



SARA

Softvér pre analýzu rizík

SYNCHRONIX, a.s.

Jaroslav Plaček

iDEME, 20.6.2024



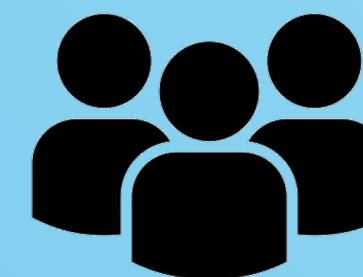
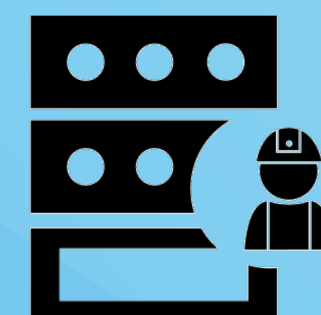
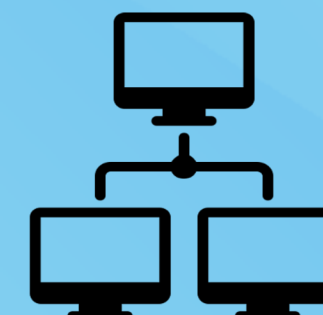
Agenda

- 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**





Potrebuje 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 ošetrovanie 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

The image shows two overlapping Excel spreadsheets. The top one is a general asset inventory, and the bottom one is a detailed risk assessment table titled 'HODNOCENÍ RIZIK'.

ID	Aktívum	Hodnota dopadu - dostupnosť	Hodnota dopadu - dôverynosť	Hodnota dopadu - integrita	Zraniteľnosť	Hodnota zraniteľnosti	Hrozba	Hodnota hrozby	Hodnota rizika - dostupnosť	Hodnota rizika - dôverynosť	Hodnota rizika - integrita	závažnosť rizika	komentár
R1	PO1: Aplicační server (HW)	3	Nerelevantní	3	Z2: Zastaralost aktiv	4	H2: Poškození nebo sešláhání technického nebo programového vybavení	3	36	Nerelevantní	36	redukce	aplicační servery mají 7 let, už nejsou podporovány výrobcem
R2	PO1: Aplicační server (HW)	3	Nerelevantní	3	Z7: Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností lidských zdrojů	4	H2: Poškození nebo sešláhání technického nebo programového vybavení	3	36	Nerelevantní	36	redukce	v případě mimořádné události hrozí, že bude aplicační server obsluhováno mimo provoz, protože nejsou dostatečně zapracovány plány kontinuity úkonů a havarijní plány
R3	PO2: Databázový server (HW)	3	Nerelevantní	3	Z2: Zastaralost aktiv	4	H2: Poškození nebo sešláhání technického nebo programového vybavení	3	36	Nerelevantní	36	redukce	zastaralý BIOS, není sešláhání OS
R4	PO5: Operační systém - databázový server	3	Nerelevantní	3	Z1: Nedostatečná údržba aktiv	4	H2: Poškození nebo sešláhání technického nebo programového vybavení	3	36	Nerelevantní	36	redukce	neoprávněné nastavení, špatná konfigurace
R5	PO5: Operační systém - databázový server	3	Nerelevantní	3	Z1: Nedostatečná údržba aktiv	4	H2: Poškození nebo sešláhání technického nebo programového vybavení	3	36	Nerelevantní	36	redukce	neoprávněné nastavení, špatná konfigurace
R6	PO3: Webový server (HW)	3	Nerelevantní	3	Z2: Zastaralost aktiv	4	H2: Poškození nebo sešláhání technického nebo programového vybavení	3	36	Nerelevantní	36	redukce	neoprávněné nastavení, špatná konfigurace
R7	PO4: Operační systém - aplicační server	3	Nerelevantní	3	Z7: Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností lidských zdrojů	4	H2: Poškození nebo sešláhání technického nebo programového vybavení	3	36	Nerelevantní	36	redukce	neoprávněné nastavení, špatná konfigurace
R8	PO4: Operační systém - aplicační server	3	Nerelevantní	3	Z1: Nedostatečná údržba aktiv	4	H2: Poškození nebo sešláhání technického nebo programového vybavení	3	36	Nerelevantní	36	redukce	neoprávněné nastavení, špatná konfigurace



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



















































Aktíva

+ Vytvoriť aktívum

Exportovať

Uložiť úpravy

Iba aktívne ▾

<input type="checkbox"/> Akcie	Názov aktíva ↑	Označenie	Popis	Stav	Garant aktíva	Dôvernosť	Integrita	Dostupnosť	RTO	RPO
<input type="checkbox"/>				Filtrovať...	Filtrovať...	Filtrovať...	Filtrovať...	Filtrovať...		
<input type="checkbox"/>     	Data Warehouse	DWH	erp popis7	1-V prevádzke	OwnerIS	● 3-Dôverné	● 3-Vysoká	● 3-Vysoká	24	24
<input type="checkbox"/>     	Datacentrum IT	DC1	DC primary	1-V prevádzke		● 3-Dôverné	● 3-Vysoká	● 3-Vysoká	24	24
<input type="checkbox"/>     	Datacentrum OT	DC2	Datacentrum secundus	1-V prevádzke		● 3-Dôverné	● 3-Vysoká	● 3-Vysoká	24	24
<input type="checkbox"/>     	Dochádzkový systém	DOCH	Hlavný dochádzkový sys...	1-V prevádzke	Jaroslav Plaček	● 2-Interné	● 2-Stredná	● 1-Nízka (30 dní)		
<input type="checkbox"/>     	Email server secundus	Email	Sendmail email server	1-V prevádzke	OwnerIS	● 3-Dôverné	● 2-Stredná	● 2-Stredná		
<input type="checkbox"/>     	Enterprise Network	NET1	Main network	1-V prevádzke		● 2-Interné	● 2-Stredná	● 1-Nízka (30 dní)	24	
<input type="checkbox"/>     	ERP	ERP	Enterprise resource plan...	1-V prevádzke	Izidor Šikovný	● 3-Dôverné	● 2-Stredná	● 2-Stredná	5	
<input type="checkbox"/>     	Fortinet FW	FW		1-V prevádzke	Jaroslav Plaček	● 3-Dôverné	● 3-Vysoká	● 3-Vysoká	1	16
<input type="checkbox"/>     	Historian	OT-HIST	zapisovací server	1-V prevádzke	Izidor Šikovný	● 1-Verejné	● 2-Stredná	● 3-Vysoká	5	24
<input type="checkbox"/>     	Internetové pripojenie	Internet		2-Vo vývoji		● 1-Verejné	● 2-Stredná	● 3-Vysoká		




Previazanie aktív a vizualizácia väzieb

Väzby medzi aktívami:

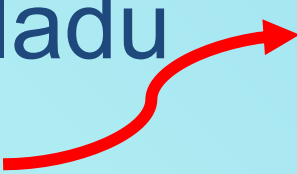
- každé aktívum môže podporovať alebo byť podporované iným aktívom

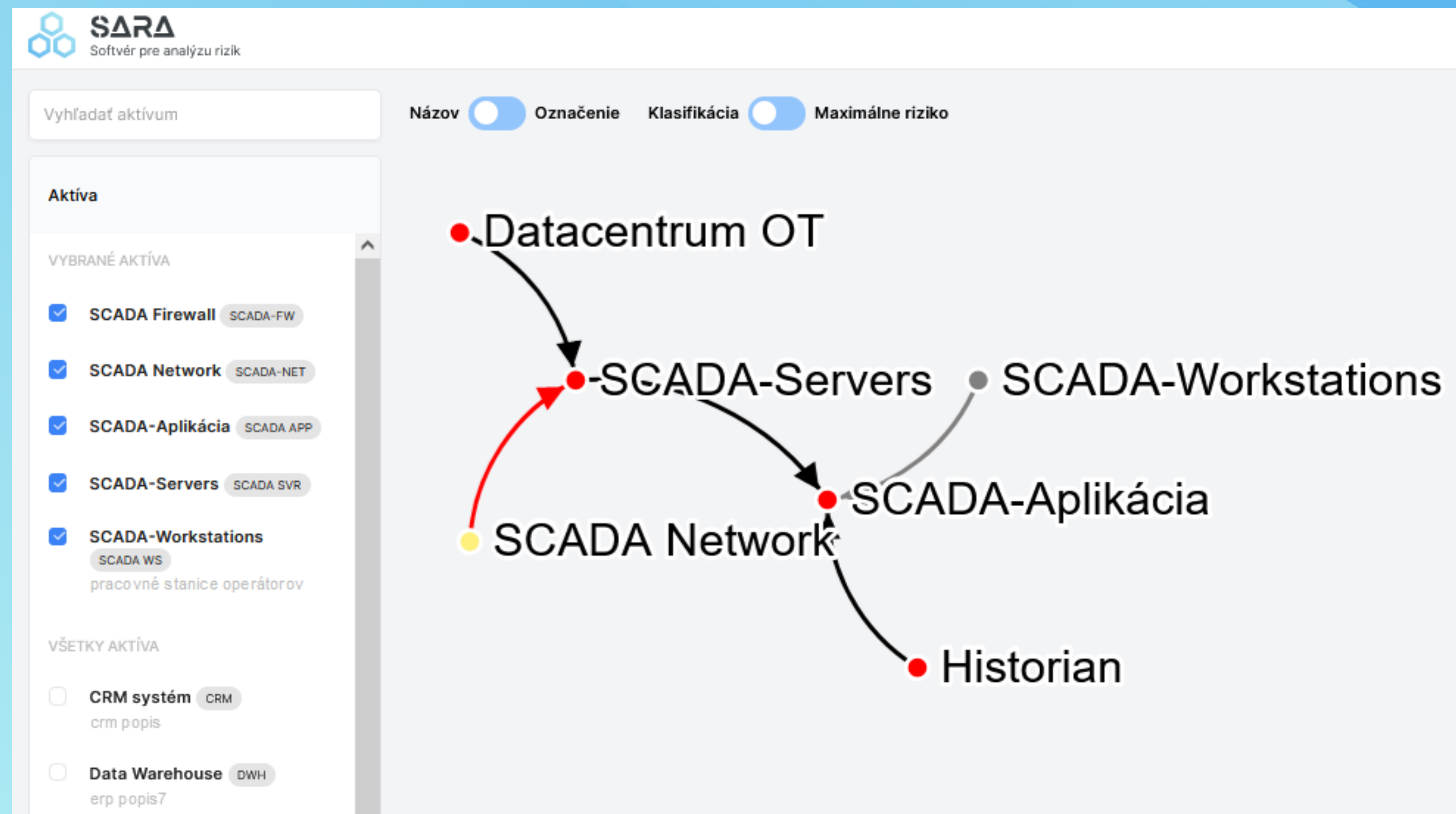
Vizualizátor:

- grafické znázornenie väzieb aktív

- farebné vyznačenie stupňa klasifikácie 

- zobrazenie chýbajúcej klasifikácie 

- zobrazenie nesúlady klasifikácie aktív 

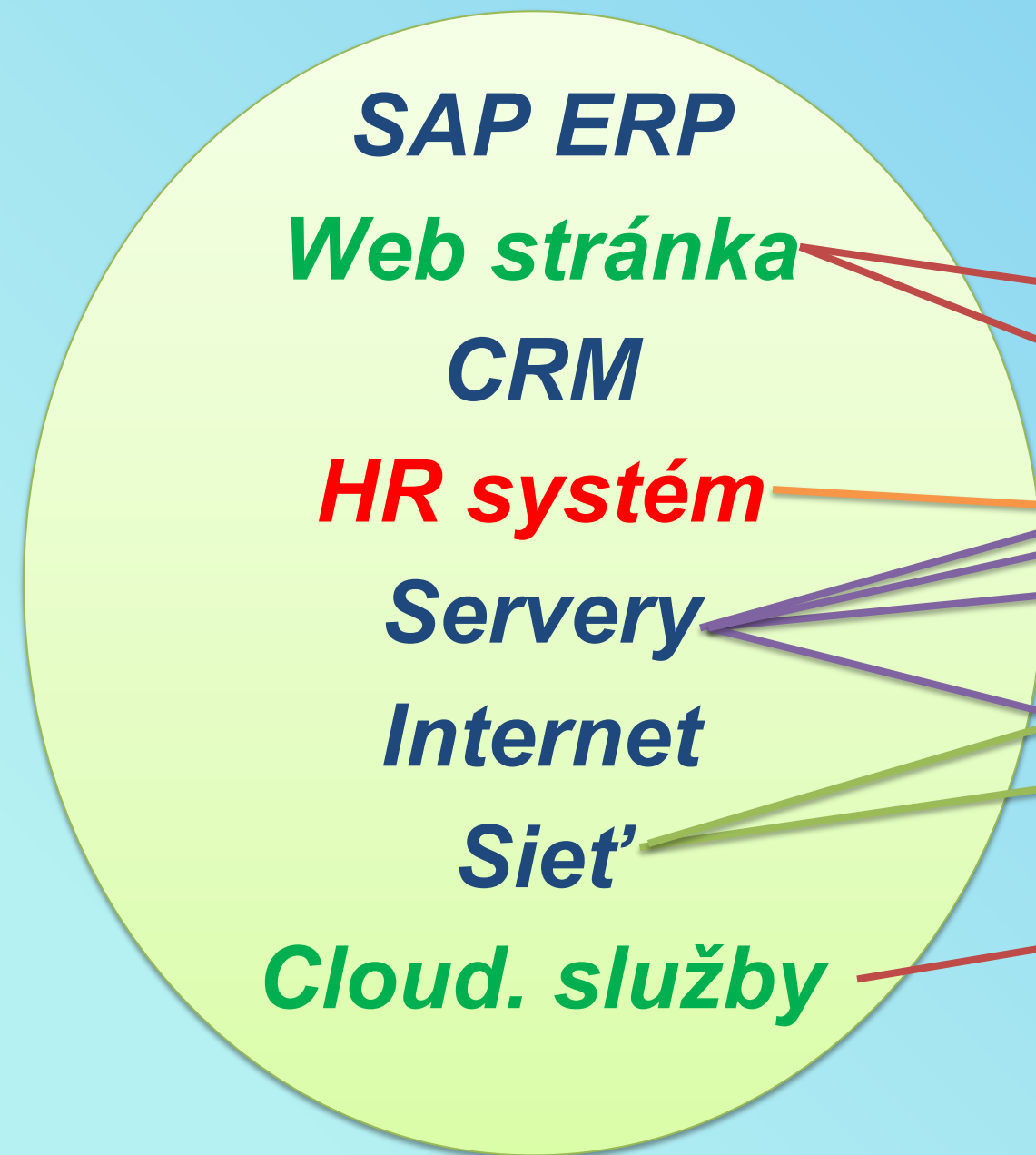


Čo považujeme za riziko?

Ohodnotené aktíva (N)

Hrozby (M)

**Riziko =
aktívum x hrozba**



**Počet rizík
je (max) MxN**

Príklad: Riziko úniku osobných údajov z HR systémom



Výpočet rizika, vysporiadanie sa s rizikom

Preskúmanie rizík: 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

Vysporiadanie sa s rizikom: **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 editovať “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 zohľadnení navrhovaných opatrení
- **riziko môžeme zduplikovať** (napr. pre odlišné hodnotenie pre rôzne komponenty aktíva, príp. samostatné hodnotenie pre rôzne zraniteľnosti)



Editácia rizík v tabuľkovej forme

SARA Softvér pre analýzu rizík

Domov Aktíva ▾ Incidenty Riziká ▾ Predpisy Číselníky ▾ Nastavenia ▾ Jaroslav Plaček ▾

Riziká

+ Vytvoríť riziko Exportovať Povolíť úpravy Rýchly filter

Názov aktíva	Názov hrozby	Je hrozb...	Existujúce zraniteľn...	Súčasná pravdepo...	Súčasná úroveň do...	Súčasný riz...	Súčasný riziko (úroveň)	Vlastník
SCADA	H07 Výpadky v dodávke elektrickej er	Áno	3-Vysoká	1-Nízka	3-Vysoká	9	4-Vysoká	
Datacentrum	H05 Mimoriadna udalosť (napr. prier	Áno	1-Nízka	1-Nízka	2-Stredná	2	1-Veľmi nízka	
Servery	H21 Neautorizovaná zmena kódu alel	Áno	1-Nízka	1-Nízka	3-Vysoká	3	2-Nízka	
Dochádzkový systé	H18 Útoky na autentifikačné a autoriz	Áno						
Internetové pripoje	H16 Zachytávanie informácií alebo ko	Áno						
CRM systém	H20 Nepovolená zmena/vymazanie d	Áno						
AI tool 1	H05 Mimoriadna udalosť (napr. prier	Áno						

Zobrazujem 1 až 50 z celkom 68 záznamov 50

1 2

vstupné údaje (úroveň zraniteľnosti, pravdepodobnosť hrozby, dopad na aktívum)

- 1-Nízka
- 2-Stredná
- 3-Vysoká

vypočítaná úroveň rizika

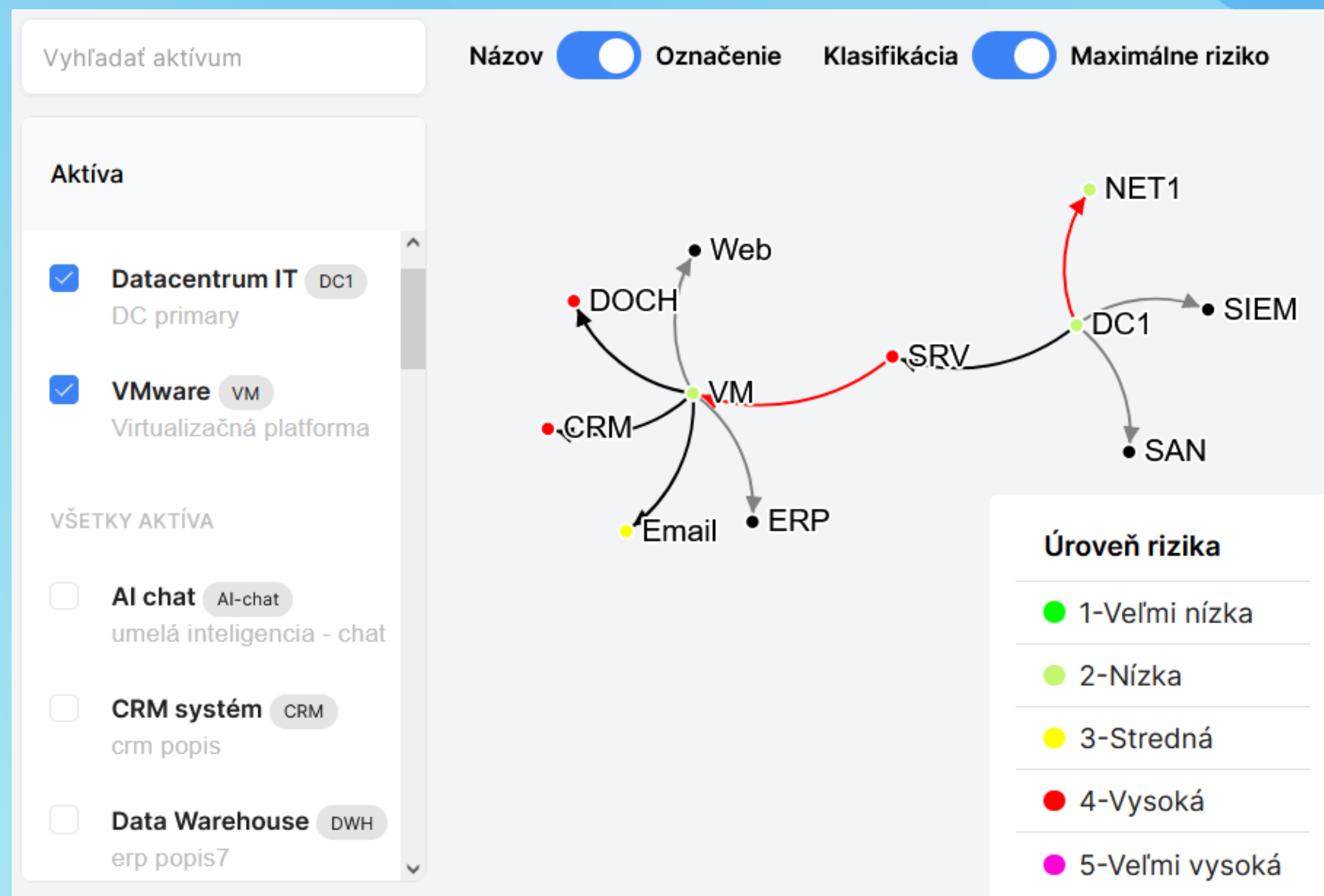
- 2-Nízka
- 4-Vysoká

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:

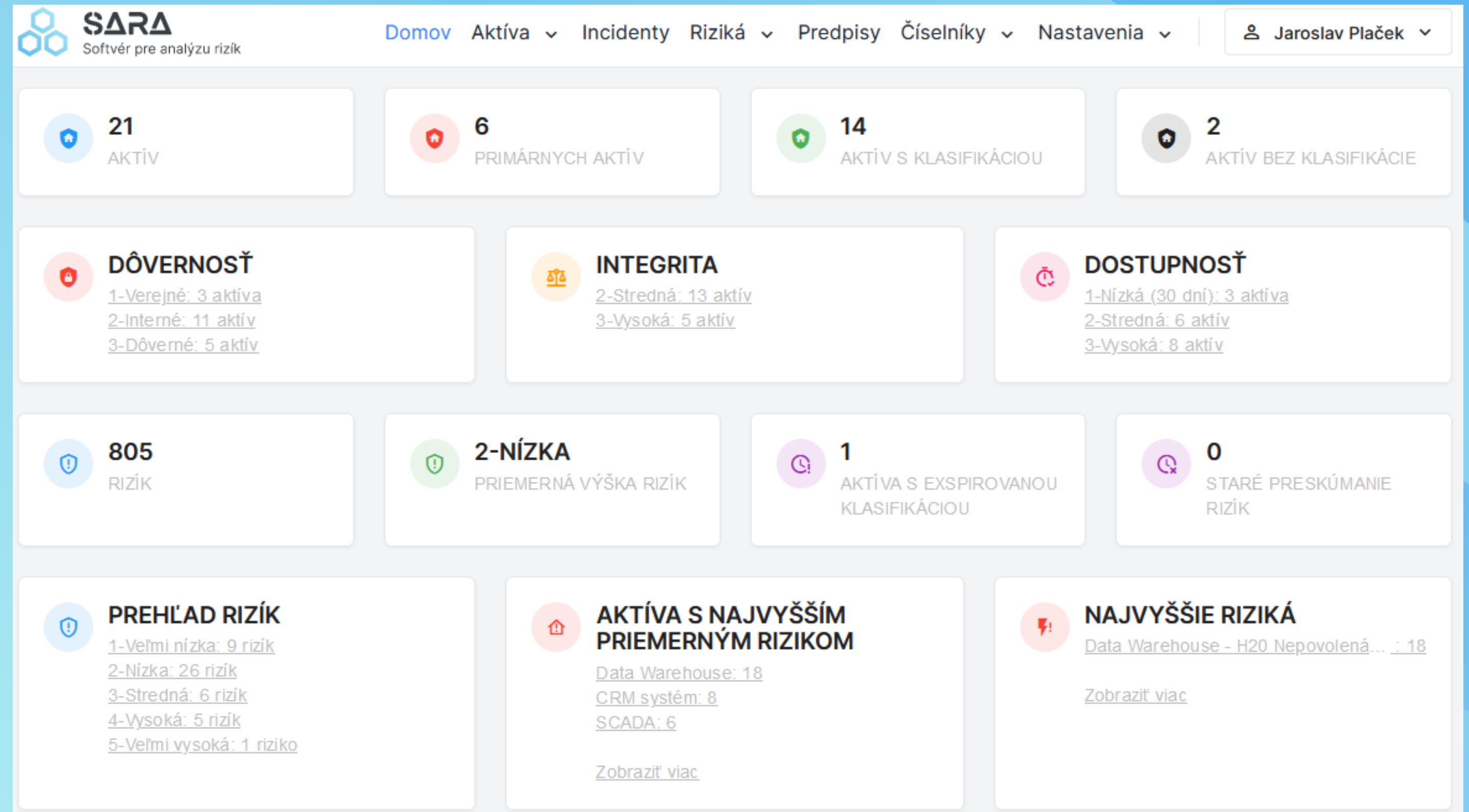
- klasifikácia aktíva

- sumár analýzy rizík

Pre manažéra KB:

- zavedené opatrenia

- trend rizikovosti



Exporty - do csv súborov, dostupné z každého tabuľkového zobrazenia



SARA – dashboards, 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 inžinierstvo, 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 navzájomvisiacich 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
- **dashboards** – 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, zoradovanie, 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?

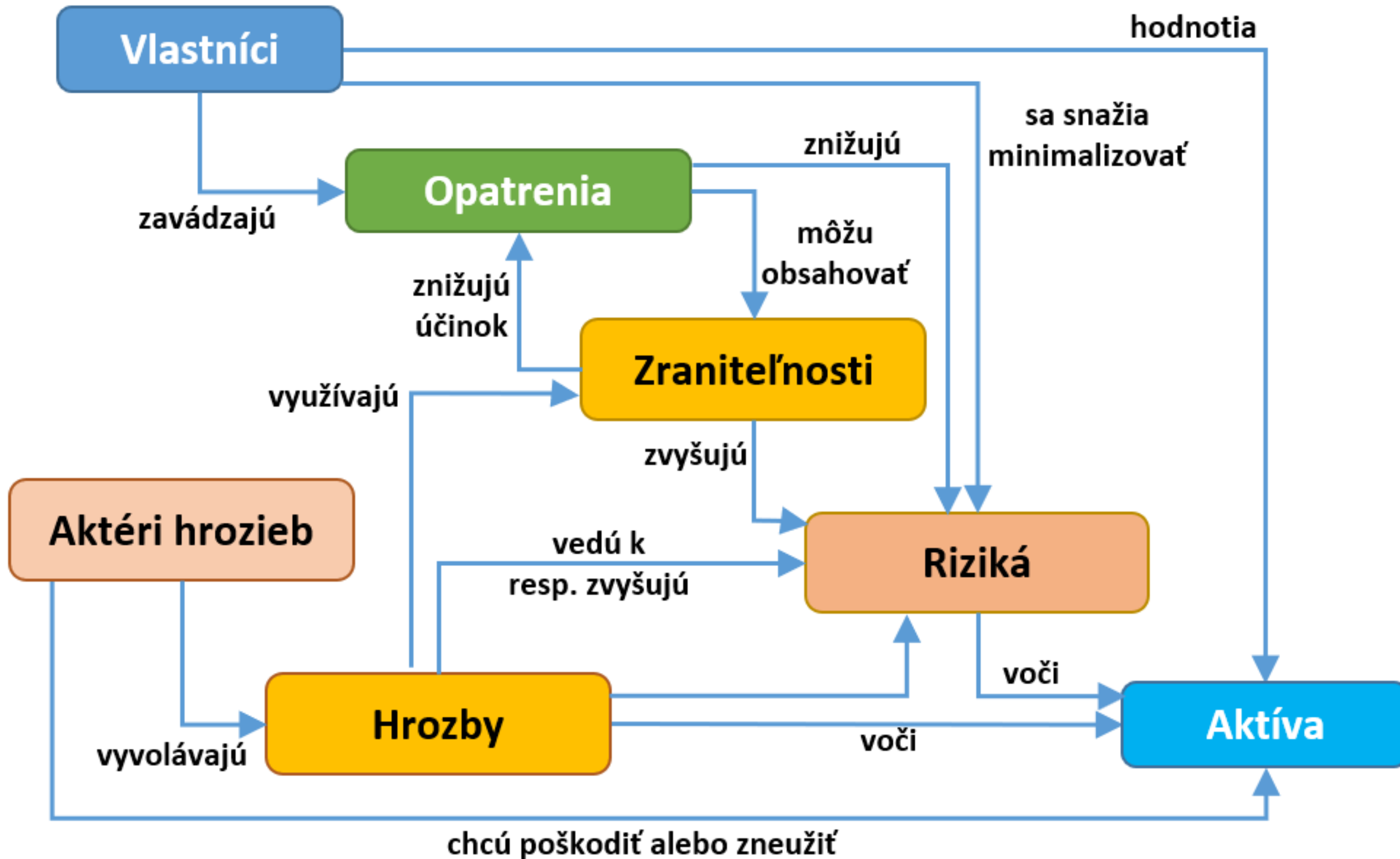
- **Efektívna editácia údajov o aktívach a ich hodnotení** (možná hromadná editácia aktív aj rizík „a la“ Excel)
- **Analýzy rizík je potrebné vykonávať pre všetky aktíva a prehľadne sumarizovať ich výstupy, ktoré treba priebežne sledovať a aktualizovať** (pri použití samostatných súborov pre analýzy 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
- **Dôvernost'**, **Dostupnost'**, **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

Názov * CRM systém	Popis crm popis
Označenie CRM2	Lokalita Pobočka Trnava
Garant aktíva Jozef Kováč	Organizácia SYNCHRONIX, a.s.
Správca aktíva Izidor Šikovný	Stav 1-V prevádzke
Vlastník rizika Vyberte...	Typy aktív 2-Software
Podporované procesy	Spracovávané údaje

 **Vymazať záznam** **Zahodiť** **Uložiť**

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

Nedostatočné riadenie prístupu

Nedostatočné riadenie zmien

Popis

Zbytočne veľa domain administrátorov; nedodržiava sa proces pre riadenie a schvaľovanie zmien vrátane účtov v AD

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...

 Vymazať záznam

Súčasná riziko

36

hodnota

Súčasná riziko

Vysoké

úroveň

Dátum aktualizácie rizika

Zahodiť

Uložiť

