

# SARA

## Softvér na analýzu rizík

**SYNCHRONIX, a.s.**

Jaroslav Plaček

**iDEME**

21.6.2023



# Agenda

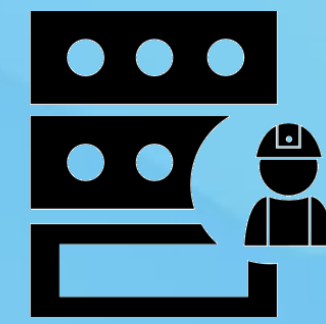
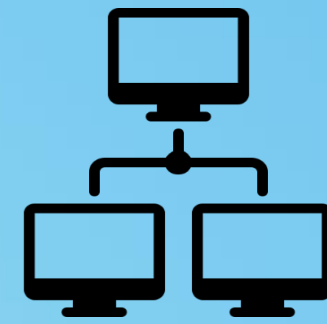
- 1) Riadenie rizík v kybernetickej bezpečnosti**
- 2) Evidencia a hodnotenie aktív**
- 3) Preskúmanie a analýza rizík - hrozby, zraniteľnosti, opatrenia**
- 4) Legislatíva pre kybernetickú bezpečnosť v SR**
- 5) SARA – predstavenie nástroja**
- 6) SARA – evidencia a hodnotenie aktív, analýza rizík**
- 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

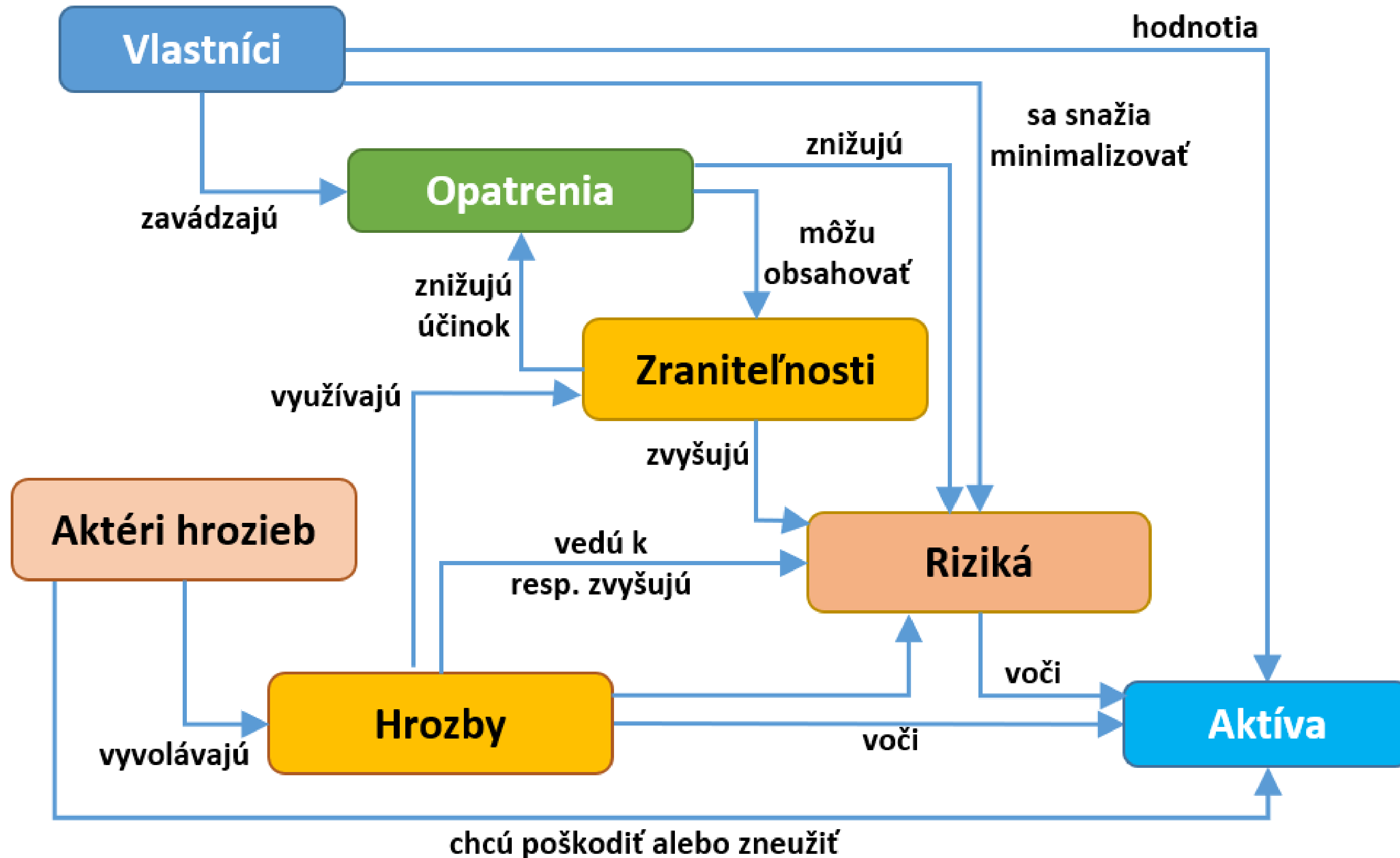
**Dostupnosť** – informačné aktíva sú dostupné v určenom čase

**Integrita** – informácie sú správne, úplné, môžu ich meniť len autorizované osoby

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



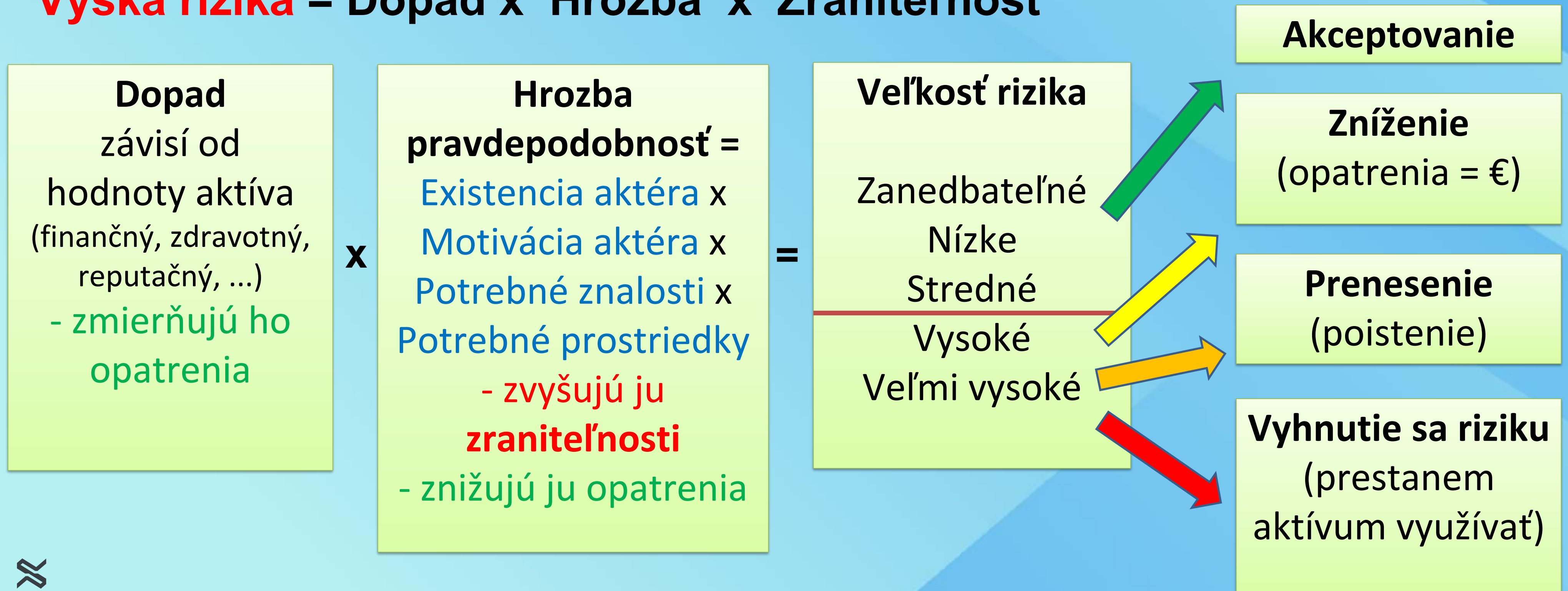
# Riadenie rizík kybernetickej bezpečnosti



# Výpočet rizika, vysporiadanie sa s rizikom

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

**Výška rizika = Dopad x Hrozba x Zraniteľnosť**



# 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 nahlásení informačného 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 dispozícii 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

The screenshot displays the SYNCHRONIX web interface for asset management. The top navigation bar includes 'Domov', 'Aktíva', 'Riziká', 'Predpisy', 'Číselníky', and 'Nastavenia'. The user 'Jaroslav Plaček' is logged in. The main section is titled 'Aktíva' and features buttons for '+ Vytvoriť aktívum', 'Exportovať', and 'Povolit úpravy'. A dropdown menu shows 'Moje aktíva (g...)'. The table below lists assets with columns for 'Akcie', 'Názov aktíva', 'Popis', 'Stav', 'Garant akt...', 'Dáv...', 'Inte...', 'Dostu...', 'RTO', and 'RPO'. Annotations highlight specific features: '1 - filtre pre zobrazenie v tabuľke' points to filter buttons; '2-klasifikácia (CIA, RTO, RPO)' points to the classification columns; '3-uložené zobrazenia' points to the 'Moje aktíva' dropdown; and '4-Ikonky pre Editáciu aktív, Väzieb, Duplikáciu, Analýzu rizík' points to the action icons in the first column.

Akcie	Názov aktíva	Popis	Stav	Garant akt...	Dáv...	Inte...	Dostu...	RTO	RPO	3-uložené zobrazenia
<input type="checkbox"/>	Dátová sieť	Interná komunikačná sieť	V produkcii	Jaroslav Plaček ...	Vysoká	Střední	Kritická			
<input type="checkbox"/>	Portal/webserver	Primárna webová stránk...	V produkcii	Jaroslav Plaček ...	Nízká	Vysoká	Vysoká	48	24	11. 8. 2022
<input type="checkbox"/>	Weather service	Popis	Ve vývoji	Jaroslav Plaček ...	Vysoká	Střední	Střední	24	24	11. 8. 2022
<input type="checkbox"/>	UPS Eaton 91PS	Popis	V produkcii	Jaroslav Plaček ...	Vysoká	Vysoká	Střední	48	3	11. 8. 2022
<input type="checkbox"/>	Kamerový systém	CCTV systém v kancelári...	V produkcii	Jaroslav Plaček ...	Vysoká	Nízká	Střední	48	1	31. 8. 2022
<input type="checkbox"/>	DNS	Domain Name System se...	V produkcii	Jaroslav Plaček ...	Střední	Vysoká	Nízká	24	7	31. 8. 2022
<input type="checkbox"/>	Adobe Acrobat	licencovaný SW Adobe A...	V testování	Jaroslav Plaček ...	Střední	Střední	Vysoká	7	3	11. 8. 2022

V tabuľkovom zobrazení je možnosť hromadnej editácie aktív



# Detail aktíva

- **Názov**, popis
- Vlastník aktíva, Správca
- **Dôvernost', Dostupnosť, Integrita**
- Spracovávané údaje,
- Podporované procesy
- Prílohy (napr. technická správa, bezpečnostný koncept, zmluva s dodávateľom)
- Dátum klasifikácie / analýzy rizík
- Uloženie záznamu klasifikácie do histórie

## Upraviť aktívum

Informácie o aktíve X

<b>Názov *</b> Kamerový systém	<b>Popis</b> CCTV systém v kanceláriách
<b>Označenie</b> KS01	<b>Organizácia</b> Synchronix
<b>Garant aktíva</b> Jaroslav Plaček - Jar...	<b>Stav</b> V produkcii
<b>Správca aktíva</b> Jaroslav Plaček - Jar...	<b>Typy aktív</b> INF.01
<b>Vlastník rizika</b> Jaroslav Plaček - Jar...	<b>Spracovávané údaje</b> videozáznamy osôb a priestorov (max 7 dní)
<b>Podporované procesy</b> - Ochrana majetku a zdravia osôb - Bezpečnostné opatrenie v rámci ISMS podľa ISO 27001	

Vymazať záznam **Zahodiť** **Uložiť**

# 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 nesúlady pri klasifikácii aktív a väzbách (červené šípky)

Nastaviť väzby pre 'Virtualizacia' ✕

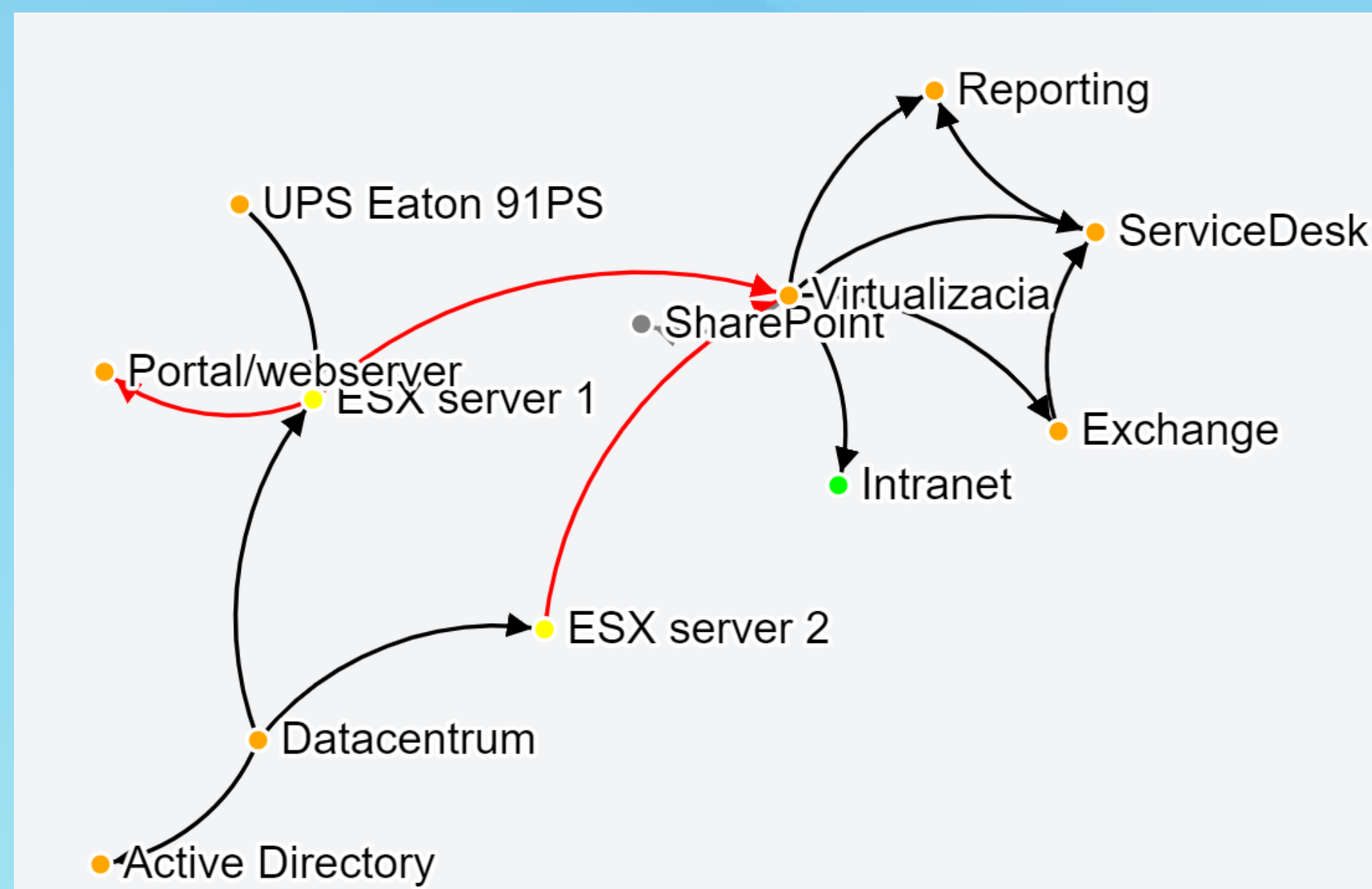
Podporuje aktíva

ServiceDesk ✕ Reporting ✕ Intranet ✕ SharePoint ✕

Podporujúce aktíva

ESX server 1 ✕ ESX server 2 ✕

Zrušiť Nastaviť väzby



# 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

Riziká								<a href="#">+ Vytvoríť riziko</a>	<a href="#">Exportovať</a>	Povolíť úpravy <input checked="" type="checkbox"/>
<input type="checkbox"/> Akcie	Názov ... ▾	Názov hrozby	Existujúce zraniteľnosti ...	Existujúce opatrenia	Súčasná pravdepod...	Súčasná úroveň dopa...	Súčasný riziko... ▾			
	Kame... ▾	Filtrovať... ▾	Filtrovať... ▾	Filtrovať... ▾	Filtrovať... ▾	Filtrovať... ▾	Filtrovať... ▾			
<input type="checkbox"/>   	Kamerový sys...	Neoprávnené používanie SW/zariadení/siete, zneužitie ale...	Nízká	Preskúmanie prístupových ...	Střední	Střední	12			
<input type="checkbox"/>   	Kamerový sys...	Injektovanie alebo modifikácia komunikácie	Střední	Sieťové opatrenia, Prístup ...	Nízká	Střední	12			
<input type="checkbox"/>   	Kamerový sys...	prezradenie / zneužitie dôverných informácií	Nízká	Politika riadenia prístupov, ...	Nízká	Vysoká	12			
<input type="checkbox"/>   	Kamerový sys...	zneužitie kompetencií, nedodržanie platnej legislatívy	Nízká		Nízká	Vysoká	12			
<input type="checkbox"/>   	Kamerový sys...	Nepovolená zmena/vymazanie dát	Nízká	Politika riadenia prístupov, ...	Střední	Střední	12			
<input type="checkbox"/>   	Kamerový sys...	krádež / poškodenie cudzími osobami	Střední		Nízká	Střední	12			
<input type="checkbox"/>   	Kamerový sys...	Neautorizovaná zmena kódu alebo komponentov systému.	Nízká	Politika riadenia prístupov, ...	Nízká	Střední	8			
<input type="checkbox"/>   	Kamerový sys...	krádež / poškodenie zamestnancami	Nízká		Nízká	Nízká	4			

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



# Detail rizika

### Upraviť riziko

**Názov aktíva \***  
Active Directory

**Názov hrozby \***  
Nepovolená zmena/vymazanie dát

**Scenár hrozby**  
neautorizované vytvorenie účtu, modifikácia členstva v AD skupinách

Je hrozba relevantná ?

**Súčasná zraniteľnosť**

Zoznam zraniteľností	Popis
Nedostatočné riadenie prístupu	Zbytočne veľa domain administrátorov; <u>nedodržia</u> sa proces pre riadenie a schvaľovanie zmien vrátane účtov v AD
Nedostatočné riadenie zmien	

### Upraviť riziko

**Súčasná opatrenia**

**Zoznam opatrení**

- Preskúmanie prístupových práv
- Poskytovanie používateľských prístupov

**Popis**

**Súčasná úroveň dopadu na aktívum**  
Vysoká (z klasifikácie) max CIA

**Súčasná úroveň hrozby**  
Střední

**Súčasná úroveň zraniteľnosti**  
Vysoká

**Vlastník rizika (predefinovanie)**  
Vyberte...

**Súčasná úroveň rizika**  
36 hodnota

**Súčasná úroveň rizika**  
Vysoké úroveň

**Dátum aktualizácie rizika**



# SARA – dashboardy, reporty, export

## Dashboardy

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

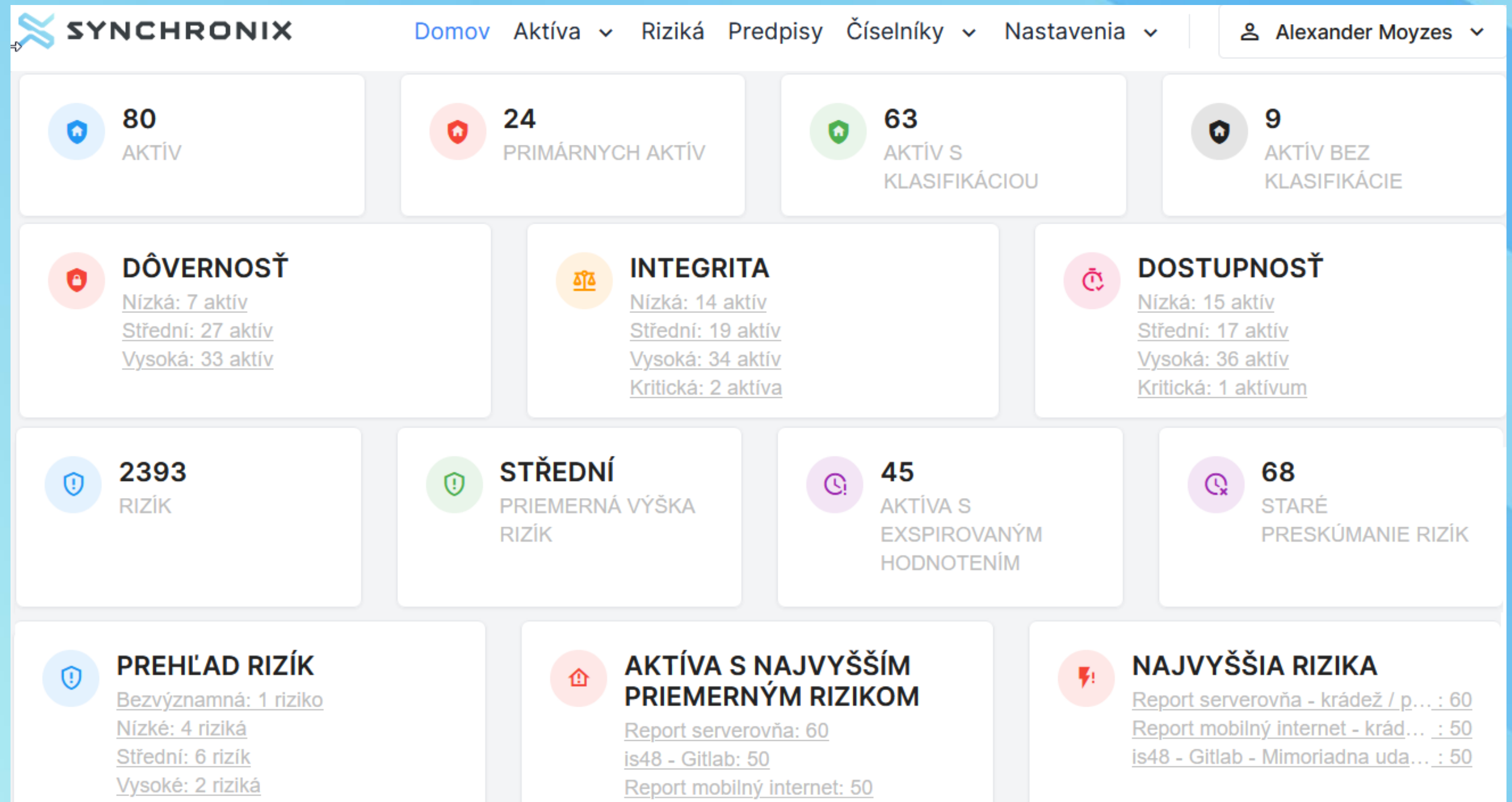
## Reporty

### 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
- **dashboards** – 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, zoradovanie, 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

?