SARA

Softvér pre analýzu rizík

SYNCHRONIX, a.s.
Jaroslav Plaček
iDEME, 20.6.2024

Agenda

1) Prečo potrebujeme takýto SW?
2) Evidencia a hodnotenie aktív
3) Preskúmanie a analýza rizík
4) Aká je bežná prax a ako je to v nástroji SARA
5) Dashboardy, reporty, konfigurovateľnosť
6) Aké výhody prináša používanie aplikácie SARA?

Prečo potrebujeme takýto SW?

Cieľ: Chrániť dôvernosť, dostupnosť a integritu (informačných) aktív.

Kybernetická bezpečnosť sa zameriava na ochranu troch vlastností **aktív**:

Dôvernosť – aktíva/údaje sú prístupné len pre autorizovaných používateľov
Dostupnosť – aktíva sú dostupné v určenom čase
Integrita – informácie sú správne, úplné a môžu ich meniť len oprávnené osoby

Tieto požiadavky určuje **Vlastník aktíva**

Potrebujeme vedieť ČO, PRED ČÍM a AKO INTENZÍVNE máme chrániť, preto vykonáme ANALÝZU RIZÍK, ktorou a identifikujeme najvýznamnejšie hrozby s najväčším dopadom na dôležité aktíva. Vyžaduje to od nás:

- **Zákon č. 69/2018 o kybernetickej bezpečnosti**
- **Vyhláška NBÚ SR č. 362/2018** (Klasifikácia informácií, Kategorizácia sietí a IS, Analýza rizík, Bezpečnostné opatrenia)
- **Norma ISO 27001** - posúdenie a ošetrenie rizík informačnej bezpečnosti (6.1.2, 6.1.3)

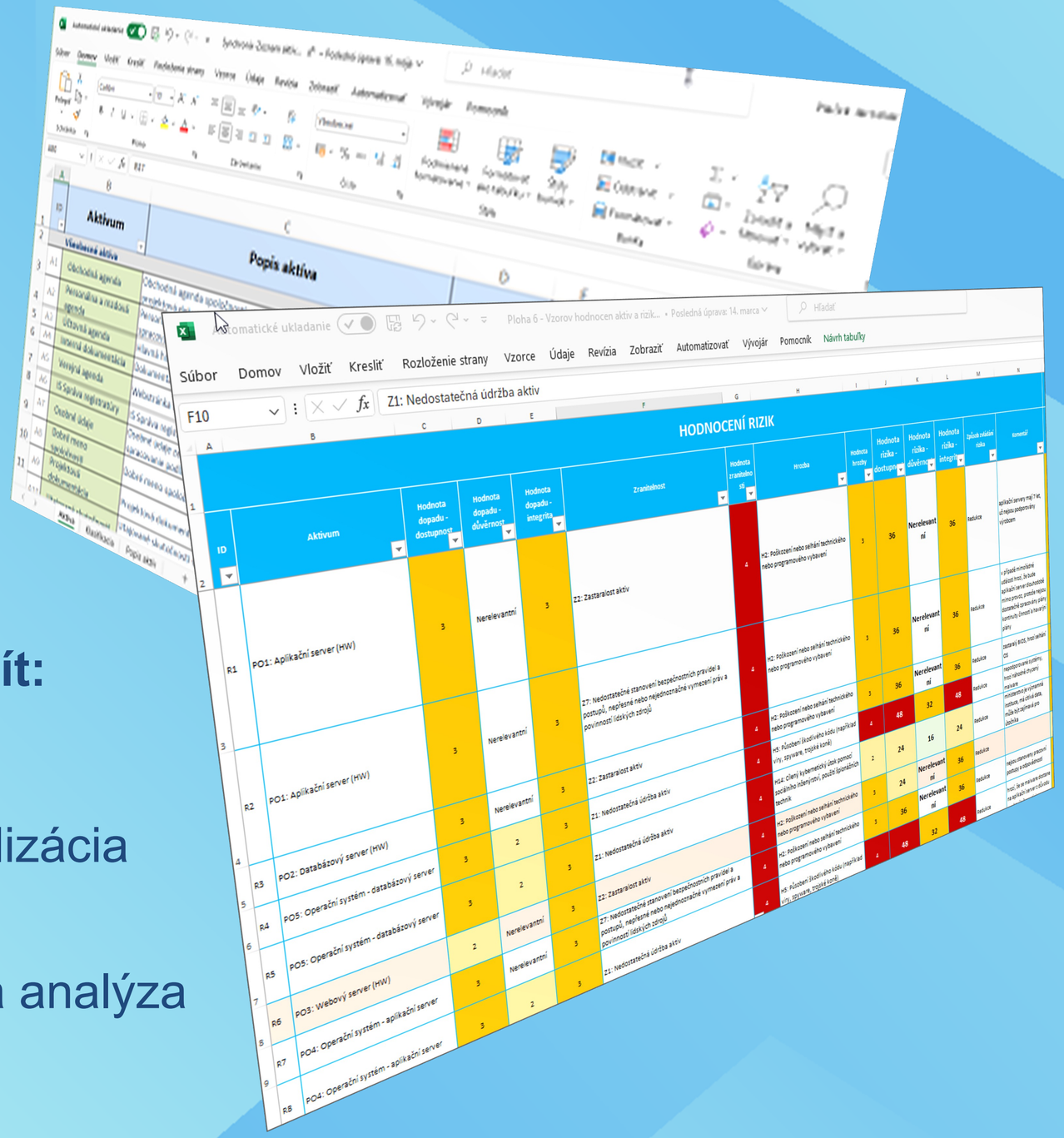
Aká je bežná prax?

Evidencia aktív:
- Excel
- Účtovná evidencia
- ServiceDesk

Analýza rizík:
- Excel – niekedy 1 súbor pre 1 aktívum
- ServiceDesk

Nevýhody Excelu – absencia funkcionalít:
- riadenie prístupových oprávnení
- história a zaznamenávanie zmien
- vytváranie väzieb medzi aktívami, vizualizácia
- reporting

Nevýhody ServiceDesku: zvyčajne chýba analýza rizík a “workflow” pre klasifikáciu



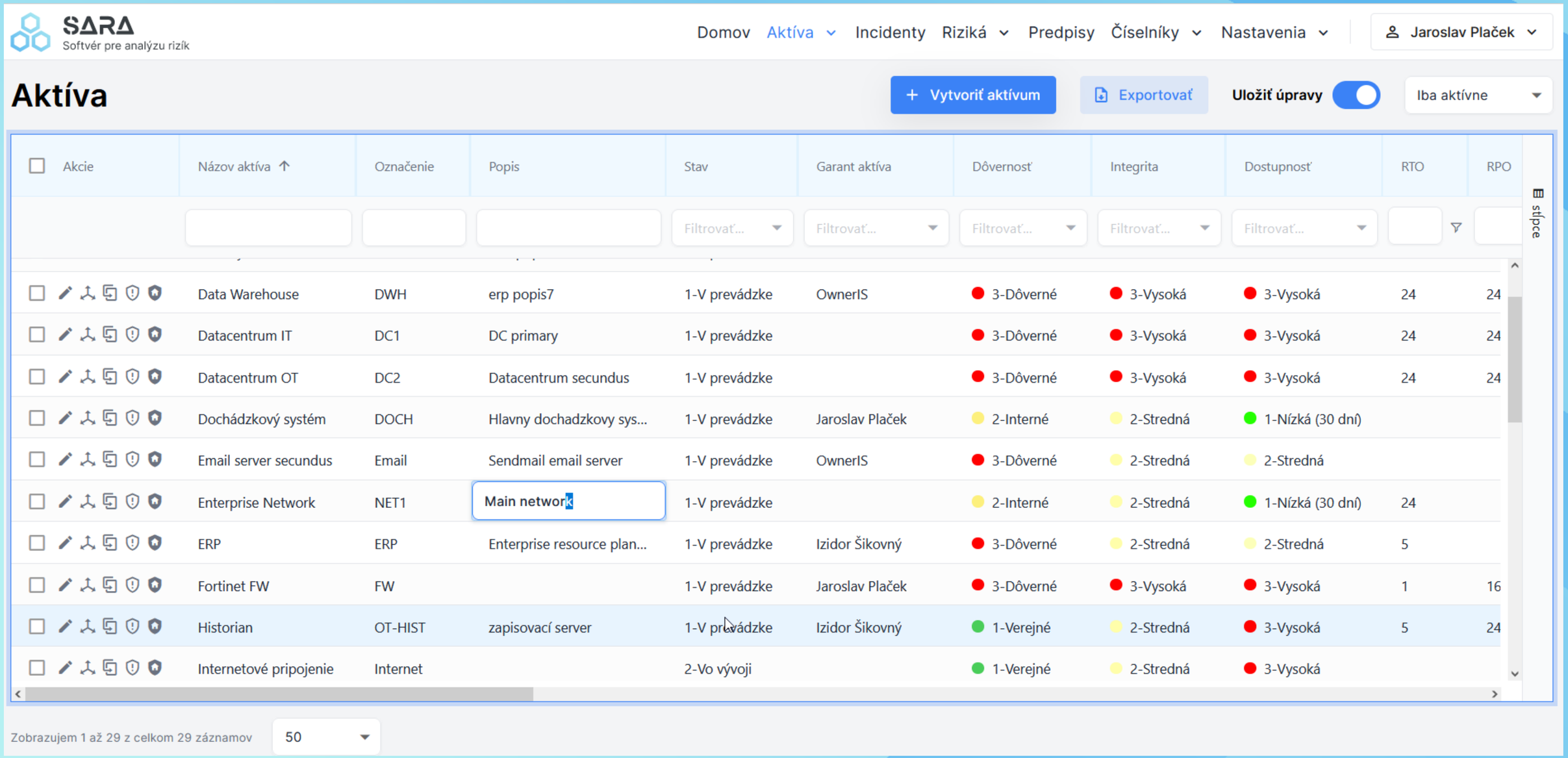
Ako je to v SARA?

Evidencia aktív:
- editovanie možné aj v tabuľke „a la“ Excel (copy / paste funkcia, hromadné úpravy)
- editovanie v detaile aktíva
- možnosť ukladania príloh

Prístupové roly:
- možnosť editovania v závislosti od roly a vzťahu k aktívu, dostupnosť funkcionalít
- Admin, Manažér KB, Vlastník/Správca aktíva, Audítor

História klasifikácií:
- zaznamenávanie vykonania zmien
- uloženie klasifikácie k zvolenému dátumu
- upozornenie na exspirované hodnotenie

SARA - Evidencia aktív



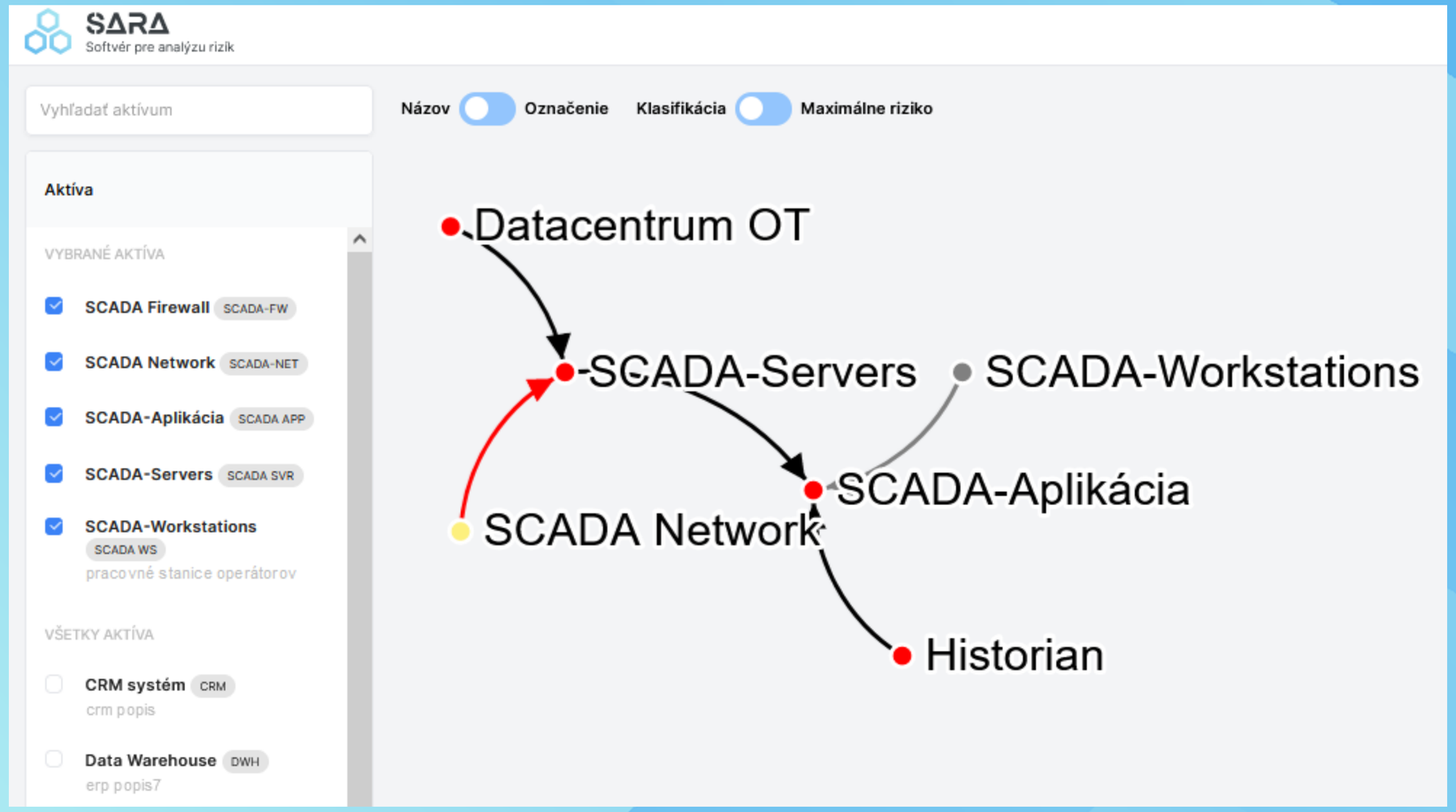
Previazanie aktív a vizualizácia väzieb

Väzby medzi aktívami:

- každé aktívum môže podporovať alebo byť podporované iným aktívom

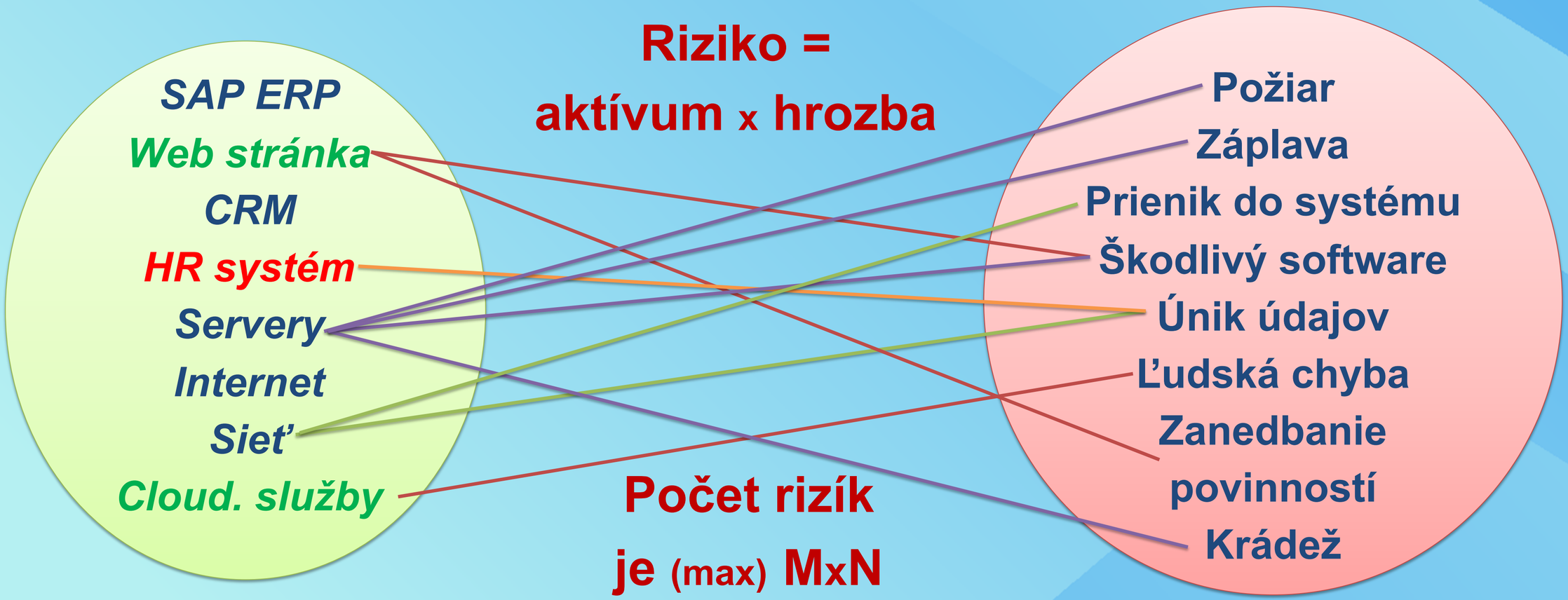
Vizualizátor:

- grafické znázornenie väzieb aktív
- farebné vyznačenie stupňa klasifikácie
- zobrazenie chýbajúcej klasifikácie
- zobrazenie nesúladu klasifikácie aktív



Čo považujeme za riziko?

Ohodnotené aktíva (N)



Príklad: Riziko úniku osobných údajov z HR systému

Výpočet rizika, vysporiadanie sa s rizikom

<u>Preskúmanie rizík</u>: identifikácia rizikových scenárov + analýza rizík (výpočet)

Výpočet výšky rizika = Dopad x Hrozba x Zraniteľnosť

Výsledkom analýzy rizík je hodnota a úroveň rizika

Zanedbateľné | Nízke | Stredné | Vysoké | Kritické

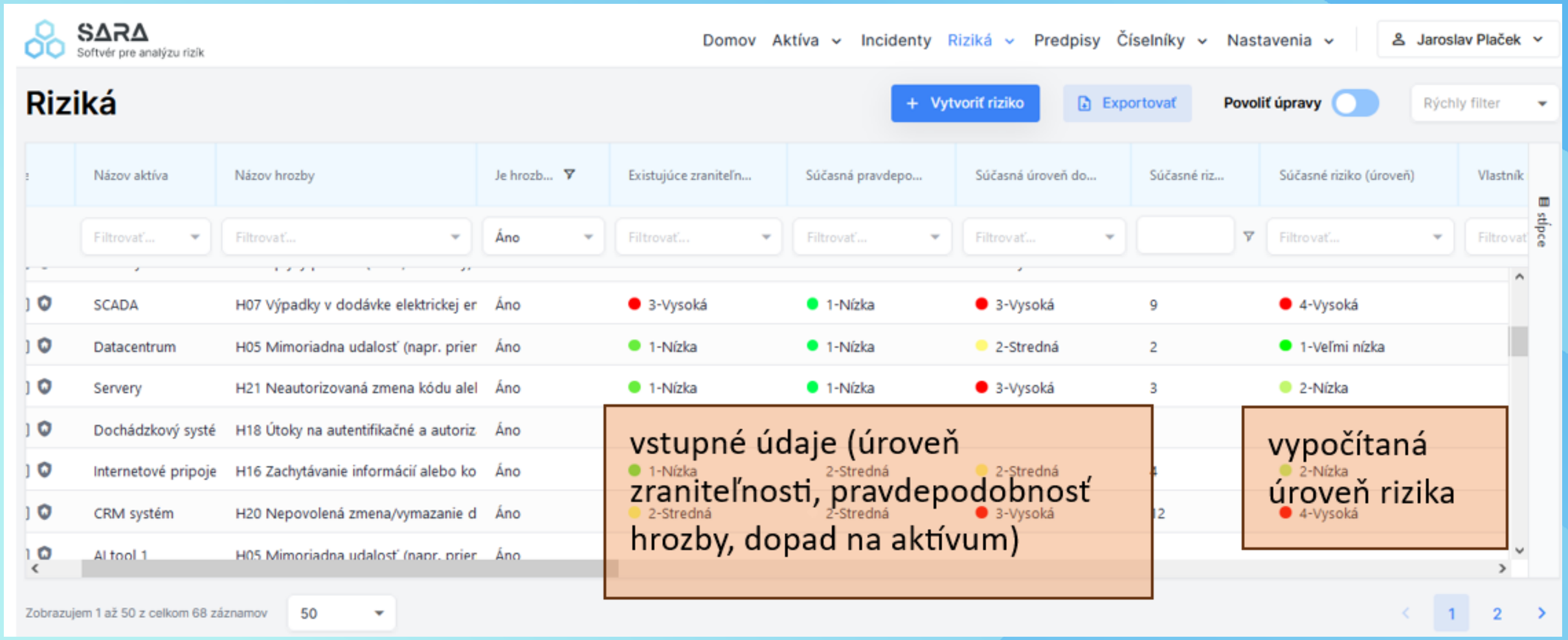
<u>Vysporiadanie sa s rizikom</u>: **Akceptácia** (vlastník aktíva), **Zníženie** (opatrenia = €), **Prenos** (napr. poistenie), **Vyhnutie sa riziku** (prestanem to robiť)

Preskúmanie rizík v SARA

Postup:

- pri vytvorení aktíva sa vytvorí zo zoznamu hrozieb **register rizík** pre aktívum
- riziká môžeme editolvať “hromadne” - v tabuľkovej forme alebo aj v detaile
- pre relevantné hrozby zadáme **dopad, pravdepodobnosť** a **úroveň zraniteľnosti** (dopad vieme vypočítať aj automaticky z klasifikácie a aj pre viacero hrozieb naraz)
- automaticky sa vypočíta **číselná hodnota a úroveň rizika**
- k riziku možno uviesť ďalšie informácie: podrobný scenár, existujúce **opatrenia** a **zraniteľnosti**
- doplníme **spôsob vysporiadania sa s rizikom** (min. pre vysoké riziká) a môžeme vypočítať **budúcu úroveň rizika** pri zohľadení navrhovaných opatrení
- **riziko môžeme zduplikovať** (napr. pre odlišné hodnotenie pre rôzne komponenty aktíva, príp. samostatné hodnotenie pre rôzne zraniteľnosti)

Editácia rizík v tabuľkovej forme

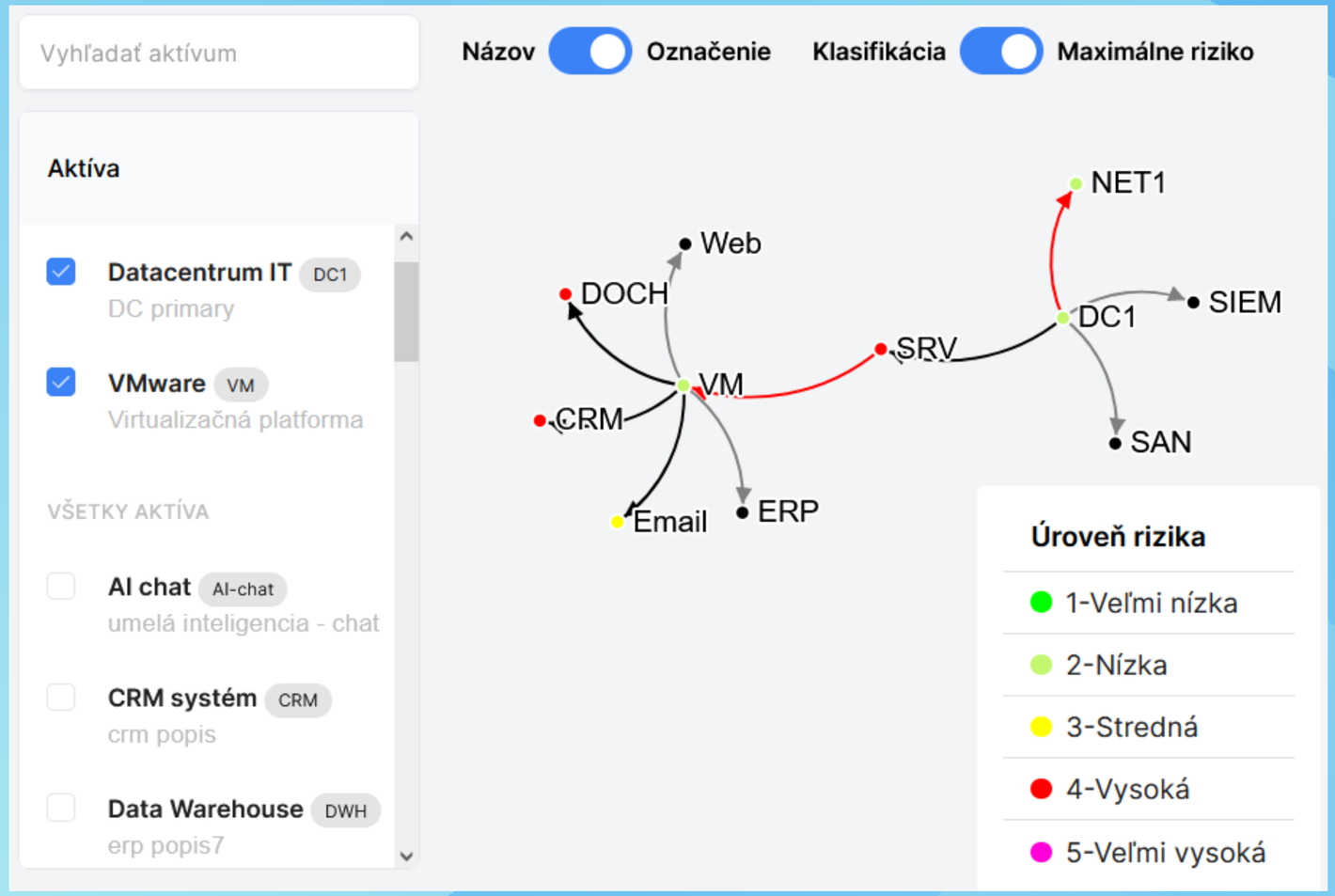


Vizualizátor – zobrazenie rizík

Zobrazenie maximálnej úrovne rizík – pre každé aktívum, u ktorého bolo vyhodnotené niektoré riziko, sa farebne zobrazí najvyššia dosiahnutá úroveň rizík.

Upozornenie na rizikovosť podporujúcich aktív – ak je riziko podporujúceho aktíva vyššie ako u podporovaného aktíva, ich väzba sa zobrazí červeno

V zozname aktív vľavo sa vyberajú (viaceré) aktíva na zobrazenie v grafe



SARA – dashboardy, reporty

Dashboardy

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

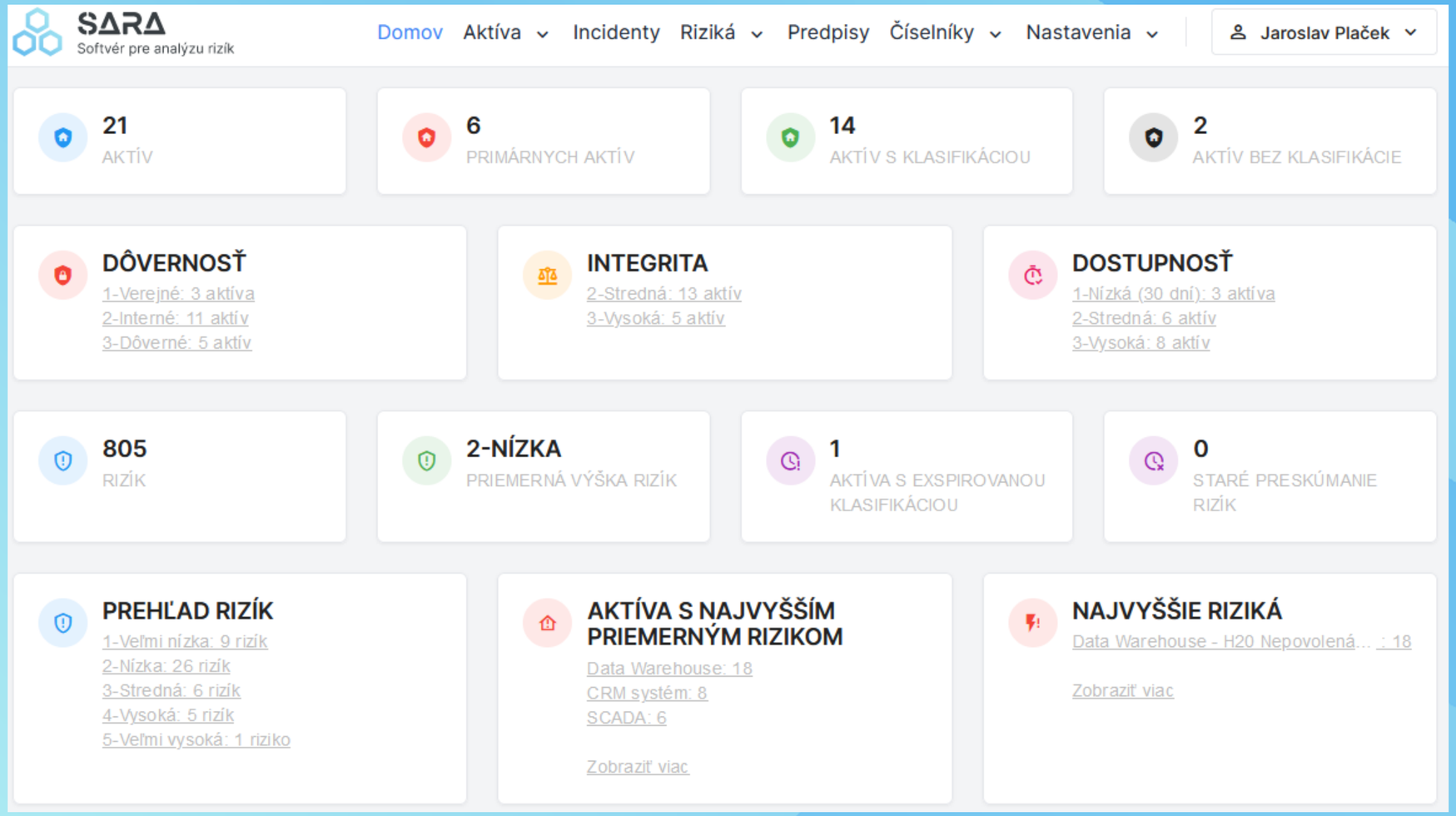
Reporty

Pre vlastníka aktíva:

- klasifikácia aktíva
- sumár analýzy rizík

Pre manažéra KB:

- zavedené opatrenia
- trend rizikovosti



Exporty - do csv súborov, dostupné z každého tabuľkového zobrazenia

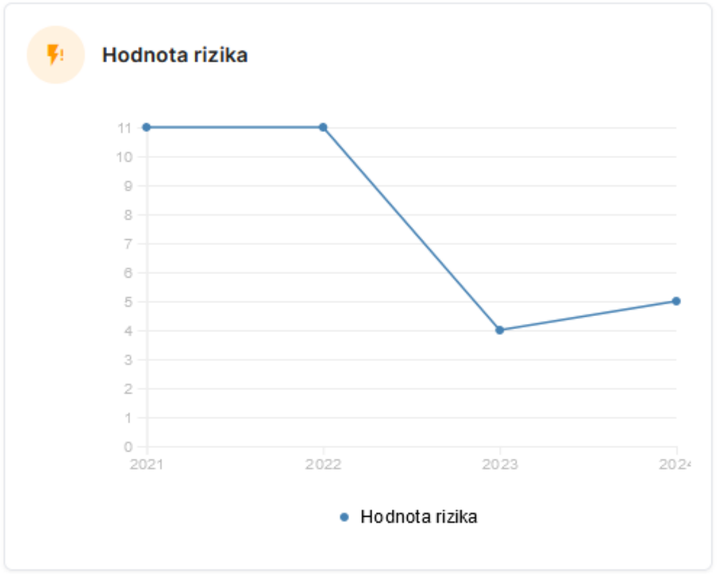
SARA – dashboardy, reporty

Rizikový profil spoločnosti

Označenie hrozby	Názov hrozby	Priemerná hodnota rizika	Priemerná úroveň rizika
MAL05	H20 Nepovolená zmena/vymazanie dát	15	4-Vysoká
MAL03	H18 Útoky na autentifikačné a autorizačné mechanizmy, falšovanie identity	12	4-Vysoká
MAL07	H22 Škodlivý SW	12	4-Vysoká
MAL09	H24 útok odopretia služby (DoS, DDoS)	12	4-Vysoká
MAL01	H16 Zachytávanie informácií alebo komunikácie, odpočúvanie, únik informácií	9	4-Vysoká
SUP05	H11 nedostatok / nedostupnosť personálu	8	3-Stredná
MAL02	H17 Injektovanie alebo modifikácia komunikácie	6	3-Stredná
MAL04	H19 Neoprávnené používanie SW/zariadení/ siete, zneužitie alebo falšovanie prístupových práv	6	3-Stredná
MAL06	H21 Neautorizovaná zmena kódu alebo komponentov systému.	6	3-Stredná
MAL08	H23 Sociálne inžinerstvo, phishing	5	3-Stredná
SUP03	H09 Výpadky v komunikačných/sieťových službách	4	2-Nízka
TECH03	H14 nedostatočná kapacita / preťaženie zariadenia	4	2-Nízka
TECH04	H15 Nedostupnosť nadväzujúcich systémov	4	2-Nízka

Priemerné riziko za posledných 5 rokov pre všetky aktíva

Rok	Hodnota rizika	Úroveň rizika
2021	11	4-Vysoká
2022	11	4-Vysoká
2023	4	2-Nízka
2024	5	3-Stredná



SARA – zhrnutie funkcionality

- **evidencia a hodnotenie aktív** vrátane histórie, efektívna editácia
- **preskúmanie a hodnotenie rizík** vrátane histórie, efektívna editácia
- **dashboardy** – prehľad o stave KB (počet identifikovaných rizík rôznych úrovní, priemerné riziko), prehľad klasifikácií (exspirované klasifikácie), o trendoch rizík,
- **reporty** – priemerné riziko per aktívum / celkovo, rizikový profil spoločnosti, vyhlásenie o aplikovateľnosti opatrení
- **zoznam predpisov** (legislatíva, interné predpisy)
- **evidencia incidentov** (väzba na dotknuté aktíva, kategorizácia incidentov podľa Zákona o KB, resp. definovateľná používateľom, stav riešenia incidentu)
- **roly a oprávnenia používateľov,** podporovaná väzba na Active Directory
- **prispôsobiteľnosť aplikácie -** na úrovni číselníkov
- **prispôsobenie pre používateľa** (zobrazenie stĺpcov, zoraďovanie, filtrovanie ...), tri jazykové mutácie (SK, EN, CZ)

SARA – zhrnutie účelu použitia

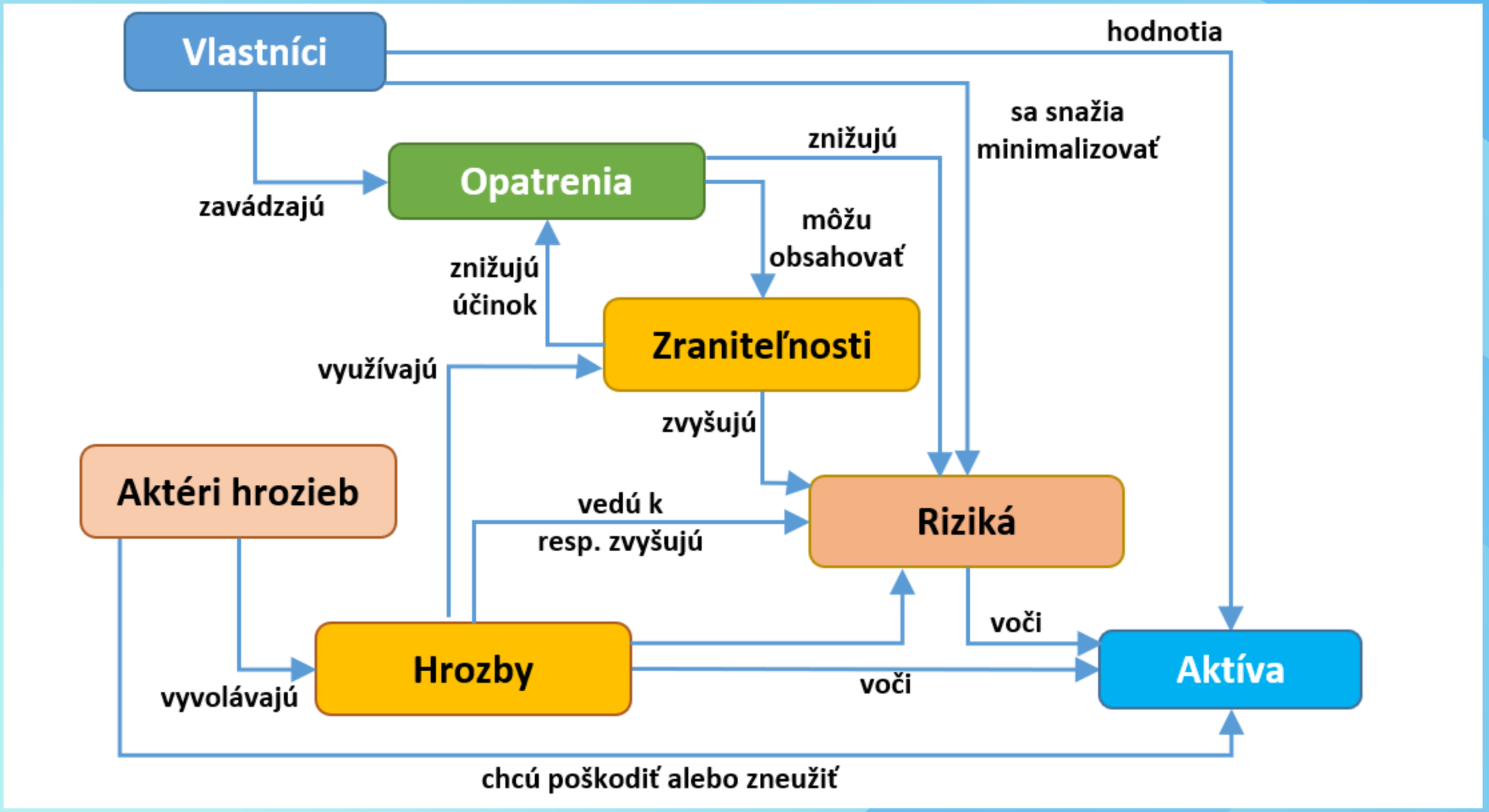
Pre koho je softvér určený?		
Manažéri KB, bezpečnostní špecialisti, vlastníci / garanti aktív, správcovia aktív, experti na riadenie rizík, audítori.		
SARA nám pomôže evidovať a odhaliť:		
Čo a ako dôkladne to mám chrániť?	**Evidencia, Klasifikácia, Reporty pre vlastníkov**	Manažér KB (Tímy KB) Vlastníci/garanti 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, reporty**	Manažér KB, Vedenie spoločnosti

Prečo je výhodné používať SARU?

- **Efektívna editácia údajov o aktívach a ich hodnotení** (možná hromadná editácia aktív aj rizík „a la“ Excel)
- **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 aktív – 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)

Ďakujem za pozornosť!

Riadenie rizík kybernetickej bezpečnosti



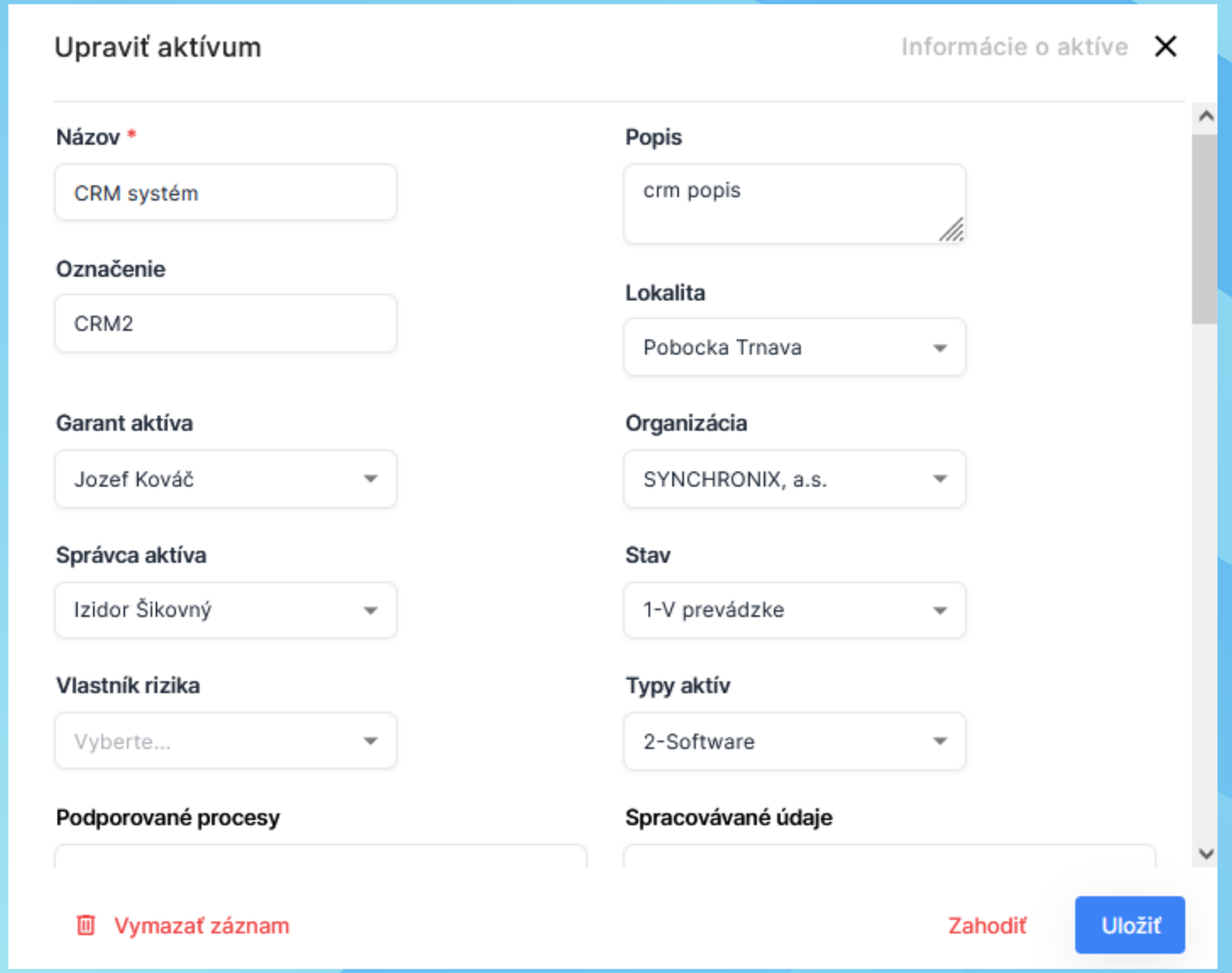
Detail aktíva

- **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**



Detail rizika