SARA

Softvér na analýzu rizík

SYNCHRONIX, a.s.
Jaroslav Plaček

iDEME
21.6.2023

Agenda

1) Riadenie rizík v kybernetickej bezpečnosti
2) Evidencia a hodnotenie aktív
3) Preskúmanie a analýza rizík - hrozby, zraniteľnosti, opatrenia
4) Legislatíva pre kybernetickú bezpečnosť v SR
5) SARA – predstavenie nástroja
6) SARA – evidencia a hodnotenie aktív, analýza rizík
7) SARA – dashboard, reporty, konfigurovateľnosť
8) Aké výhody prináša používanie aplikácie SARA?

Ciele kybernetickej bezpečnosti

Chrániť dôvernosť, dostupnosť a integritu (informačných) aktív.

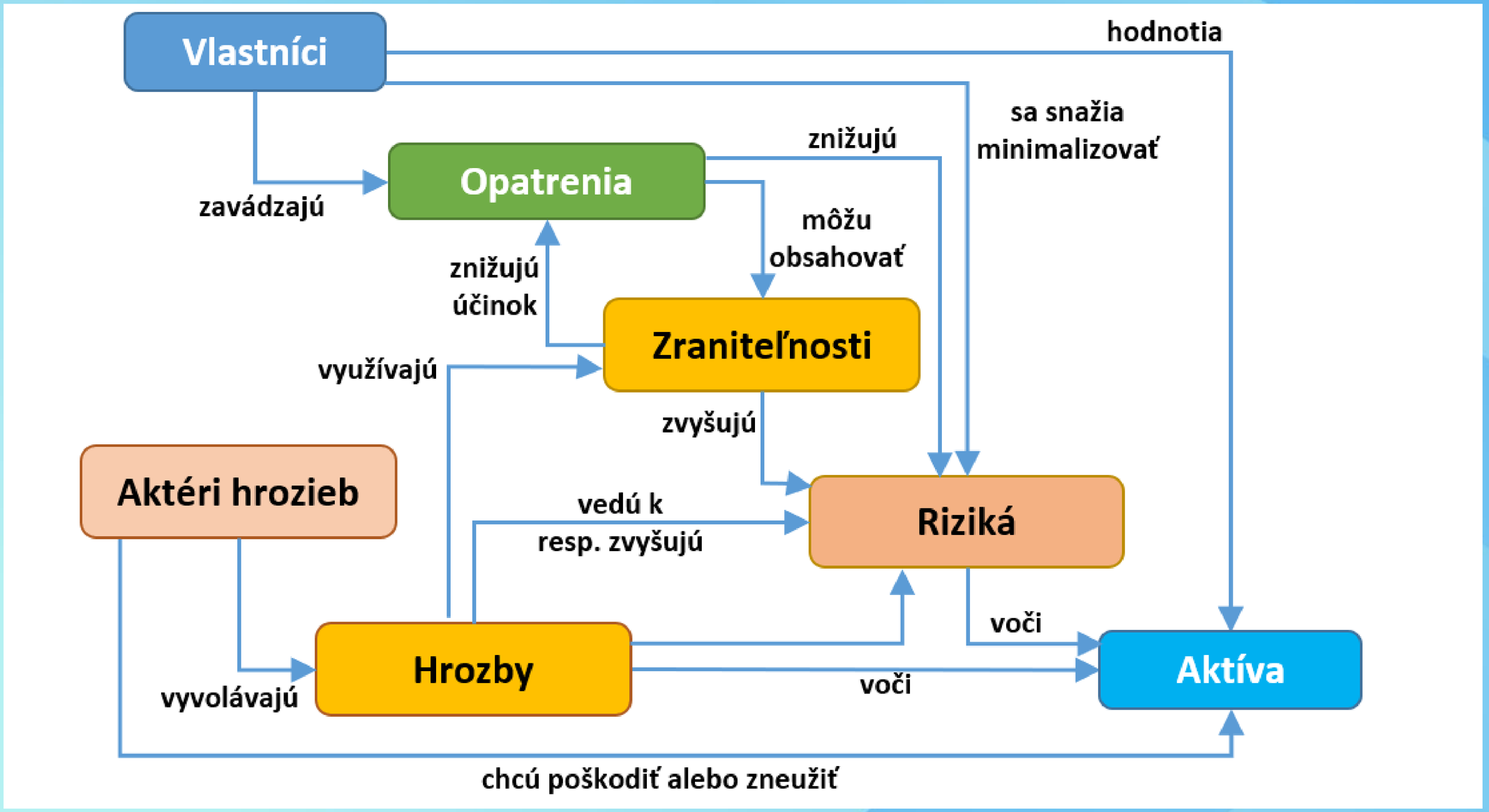
Aktíva – informácie, aplikácie, počítače, mobilné zariadenia, siete a pod.

Kybernetická bezpečnosť sa zameriava na ochranu troch vlastností aktív:

Dôvernosť – informačné aktíva sú prístupné len autorizovanému personálu
Dostupnosť – informačné aktíva sú dostupné v určenom čase
Integrita – informácie sú správne, úplné, môžu ich meniť len autorizované osoby

Požiadavky na bezpečnosť určuje **Vlastník aktíva** (business owner, garant aktíva)

Riadenie rizík kybernetickej bezpečnosti



Výpočet rizika, vysporiadanie sa s rizikom

Preskúmanie rizík: identifikácia scenárov + analýza (výpočet úrovne) rizík

Výška rizika = Dopad x Hrozba x Zraniteľnosť

Dopad
závisí od
hodnoty aktíva
(finančný, zdravotný, reputačný, ...)
- zmierňujú ho opatrenia

x

Hrozba
pravdepodobnosť =
Existencia aktéra x
Motivácia aktéra x
Potrebné znalosti x
Potrebné prostriedky
- zvyšujú ju **zraniteľnosti**
- znižujú ju opatrenia

=

Veľkosť rizika

Zanedbateľné
Nízke
Stredné
Vysoké
Veľmi vysoké

Akceptovanie

Zníženie
(opatrenia = €)

Prenesenie
(poistenie)

Vyhnutie sa riziku
(prestanem aktívum využívať)

Spôsoby evidencie aktív a preskúmania rizík

Zoznam aktív – zaužívané spôsoby evidencie:

- Papierová evidencia
- Export z ERP systému (účtovaná/majetková evidencia?)
- Excel - zoznam aktív vrátane ich ohodnotenia, úroveň detailu je rôzna, niekedy sú hodnotené len triedy aktív – servery, notebooky, aplikačný SW
- ServiceDesk resp. CMDB („konfiguračná databáza“)
- Evidenčné listy vypracované pri nahlásenníinformačného systému na NBÚ

Preskúmanie rizík

- Najčastejšie Excel – rôzne metodiky (jednoduché, zložitejšie)
- Zriedkavejšie sa používajú aj špecializované programy, najmä ak AR vypracuje dodávateľ v rámci poskytovania konzultačných služieb. Organizácia má k dipozícii často len finálne výstupy vo forme PDF, WORD, Excel bez možnosti zmien.

Legislatíva SR

- **Zákon č. 69/2018 o kybernetickej bezpečnosti**
- Platí pre poskytovateľov základných služieb (PZS), t.j. vrátane miest a obcí

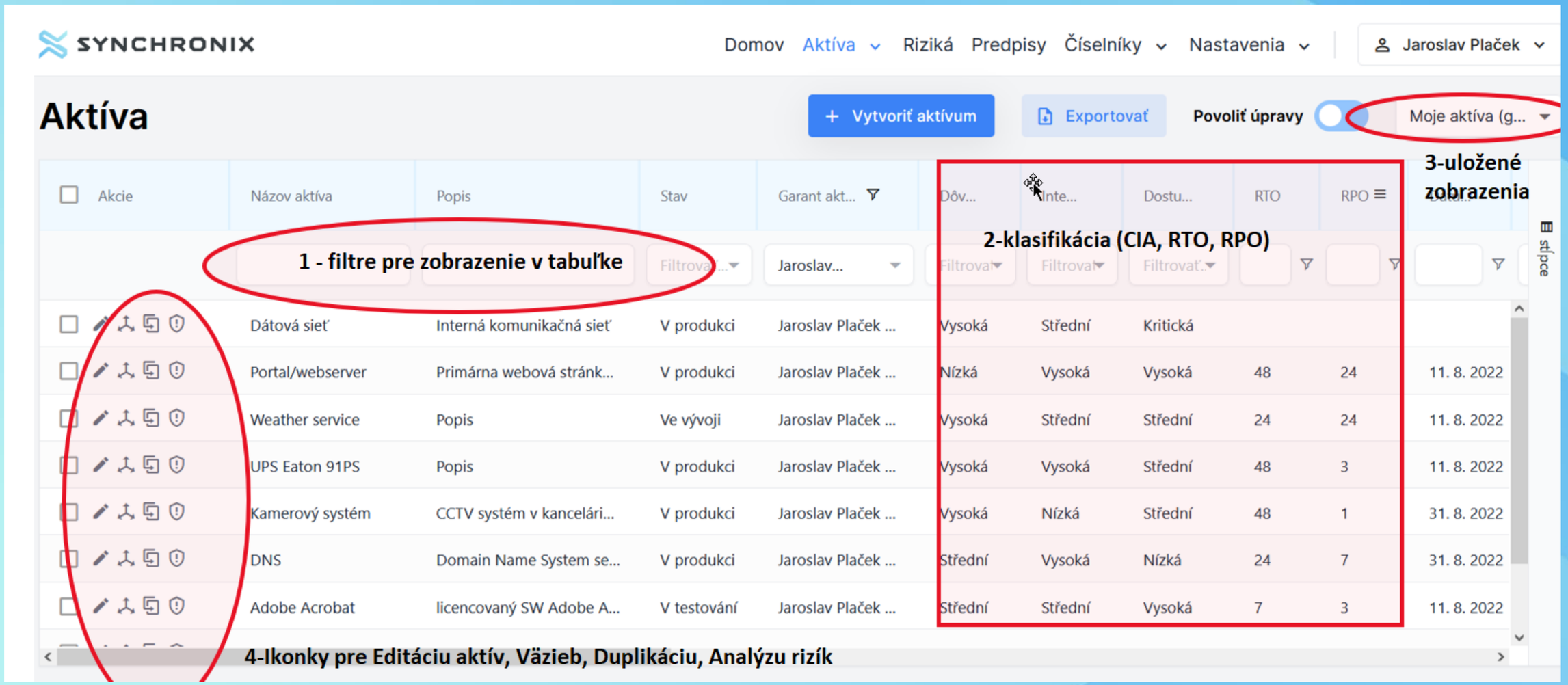
- **Vyhláška č. 362/2018**
  - **Klasifikácia** informácií, **Kategorizácia** sietí a informačných systémov
  - **Analýza rizík**
  - **Obsah a štruktúra** dokumentácie, **Bezpečnostné opatrenia**

- **Vyhláška č. 165/2018** – kategórie incidentov, spôsob nahlasovania
- **Vyhláška č. 179/2020** – bezpečnostné opatrenia pre IS VS

SARA – Softvér na Analýzu Rizík

Pre koho je softvér určený?		
Pre ľudí, ktorí sa podieľajú na zabezpečení informačných aktív - **manažéri KB, bezpečnostní špecialisti, vlastníci / garanti aktív, správcovia aktív, experti na riadenie rizík, audítori**.		
SARA nám pomôže evidovať a odhaliť:		
Čo a ako dôkladne to mám chrániť?	**Evidencia, Klasifikácia, Reporty pre vlastníkov**	Manažér KB (Tímy KB) Vlastníci/garanti aktív
Ako to mám chrániť? **Na čo si dať pozor?**	**Opatrenia pre aktíva** **Zraniteľnosti**	Manažér KB, Správca aktíva, Externý dodávateľ
Kde sú moje slabé miesta? **Ako som na tom a ako situáciu zlepšiť?**	**Úroveň rizík** **Register rizík** **Navrhované opatrenia**	Manažér KB, Riadenie rizík, Správca aktíva Audítor
Dôkazy o plnení povinností / audit	**Read-only prístup, reporty**	Interný / externý auditor
Ako sa mení situácia v čase	**Dashboardy**	Manažér KB, Vedenie spoločnosti

Evidencia a hodnotenie aktív



V tabuľkovom zobrazení je možnosť hromadnej editácie aktív

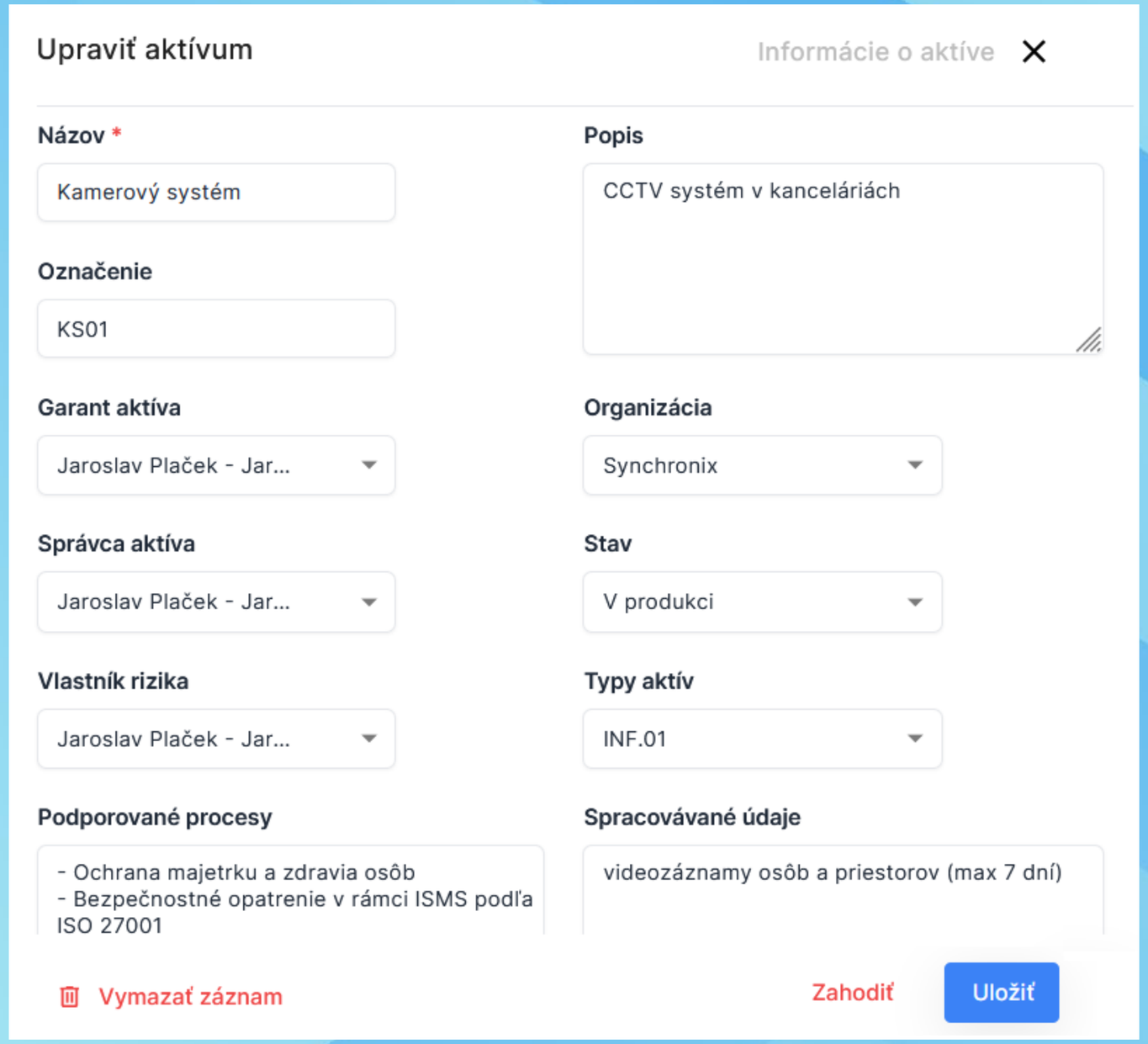
Detail aktíva

- **Názov, popis**
- **Vlastník aktíva, Správca**

- **Dôvernosť, Dostupnosť, Integrita**

- **Spracovávané údaje,**
- **Podporované procesy**
- **Prílohy** (napr. technická správa, bezpečnostný koncept, zmluva s dodávateľom)

- **Dátum klasifikácie / analýzy rizík**
- **Uloženie záznamu klasifikácie do histórie**



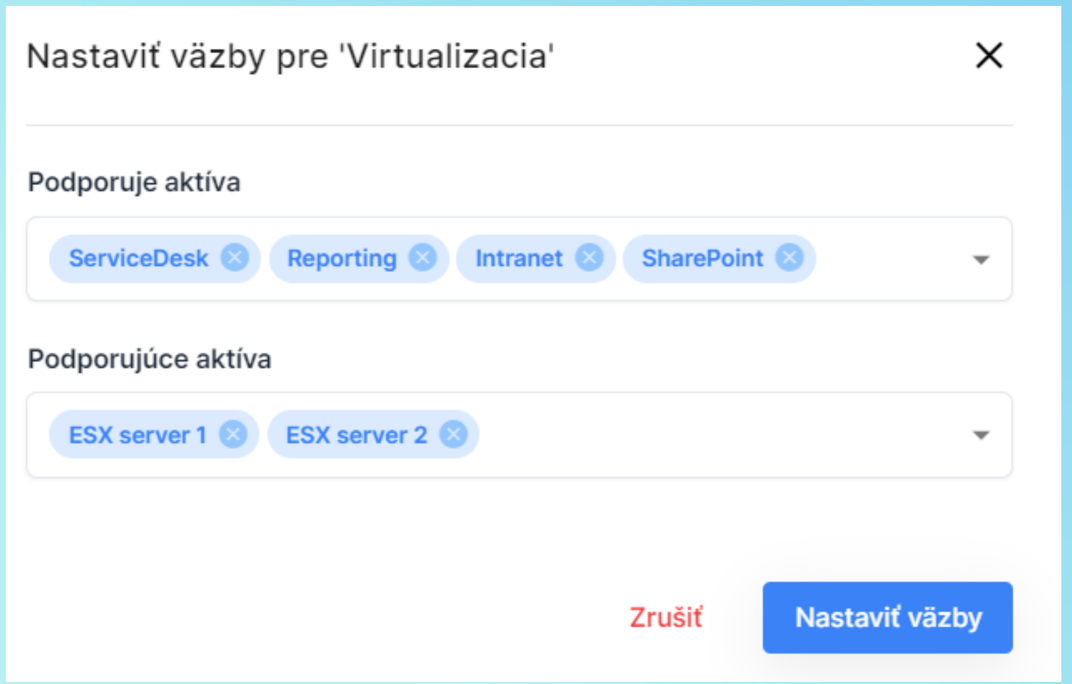
Previazanie aktív a vizualizácia väzieb

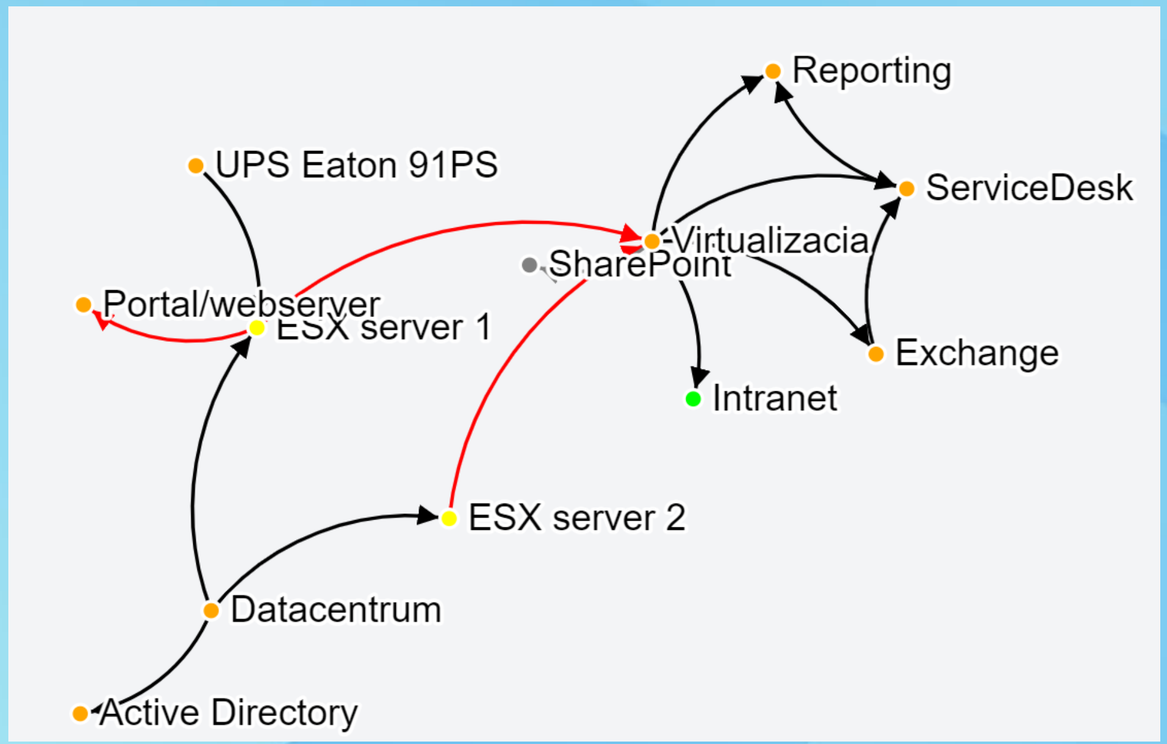
Tvorba väzieb

- každé aktívum môže podporovať a/alebo byť podporované iným aktívom

Vizualizátor:

- grafické znázornenie väzieb
- vyznačenie klasifikácie aktíva
- zobrazenie nesúladu pri klasifikácii aktív a väzbách (červené šípky)





Preskúmanie rizík

Pri vytvorení aktíva sa vytvorí z katalógu hrozieb register rizík pre aktívum (zatiaľ neohodnotených)

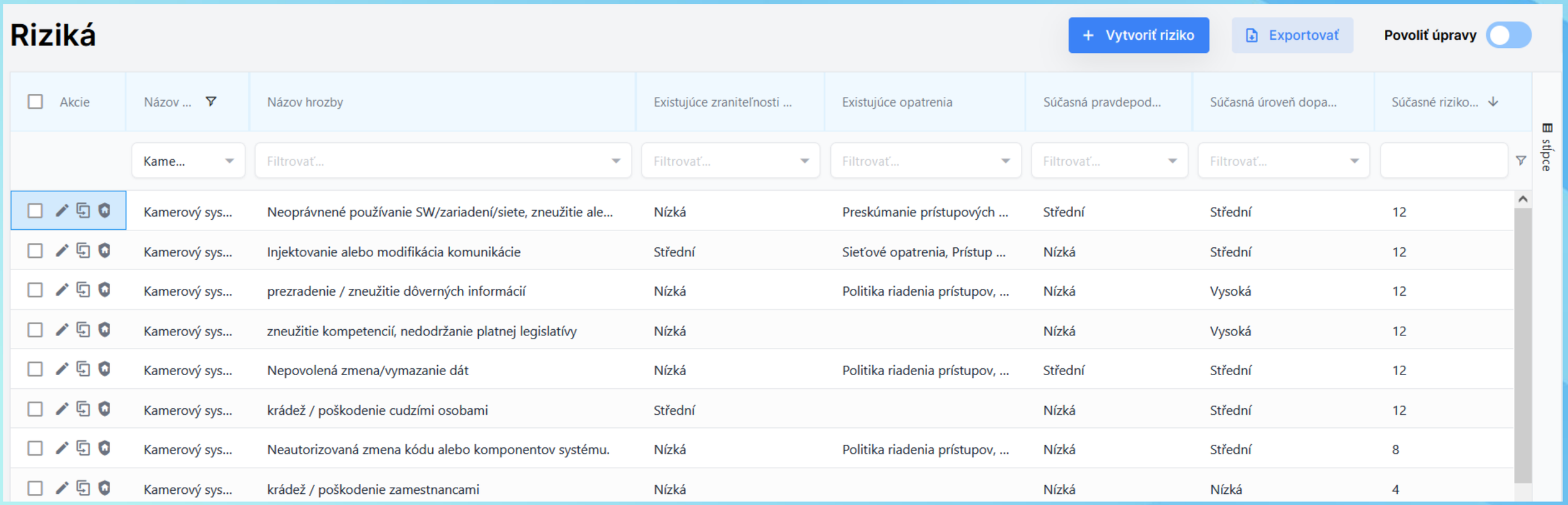
Po zadaní úrovne **dopadu, pravdepodobnosti a zraniteľnosti sa vypočíta číselná úroveň a trieda rizika** (Nízke, Stredné, Vysoké...), čo je vhodné pre reporting, dashboardy, štatistiky, trendy

V detaile pre dané riziko možno uviesť aj **podrobný scenár, existujúce opatrenia alebo zraniteľnosti** z príslušných katalógov

Možné zadať aj navrhované opatrenia a odhadnúť aj budúcu úroveň rizika (vhodné pri vysoké riziká)

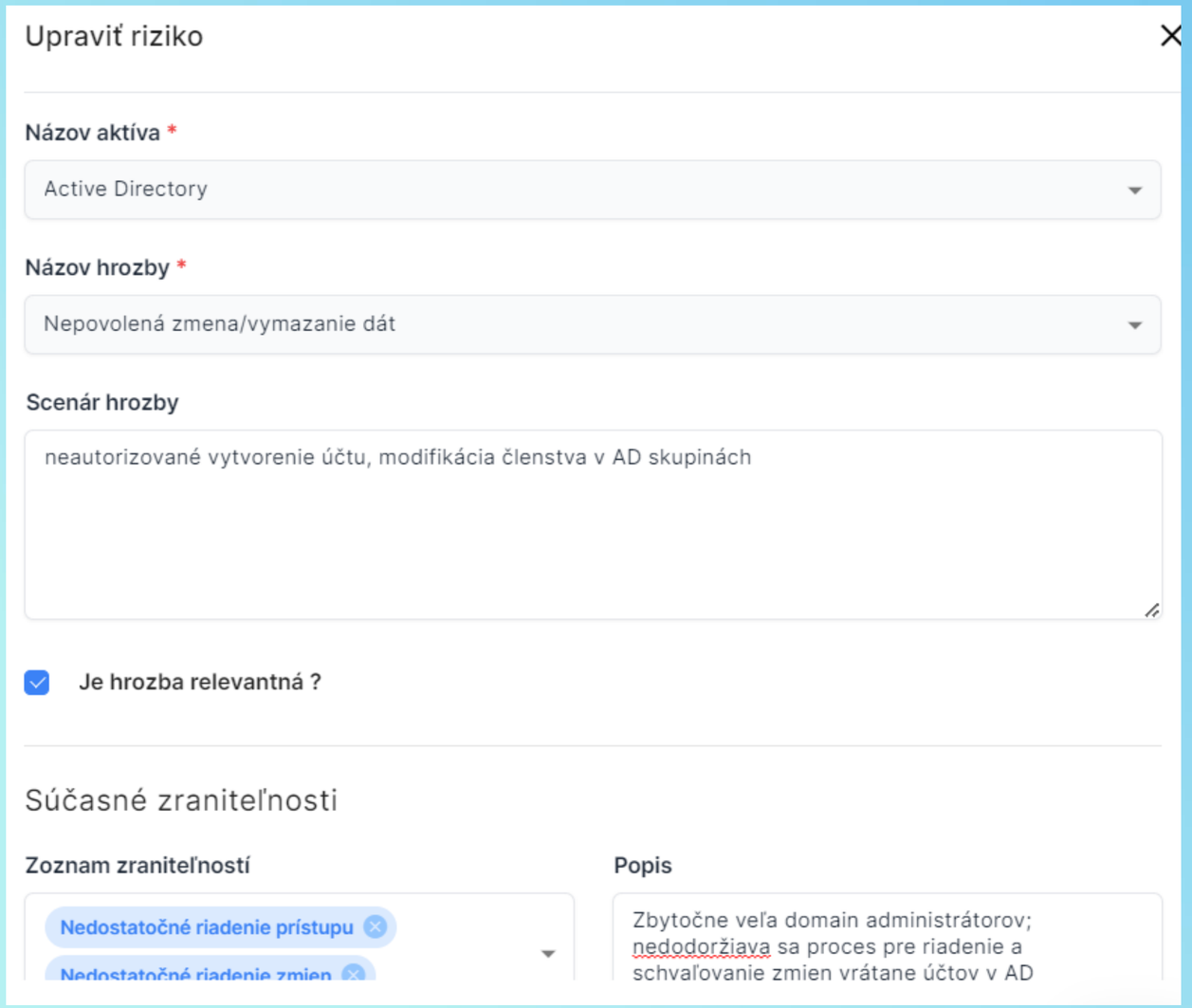
Riziko môžeme zduplikovať (napr. pre odlišné hodnotenie pre rôzne komponenty aktíva, príp. samostatné hodnotenie pre rôzne zraniteľnosti)

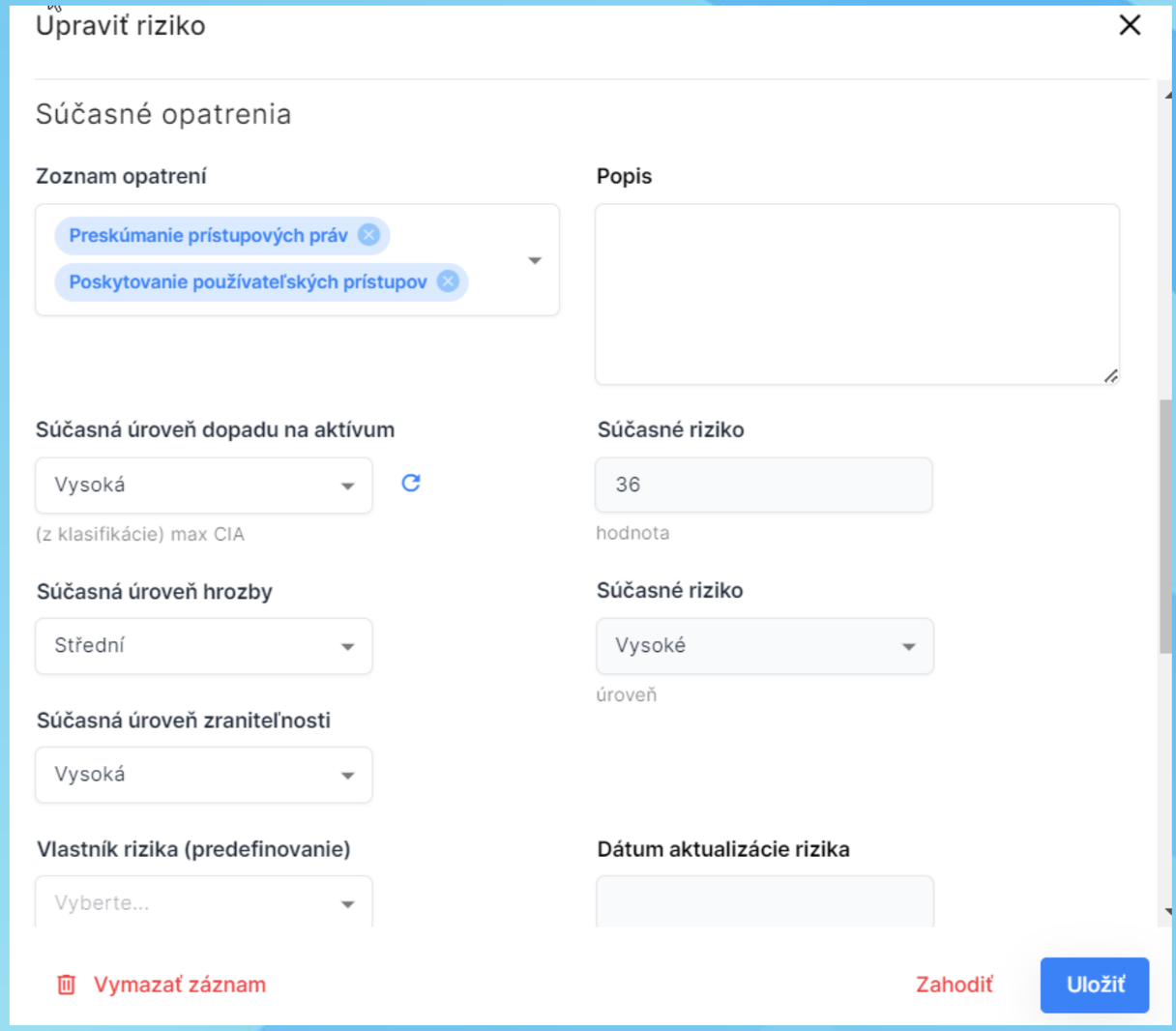
Preskúmanie rizík – tabuľkový prehľad



Podporovaná je editácia buniek podobne ako v tabuľkovom editore (napr. Exceli) alebo v detaile

Detail rizika





SARA – dashboardy, reporty, export

Dashboardy

- kľúčové ukazovatele o stave aktív a rizík
- preklik na tabuľky

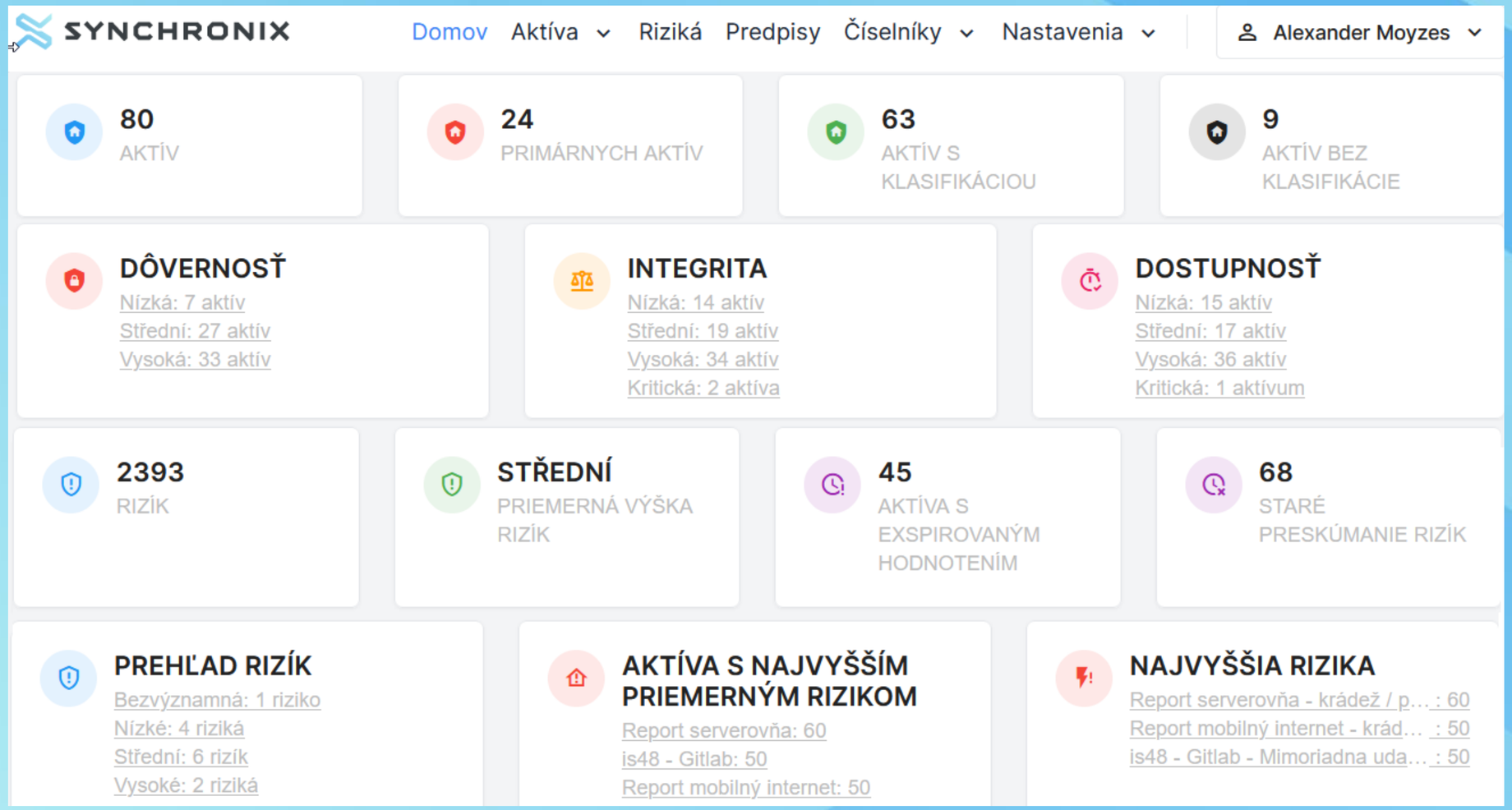
Reporty

Pre vlastníka aktíva:

- klasifikácia aktíva
- sumár analýzy rizík

Pre manažéra KB:

- zavedené opatrenia



Exporty - do csv súborov, dostupné z každého tabuľkového zobrazenia

SARA – zhrnutie funkcionality

- **evidencia a hodnotenie aktív** + časová stopa
- **preskúmanie a hodnotenie rizík** (hrozby, zraniteľnosti, opatrenia) + časová stopa
- **dashboardy** – prehľad o stave, o trendoch, o úlohách (exspirované klasifikácie)
- **reporty** – pre manažéra KB, pre vedenie spoločnosti, pre vlastníkov aktív, audítorov
- **roly používateľov** – manažér, audítor, správca, vlastník
- **zoznam platných predpisov** (legislatíva, interné)
- **evidencia bezpečnostných incidentov**
- **prispôsobiteľnosť aplikácie** (základné číselníky – úroveň pre CIA, dopad, hrozby, zraniteľnosti, výpočet rizika, zoznamy hrozieb, zraniteľností, opatrení a pod.
- **prispôsobenie pre používateľa** (výber zobrazenia stĺpcov, zoraďovanie, filtrovanie, uložené filtre a zobrazenia)
- **3 jazykové mutácie** – SK / EN / CZ

Prečo je výhodné používať SARU?

- **Efektívna editácia údajov o aktívach a ich hodnotení** (možná hromadná „a la“ Excel editácia aktív aj rizík)
- **Analýzy rizík je potrebné vykonávať pre všetky aktíva a prehľadne sumarizovať ich výstupy, ktoré treba priebežne sledovať a aktualizovať** (pri použití samostatných súborov pre analýzy – napr. Excel – sa toto plní veľmi náročne, chýba história)
- **Široká prispôsobiteľnosť aplikácie** (pre veľké aj malé organizácie)**, možné sú rôzne spôsoby využívania** (príprava AR analytikom – výber relevantných hrozieb, samostané vyplnenie AR znalým IT správcom, rýchla analýza všetkých scenárov s následným dôkladným preskúmaním vysokých rizík)
- **Audítorom aj tretej strane je možno poskytnúť dôkaz, že ochrane informačných aktív je venovaná náležitá starostlivosť vrátane zavedených opatrení**
- **Automatizácia výstupov** (napr. príprava reportu pre vlastníka aktíva)

Diskusia

?

SYNCHRONIX