dle typu výzkumu a partnerů		
výzkumná data	zpracování a uložení výzkumných dat ve správě součástí			informace	střední	vysoká	střední			dle typu výzkumu a partnerů		
výzkumná data	zpracování a uložení výzkumných dat ve správě součástí			informace	střední	vysoká	střední			dle typu výzkumu a partnerů		
výzkumná data mimo centrální správu	ostatní úložiště pod osobní kontrolou pracovníků	PR-V		informace	střední	střední	nízká			dle typu výzkumu a partnerů		
Podpůrná aktiva												
WEBnet	počítačová síť WEBnet včetně internetové konektivity	ředitelka CIV		technické	vysoká	střední	střední		409/2025 příloha 1 - Vazba na primární aktiva			
Serverovny a HW	technická zařízení infrastruktury IT včetně samotných serveroven	ředitelka CIV		technické	vysoká	střední	vysoká		všechna primární aktiva			
SW infrastruktura	centrálně spravovaný SW, servery i stanice	ředitelka CIV		technické	vysoká	vysoká	vysoká		aktiva typu služba			
Lidské zdroje	dostatek kvalifikovaných IT pracovníků	ředitelka CIV		zaměstnanec	střední	střední	vysoká		všechna primární aktiva			
KB procesy	funkční procesy pro provozní KB	ředitelka CIV		zaměstnanec	vysoká	vysoká	vysoká		všechna primární aktiva			
KB nástroje	moderní nástroje pro efektivní řízení KB	ředitelka CIV		technické	vysoká	vysoká	vysoká		všechna primární aktiva			

Potřeby

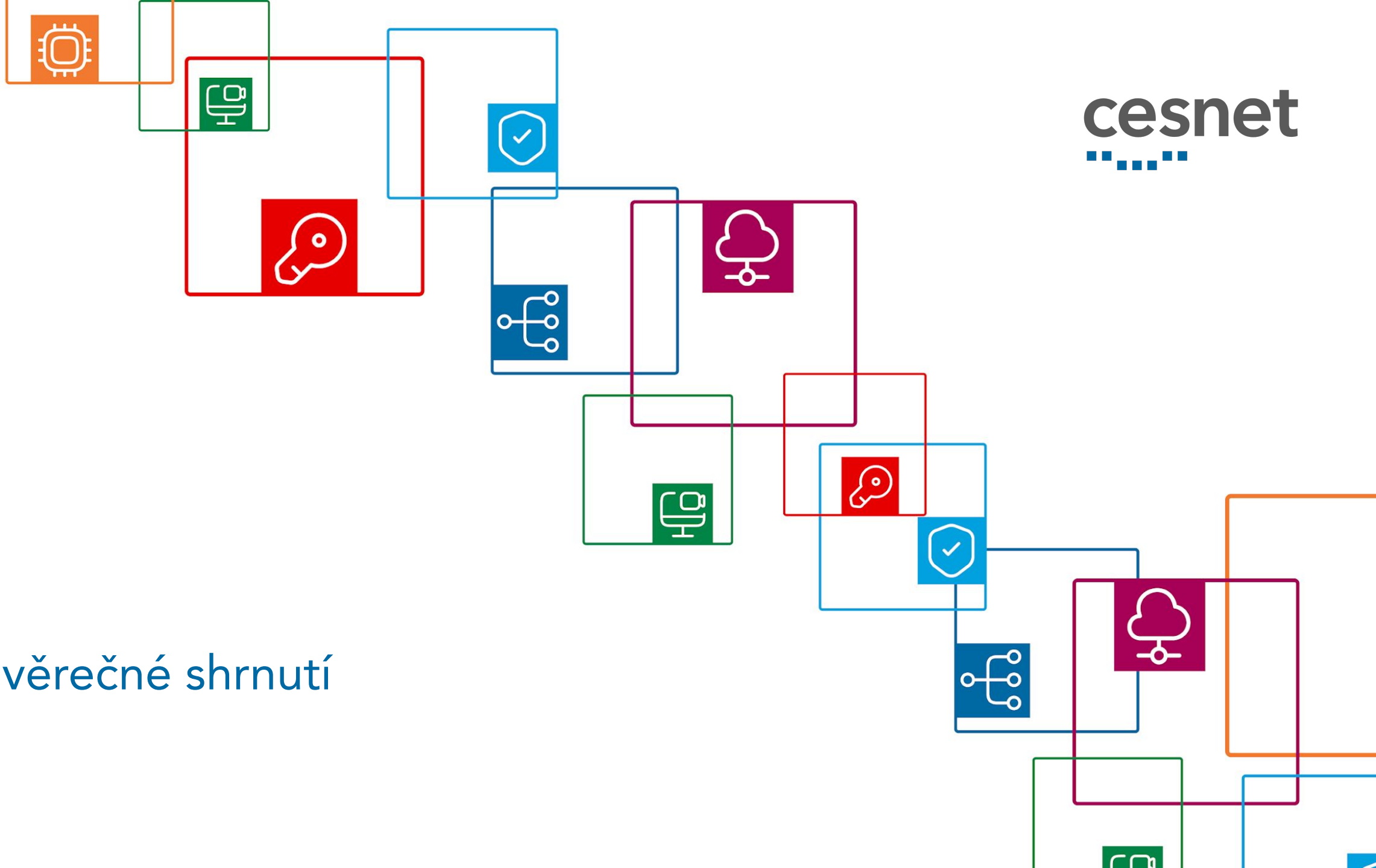
- tvorba pravidel
 - příprava politiky řízení aktiv a dalších dokumentů,
 - je třeba prodiskutovat a implementovat potřeby řízení KB i správců aktiv
- proškolení rolí
 - doložit, že garanti byli po určení proškoleni (obměna funkcionářů)
- komunikační kanál MKB (aktualizace dat, provedení analýzy rizik...)
- úložiště související dokumentace a odkazů

Řešení

- kurz v Moodle
 - zapsání všichni garanti a techničtí správci
 - články k základním tématům, politika řízení aktiv, odkazy na návody
 - možnost povinného absolvování některých částí
 - auditní záznam o absolvování
 - fórum jako diskuzní prostor, Q&A, e-mailová oznámení
- doplněno dle potřeb individuálním nebo skupinovým setkáním/seminářem



Závěrečné shrnutí



1. regulované služby
 - a. samoidentifikace
 - b. ohlášení regulovaných služeb
 - c. registrace regulovaných služeb
2. stanovení rozsahu řízení KB
 - a. identifikace všech aktiv
 - b. výběr evidovaných aktiv
 - c. vyloučení vybraných aktiv + zdůvodnění
3. určení garantů aktiv
4. analýza rizik + definice opatření
5. dokumentace a školení
 - a. metodika určování a hodnocení aktiv
 - b. školicí materiály pro guaranty a další role



1. přezkoumání regulovaných služeb
2. přezkoumání rozsahu řízení KB
3. aktualizace evidovaných aktiv a jejich garantů
4. kontrola opatření předchozího roku
5. aktualizace rizik
6. návrh nových opatření
7. související dokumentace (ke všem krokům)



Děkuji za pozornost

borik@cesnet.cz