MUNI
ICS

Softwarový nástroj pro zavádění SŘBI v akademickém prostředí

Mgr. Jakub Sauer, Vedoucí pracoviště Řízení bezpečnosti informací

Masarykova univerzita – kontext organizace

- 2. největší univerzita v České republice
- 10 fakult a 2 vysokoškolské ústavy
- Přes 7 000 zaměstnanců a 30 000 studentů
- 13,7 mld. pro rok 2025 (11,8 mld. pro rok 2024)

MUNI ICS

Masarykova univerzita – kontext organizace

- Složitá vnitřní organizační struktura
  - velký počet rolí
  - 1 osoba zastává několik rolí
- Velká autonomie jednotlivých součástí s prvky centrálního řízení rektorátem
- Velká provázanost se zahraničními organizacemi
  - sdílení dat
  - přístup osob
- Velká různorodost fyzických objektů (vlastní správa / externí správa)
- Centrální IT služby / využívání IT služeb externě (bez dohledu centrálního pracoviště pro IT)

MUNI ICS

Masarykova univerzita – SŘBI

- Problém uchopit běžnými přístupy pro řízení bezpečnosti informací (velké množství aktiv, rizik, nesystémové zavádění bezpečnostních opatření)
- Snaha o vlastní koncept založený na
  - Vhodné agregaci aktiv
  - Vhodném řízení rizik
  - Zapojení jednotlivých organizačních útvarů
  - Minimalizace administrativních nákladů

  - Politiky, metodiky, bezpečnostní dokumentace a její evidence, školení
  - **Nástroj SŘBI a metodika SŘBI**

MUNI ICS

Interní

Nástroj SŘBI – Obecné informace

- Vývoj za podpory **Fondu rozvoje CESNET**
- **Harmonogram**: leden/2024 – prosinec/2025, zveřejnění leden 2026
- **5 spolupracujících VVŠ**
  - AVU, ČZU, UPCE, VŠCHT, ZČU
- Vydán jako open-source pod **MIT licencí, TLG 6**
  - **prototyp**
- **Součástí je metodika SŘBI pro vysokoškolské prostředí**

Nástroj SŘBI - Cíl projektu

- Podpora pragmatického přístupu v oblasti řízení KB, reflexe reality
- Soulad s řízením IT
- Integrace do řízení vysoké školy
- Zapojení širšího okruhu osob – ne ONE Man show

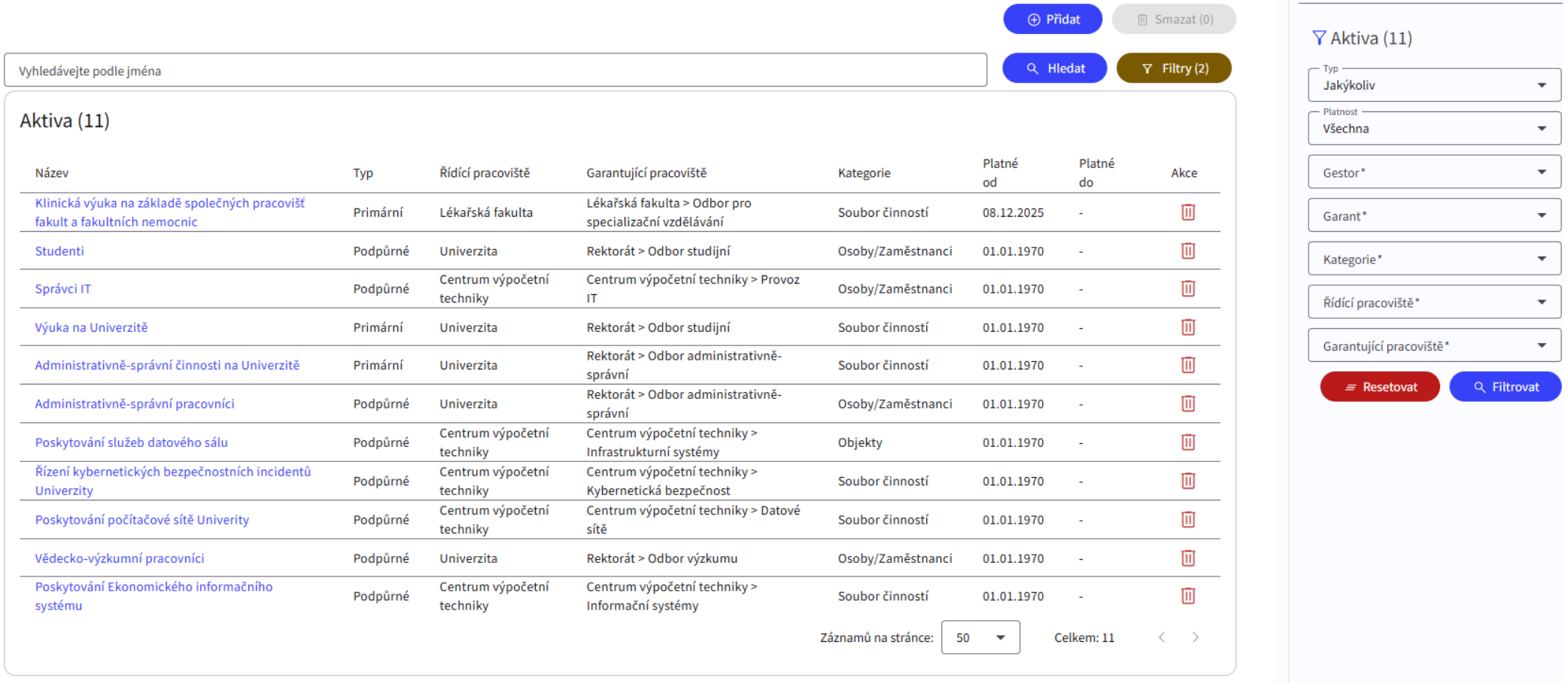
- Kompromis mezi
  - otevřeným prostředím
  - zvýšením úrovně kybernetické bezpečnosti
  - optimální míra nákladů

MUNI ICS

Nástroj SŘBI

- Pokrývá oblast řízení aktiv a rizik
  - Evidence aktiv, vztahů mezi aktivy, stanovením hodnoty důležitosti, řízení rizik – zpráva o hodnocení rizik a plán zvládání rizik
  - Podpora pro kvalitativní i kvantitativní analýzu rizik
- Ne
  - Komunikační platforma, úložiště bezpečnostní dokumentace (evidence významných dodavatelů, plány kontinuity, ….)
  - Prostor do budoucna?
- Katalogy
  - Součástí v omezené formě, potřeba aby organizace vytvořila / prostor pro budoucí spolupráci

Ukázka aktiv



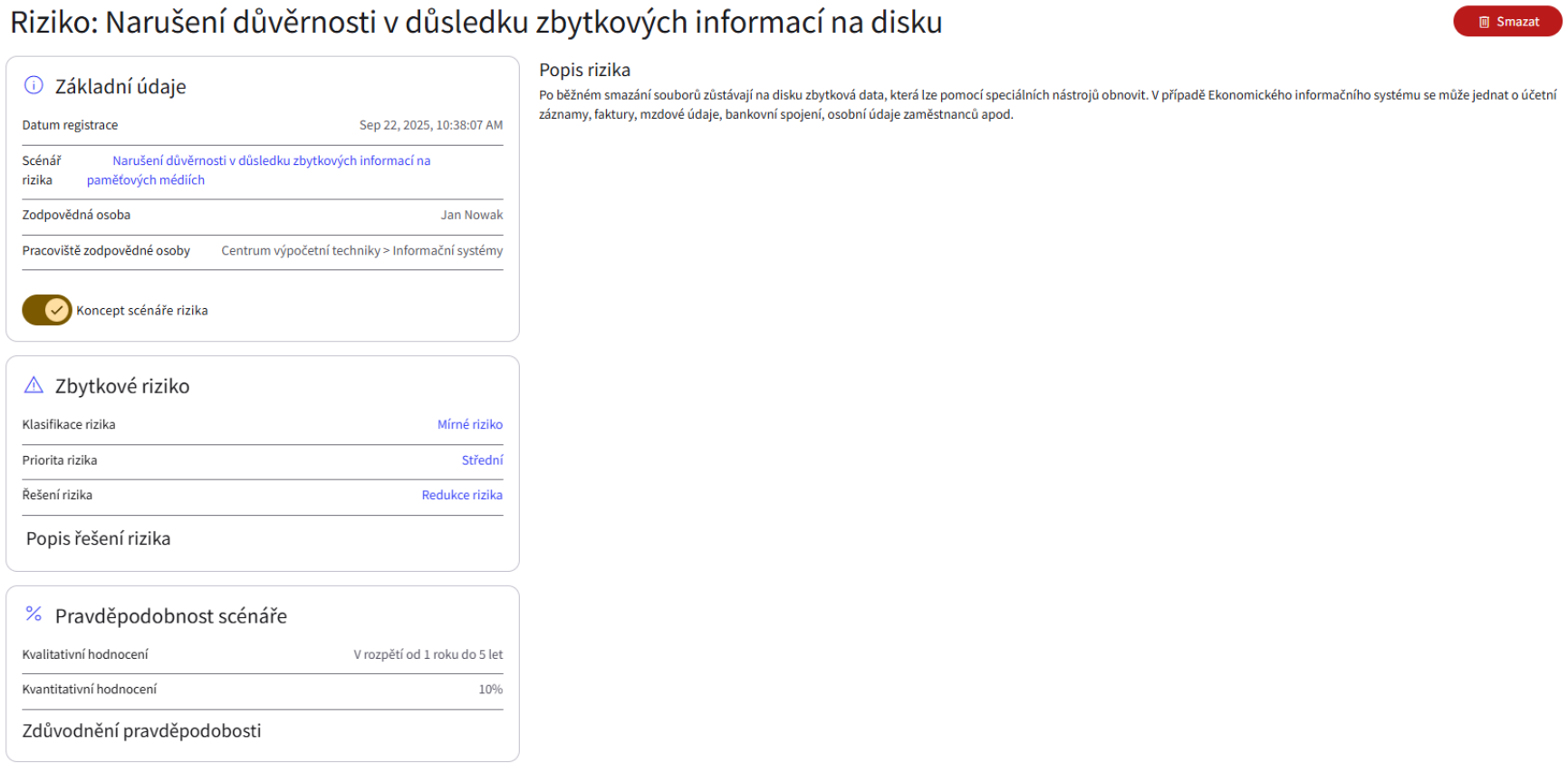
Ukázka stanovení hodnoty důležitosti aktiv

Hodnocení dle kritérií pro úroveň narušení: Narušení dostupnosti > 1 hod

Kritérium	Žádný dopad	Nízká	Střední	Vysoká	Kritická	Kvantitativní hodnocení
Rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů **V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv přímo na subjekty údajů, tedy na jednotlivé osoby, jejichž údaje jsou v daném IS zpracovávány. Jak moc budou jednotlivé osoby po fyzické nebo psychické stránce dotčeny, když budou narušeny jejich osobní údaje.** *Příklad: Únik osobních údajů fyzické osoby z IS (např. o zdravotním stavu apod.) a jejich následné zveřejnění na internetu.*	◉	Může vést k nepohodlí subjektu osobních údajů (podrážděnost, krátkodobé časové nároky pro opětovné zadávání údajů, nutnost další komunikace s organizací). ○	Může vést k menší újmě subjektu osobních údajů (stres, nepohodlí, drobné fyzické obtíže, nedostatek porozumění, omezení přístupu ke službám organizace nebo jiných subjektů, časové nároky spojené s řešením dopadů). ○	Může vést k závažné újmě subjektu osobních údajů (napadení, nepříznivý zdravotní stav, deprese, ztížené uplatnění, ekonomické znevýhodnění (černé listiny), krádež identity, předvolání vyšetřujícími orgány). ○	**Může vést k velmi vážné újmě subjektu osobních údajů, přímému ohrožení či ztrátě života(smrt, invalidita, dlouhodobě nepříznivý zdravotní stav a pracovní neschopnost, ztráta zaměstnání, velmi ztížené uplatnění, vyloučení, omezení práv).** ○	Kvantitativní hodnocení
Rozsah dotčených právních povinností nebo jiných závazků nebo obchodního tajemství **V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na plnění zákonných a smluvních povinností, kterými je organizace zavázána.** *Příklad: • Nemožnost vydání rozhodnutí v zákonné lhůtě z důvodu nedostupnosti IS. • Narušení povinnosti zveřejňovat dokumenty na elektronické úřední desce, která je nepřetržitě dostupná vzdáleným přístupem.*	◉	○	Může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností, např. provozní důvody, nedostatek zaměstnanců. ○	Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody. ○	**Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.** ○	Kvantitativní hodnocení

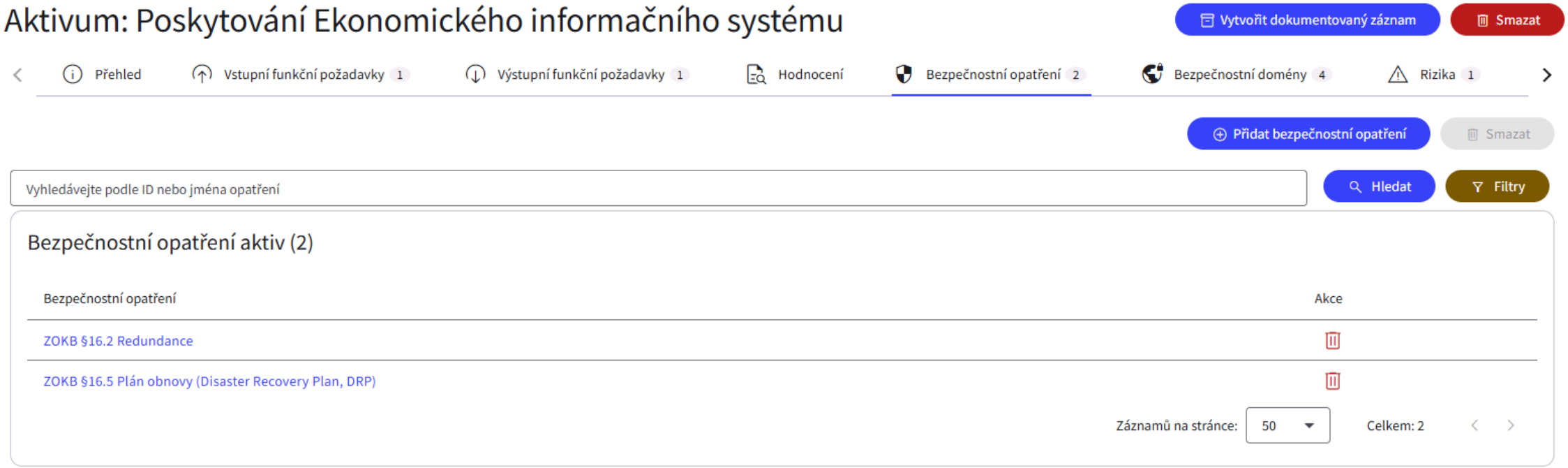
MUNI ICS

Ukázka rizikového scénáře



MUNI ICS

Ukázka bezpečnostních opatření



MUNI ICS

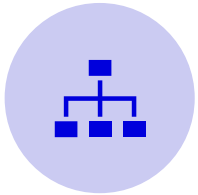
Interní

Principy a východiska nástroje SŘBI

- Zachyceno v metodice SŘBI
- Popsání zákonných povinností
- Ukázka implementace do vysokoškolského prostředí

Metodika SŘBI pro vysokoškolské prostředí – Zohlednění PDCA cyklu SŘBI

Zavádění SŘBI (hlášení regulovaných služeb, stanovení rozsahu SŘBI, stanovení cílů SŘBI)



Ustanovení SŘBI (vhodná tvorba směrnic, strategie implementace SŘBI)

Řízení aktiv (mapování aktiv, obecná „celouniverzitní“ aktiva / lokální aktiva, stanovení dopadu, stanovení bezpečnostních domén, stanovení závislostí)

Řízení rizik (rizikové scénáře, proces řízení rizik, zpráva o hodnocení rizik, plán zvládání rizik)

Provozování SŘBI (nastavení pravidel pro provoz – komunikace, uchovávání dokumentace, zapojení Nástroje SŘBI)

Přezkoumání SŘBI (zapojení vedení, identifikace neshod, zpráva o přezkoumání)

Neustále zlepšování SŘBI (řízení neshod, příležitostí)

MUNI ICS

Klíčové části metodiky / nástroje SŘBI - struktura rolí

- Dostatečná variabilita pro organizaci
  obecný návrh s ohledem na zkušenosti řešitelského týmu

Výbor KB – řeší systémová rizika a doporučuje rozhodnutí vedení

Manažer KB – metodické řízení, pokyny, reporting, komunikace s dohledem

Architekt KB – mapuje požadavky ZoKB na aktiva, návrh opatření

Garant aktiva – odpovědnost za rizika, opatření a implementaci

Gestor KB – schvaluje rizika, zajišťuje zdroje (zástupce součásti)

Auditor KB – nezávislé ověření účinnosti opatření

Pověřenec KB – podpora při outsourcingu MKB, interní komunikace)

MUNI ICS

Interní

Klíčové části metodiky / nástroje SŘBI - aktiva

Obecná aktiva –zastřešují běžné vysokoškolské činnosti, role, objekty běžně se vyskytující na vysoké škole

- Plošná zabezpečení
- Garant aktiva – bezpečnostní tým
- Gestor KB – vedení vysoké školy
- **Plošná pravidla pro všechny nezávisle na organizačním útvaru**

Lokální aktiva

- Opt-out z obecných aktiv / zohlednění specifické činnosti
- Garant aktiva – součást / organizační útvar
- Gestor KB – vedení součásti / organizačního útvaru + informování bezpečnostního týmu
- **Vydávaná pravidla pro jasně vymezený organizační útvar**

MUNI ICS

Interní

Jak to bude vypadat?

Proběhne určení obecných aktiv

Obecná aktiva komunikována s vybranými organizačními útvary - následná revize

- Stanovených charakteristik
- Nastavené důležitosti
- Závislostí - jaké ICT prvky, objekty, kategorie osob, dodavatelé jsou zapojení

V případě odlišného názoru organizačního útvaru / velké specifikaci aktiva – vznik lokálního aktiva

MUNI ICS

Interní

Klíčové části metodiky / nástroje SŘBI - soubory činností a bezpečnostní domény

Soubor činností

- Aktivum, které umožní podle potřeby seskupovat zpracovávaná data a informace, fyzické objekty, činnosti zaměstnanců, poskytování plnění dodavatelů i informační technologie do logických celků

Bezpečnostní domény

- Způsob, jak z pohledu KB přehledně a transparentně popsat aktivum – přiřadit mu rizikové scénáře a bezpečností opatření vycházející ze zákona a to na základě charakteristiky aktiva

MUNI ICS

Interní

Jak fungují bezpečnostní domény / ošetření rizik ?

Garant aktiva
Detailní popis aktiva

↓

Manažer KB / Architekt KB
Určení bezpečnostních domén charakterizujících aktivum
[*Řízení kontinuity činností, Bezpečnost lidských zdrojů, …*]

↓

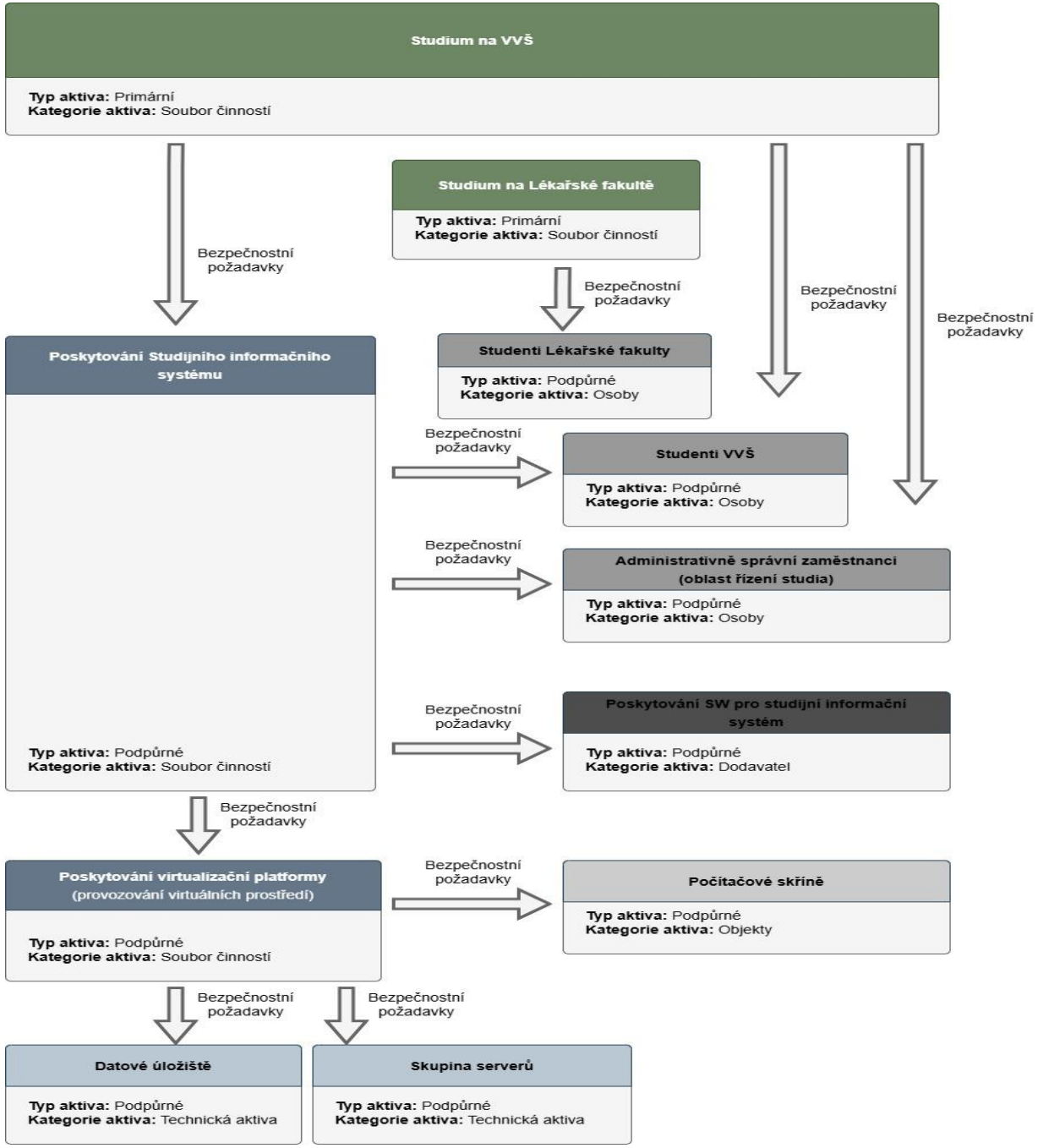
Garant aktiva
Vybere a specifikuje relevantní rizikové scénáře z určených bezpečnostních domén aktiva
[př. *Narušení dostupnosti kritických cloudových služeb, …*]
Výběr a specifikace relevantních bezpečnostních opatření z určených bezpečnostních domén aktiva mitigujících vybrané rizikové scénáře.
[*Plán kontinuity činností (BCP), Plán obnovy (DRP), …*]

↓

Gestor KB
Schvaluje způsob vypořádání s rizikem + informuje manažera KB, dotčené garanty aktiv a gestory KB

MUNI
ICS

Ukázka struktury aktiv



Zveřejnění

KDY

JAK

MUNI ICS

Závěr

- Děkuji za pozornost!
- Diskuze

sauer@ics.muni.cz

MUNI ICS