Bližší pohled na NIS2 ve veřejné správě a analýzu rizik

František Janů - vedoucí oddělení Služby Cyber Security
Miroslav Dvořák - ředitel odboru Správa informační bezpečnosti

Co se mění?

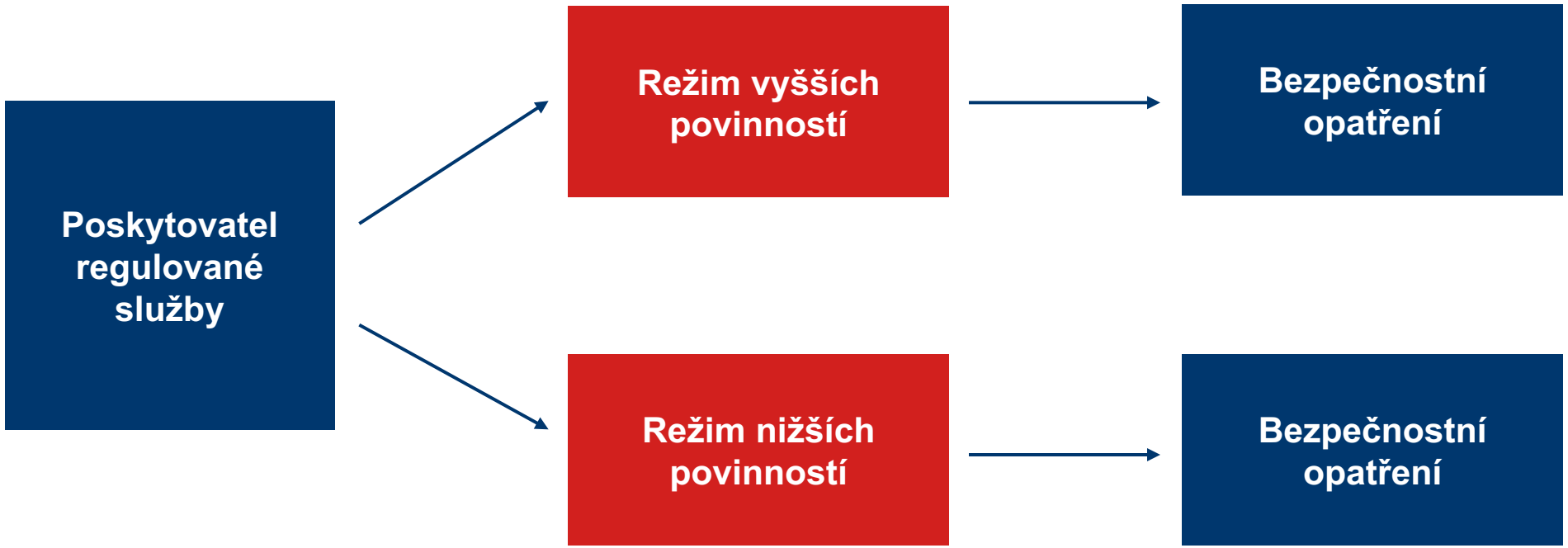
- Změny v typech regulovaných subjektů
  - jeden typ regulovaného subjektu - poskytovatel regulované služby
  - dva režimy regulace - nižší a vyšší
- Změna ve způsobech určování regulovaných osob
  - až na výjimky na základě povahy businessu dle kategorií uvedených ve vyhlášce o regulovaných službách
- Změna u současných významných informačních systémů
  - některé mohou spadnout do vyššího režimu regulace
  - zbývající do nižšího
- Nárůst dopadu regulace obecně - i ve státní správě dopadne ZKB po jeho novele na více subjektů, než tomu bylo doposud
- Změny v povinnostech a sankcích

Co se mění?

- POSKYTOVATEL REGULOVANÉ SLUŽBY
  - Dva režimy regulace - nižší a vyšší

*zdroj NÚKIB

Nižší vs. vyšší režim regulace – co to znamená?



*zdroj NÚKIB

Nejdůležitější rozdíly v rozsahu

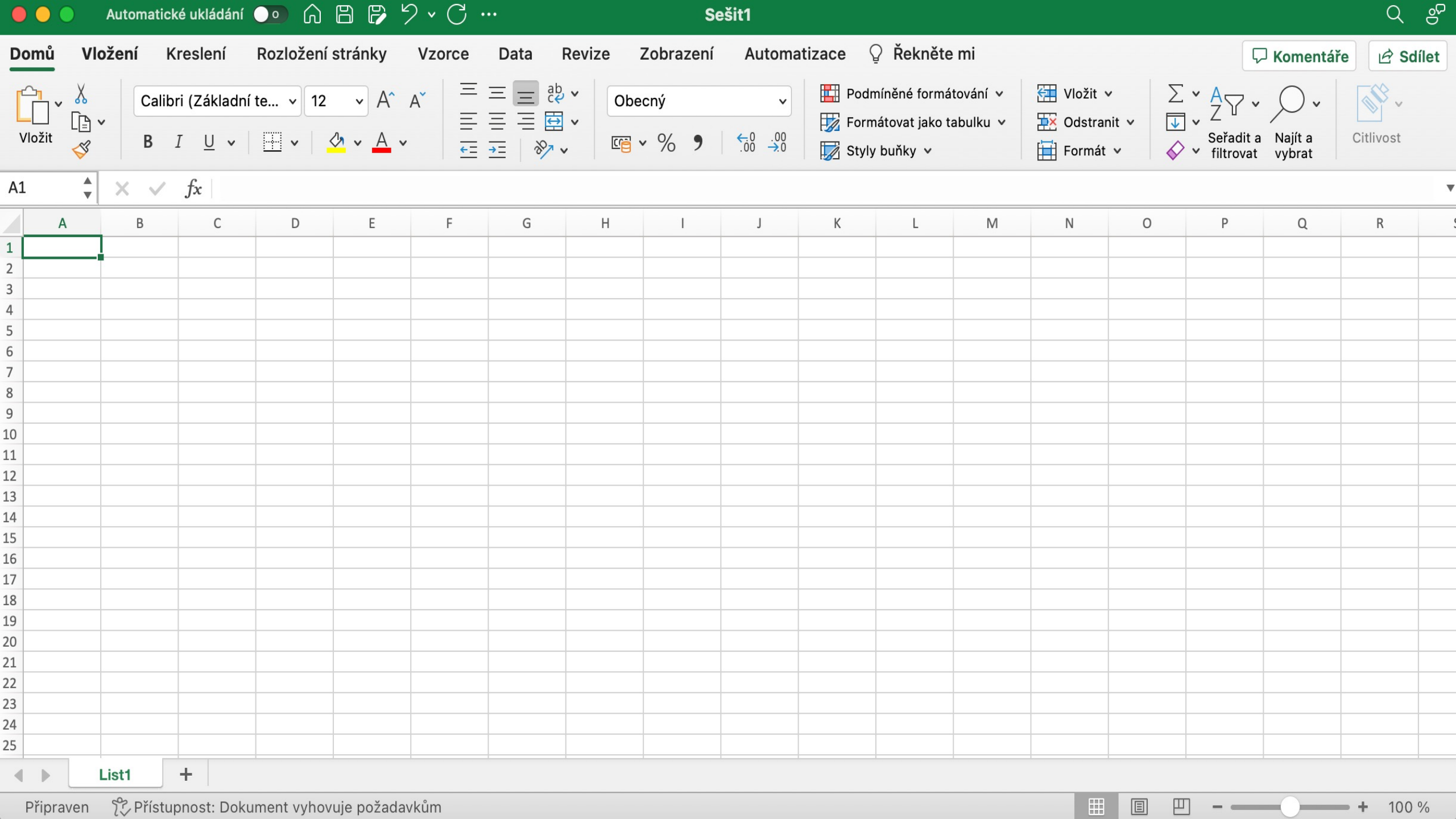
- vyšší režim regulace - oproti původní vyhlášce o KB:
  - vyšší nároky (například analýza rizik)
  - snaha o přesnější a praxi bližší pojmenování jednotlivých požadavků
  - hlášení všech kyber-bezpečnostních incidentů s původem v kyberprostoru

- nižší režim regulace
  - nižší nároky (např. bez celého procesu řízení rizik => **základní principy z analýzy rizik**)
  - prakticky ale dost podobné vyššímu režimu s tím, že požadavky jsou obecnější, případně mírnější
  - hlášení významných kyber-bezpečnostních incidentů

Jak na analýzu rizik?

A) TABULKOVÝ EDITOR?





Automatické ukládání
Sešit1
Domů
Vložení
Kreslení
Rozložení stránky
Vzorce
Data
Revize
Zobrazení
Automatizace
Řekněte mi
Komentáře
Sdílet
Vložit
Calibri (Základní te...
12
Obecný
Podmíněné formátování
Formátovat jako tabulku
Styly buňky
Vložit
Odstranit
Formát
Seřadit a filtrovat
Najít a vybrat
Citlivost
A1
List1
Připraven
Přístupnost: Dokument vyhovuje požadavkům
100 %

Jak postupovat?

Ročník 2018

SBÍRKA ZÁK
ČESKÁ REPUBLIKA

Částka 43 Rozeslána dne 28. května 2018

Hodnocení rizik

(1) Jednoznačné stanovení funkce pro určení rizika je nezbytnou součástí metodiky pro hodnocení rizik podle § 5.

(2) Hodnota rizika je nejčastěji vyjádřena jako funkce, kterou ovlivňuje dopad, hrozba a zranitelnost.

(3) Pro hodnocení rizik lze použít například tuto funkci:

Riziko = dopad x hrozba x zranitelnost.

(4) Dopad je v tomto případě odvozen z hodnocení aktiv podle přílohy č. 1.

(5) V případě, že povinná osoba využívá metodu pro hodnocení rizik, která nerozlišuje hodnocení hrozby a zranitelnosti, je možné stupnice pro hodnocení hrozeb a zranitelností sloučit. Sloučení stupnic by nemělo vést ke ztrátě schopnosti rozlišení úrovně hrozby a zranitelnosti. Za tímto účelem lze použít například komentář, který zřetelně vyjádří jak úroveň hrozby, tak i úroveň zranitelnosti. Obdobně se postupuje i v případech, kdy povinná osoba používá jiný počet úrovní pro hodnocení dopadů, hrozeb, zranitelností a rizik.

Tab. 1: Stupnice pro hodnocení hrozeb

Úroveň	Popis
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku
Kritická	

Tab. 2: Stupnice pro hodnocení zranitelností

Úroveň	Popis
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Tab. 1: Stupnice pro hodnocení důvěrnosti

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP") je využíváno označení TLP:WHITE.	Není vyžadována žádná ochrana. Likvidace/mazání aktiva na úrovni Nízká - viz příloha č. 4.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:GREEN nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu. Likvidace/mazání aktiva na úrovni Střední - viz příloha č. 4.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a ací komunikační sítí jsou edků. á - viz příloha č. 4.

Tab. 2: Stupnice pro hodnocení integrity

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity j sou využívány standardní nástroje (například omezení přístupových práv pro zápis).
soká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Pr sle pr ko
itická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	Pr ide dig

Tab. 3: Stupnice pro hodnocení rizik

Úroveň
Nízké
Střední
Vysoké
Kritické

Tab. 3: Stupnice pro hodnocení dostupnosti

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin.	Pro ochranu dostupnosti jsou využívány záložní systémy

	Přípustný způsob likvidace podle úrovně důležitosti aktiva			
Nosič informace	**1. Nízká**	**2. Střední**	**3. Vysoká**	**4. Kritická**
Informace na lidsky čitelném nosiči (tištěné dokumenty, poznámky a podobně)	Odstranění: Vyhození do odpadu.	Přepsání: Začernění. Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje.	Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.	
Mobilní zařízení (mobilní telefony, tablety)	Odstranění: Vymazání informací, reset zařízení do továrního nastavení.	Přepsání: Pro zařízení s šifrovaným úložištěm - odstranění informací a reset do továrního nastavení.	Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací.	
Síťová zařízení (router, switch, modem a podobně)	Odstranění: Vymazání informací, reset do továrního nastavení.	Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy a podobně.).		
Kancelářské vybavení (scanery, tiskárny, fax)				
Magnetická média (magnetické pásky, disky, HDD [Hard Disk Drive])	Odstranění: Smazání dat na úrovni souborového systému.	Přepsání: Přepsání dat. V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů		
Optická média (CD, DVD, HD-DVD, BLU-RAY)			Fyzická likvidace: Zničení nosiče informací.	

GORDIC

www.gordic.cz

Tvorba evidenčních a hodnotících sestav

Výsledná hodnota		Dostupnost			Nedostupnost 15 min	Nedostupnost 1h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 1den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více	Ztráta									Důvěrnost			Integrita	
		Dostupnost	Provozní doba pod SLA	Přípustná doba kumulovaných výpadků s měsíčním vyhodnocováním										Ztráta dat od zálohy (15 min)	Ztráta dat od zálohy (1 h)	Ztráta dat od zálohy (4 h)	Ztráta dat od zálohy (8 h)	Ztráta dat od zálohy (1 den)	Ztráta dat od zálohy (2 dny)	Ztráta dat od zálohy (1 týden)	Ztráta dat od zálohy (14 dní)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu
0	Nerelevantní																										
1	nízká	96,16%	Provozní doba pod SLA: minimálně určených 10 hodin v pracovní dny. Nezapočítávají se dny pracovního volna a dny pracovního klidu stanovené pro ČR. Např. r. 2018 má 250 pracovních dní, na bázi 10 hod. pod SLA denně, což dává max. měsíční výpadek 8,3 hod. při dostupnosti 96 % (vztaženo na dobu pod SLA).	Max. 8 hod., avšak pouze v rámci definované pracovní doby	1	1	1	1	1	1	2	2	2	nejvyšší hodnota									nejvyšší hodnota			nejvyšší hodnota	
2	střední	99,45%	Provozní doba pod SLA: 24x7 (připravenost pro služby související s úplným el. podáním). Avšak určité služby, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu. To znamená, že el. podání bude obvykle fungovat nepřetržitě, ale reakce poskytovatele na nahlášené incidenty je omezena.	Max. 4 hod. na bázi 24x7	1	1	1	2	2	3	3	3	3														
3	vysoká	99,90%	Provozní doba pod SLA: 24x7 (připravenost pro služby úplného el. podání). Určité služby, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu.	Max. 43 min. na bázi 24x7	1	1	3	3	3	3	4	4	4														
4	kritická	99,99%	Plně fault-tolerantní systém s georedundancí a replikací transakčních dat. Smluvní penále při výpadku dostupnosti služby delší než celkem 52 minut za rok (odpovídá 99,99 %).	Jednotlivý výpadek max. 15 min. Max. kumulovaný roční výpadek 52 min. (odpovídá 99,99 %)	1-2	3-4																					

STUPNICE PRO HODNOCENÍ HROZEB		
1	nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
2	střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby

Tabulky | Matice dopadu | Katalog primárních aktiv | Vazby prim. aktiv | S1 | P1 | P2 | P3

C	D	E	F	G	H	I	J	K	
Úroveň	Ochrana osobních údajů - dopady na subjekty údajů (písmeno a) VKB)	Ochrana osobních údajů - finanční újma subjektů údajů (písmeno a) VKB)	Obchodní tajemství (písmeno a) VKB)	Zákonné a smluvní povinnosti (písmeno b) VKB)	Narušení vnitřních řídících a kontrolních činností (písmeno c) VKB)	Veřejný pořádek (písmeno d) VKB)	Finanční ztráty (písmeno d) VKB)	Zajišťování nezbytných nebo základních služeb* (písmeno e) VKB)	Naruš… (…
nízká	Může vést k **nepohodlí subjektu osobních údajů** (podrážděnost, krátkodobé časové nároky pro opětovné zadávání údajů, nutnost další komunikace s organizací).	*žádné vodítko*	*žádné vodítko*	*žádné vodítko*	*žádné vodítko*	Může přímo nebo nepřímo vést ke **ztrátám menším než 0,05 %** ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit **drobné komplikace pro malé množství osob.**	K naru… nedochá… **časovým** b…
střední	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).	Odhadovaná finanční **újma do 5000 Kč/subjekt údajů.**	Může mít **negativní dopad** na skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu.	Může zapříčinit **porušení interních předpisů a postupů**, nikoli však porušení zákonných a smluvních povinností, např. provozní důvody, nedostatek zaměstnanců.	Může mít **negativní dopad** na řídící a kontrolní činnosti organizace.	Může zapříčinit rozsahem, formou nebo místem **omezené protesty (lokální nepokoje).**	Může přímo nebo nepřímo vést ke **ztrátám mezi 0,05 % a 2 %** ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit **omezení či narušení** nezbytných nebo základních služeb pro **malé množství osob,** může způsobit **krátkodobý výpadek** služeb organizace. Může způsobit méně závažné finanční ztráty.	Může **om…** činností, **…fungování** č…
vysoká	Může vést k **závažné újmě subjektu osobních údajů** (napadení, nepříznivý zdravotní stav, deprese, ztížené uplatnění, ekonomické znevýhodnění (černé listiny), krádež identity, předvolání vyšetřujícími orgány).	Odhadovaná finanční **újma od 5000 Kč do 50 000 Kč/subjekt údajů** (zneužití finančních prostředků subjektu údajů, poškození majetku).	Může mít **podstatný dopad** na skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu.	Může zapříčinit **správní nebo občanskoprávní řízení** vedoucí k pokutě nebo k náhradě škody.	Může mít **podstatný dopad** na řídící a kontrolní činnosti organizace a zapříčinit **dočasné zastavení chodu či podstatný zásah do fungování organizace**, značné finanční ztráty související s obnovením chodu.	Může zapříčinit rozsahem, formou nebo místem **omezené protesty na úrovni významné části správního území obce s rozšířenou působností,** jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje.	Může přímo nebo nepřímo vést ke **ztrátám vyšším než 2 % a nižším či rovným 10 %** ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit **závažné omezení či narušení** nezbytných nebo základních služeb **pro větší množství osob, omezení** nebo **krátkodobé zastavení** přístupu ke službám.	Může způ… **nebo pod…** činností o… rozvoj nebo…
kritická	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).	Odhadovaná finanční **újma od 50 000 Kč/subjekt údajů** (neschopnost splácet dluh, ztráta majetku).	Může mít **závažný dopad** na skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu.	Může zapříčinit **porušení právních předpisů** vedoucí k zahájení trestního stíhání.	Může mít **závažný dopad** na řídící a kontrolní činnosti a zapříčinit **dlouhodobé zastavení chodu** celé organizace.	Může zapříčinit **hromadné nepokoje,** např. generální stávku, nebo jinak závažně narušit veřejný pořádek s celostátními dopady.	Může přímo nebo nepřímo vést ke **ztrátám přesahujícím 10 %** ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit **rozsáhlé dlouhodobé omezení, narušení či nedostupnost** poskytování nezbytných nebo základních služeb pro **větší množství osob, může způsobit újmu** (např. soudní proces, likvidace, vznik nesplatitelného dluhu).	Může způso… běžný…
Popis kategorie	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.	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. Jaká finanční újma vznikne jednotlivým osobám, když budou narušeny jejich osobní údaje.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na ochranu obchodního tajemství organizace.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na plnění zákonných a smluvních povinností, kterými je organizace zavázána.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na vnitřní řídící a kontrolní činnosti organizace (kontrolní mechanismy organizace, její vedení, správu apod.).	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajištění veřejného pořádku.	V této kategorii je posuzováno, jak velké finanční ztráty může narušení primárních aktiv organizaci způsobit. Kategorie je relevantní zejména pro organizace generující zisk.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajišťování nezbytných nebo základních služeb.	V této kategor… dopad bude… aktiv na zajiš… organizace (s… rámci organi… zaměstnance…
				• Nemožnost vydání rozhodnutí v zákonné lhůtě z důvodu		• Nedostupnost informací zveřejňovaných na webu organizace	• Nedostupnost informací o fakturách	Narušení všech informací, procesů	• Narušení č… ekonomický…

Katalog aktiv
(primárních a podpůrných)

B1 | Typové primární aktivum

	Typové primární aktivum	Název	Kategorie	Specifikace	Gestor aktiva	Garant aktiva	Osobní údaje	Legislativa	Určený IS	Rozsah ISMS
S1	Služba certifikace senzorů	S1: Služba certifikace senzorů	služba	Zajištění procesu certifikace a evidence senzorů	náměstek sekce certifikací (Martin Novotný)	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)	ano	Zákon o certifikaci	ano	ano
P1	Seznam certifikovaných senzorů	P1: Seznam certifikovaných senzorů	informace	Seznam všech úspěšně certifikovaných senzorů a certifikátů samotných	náměstek sekce certifikací (Martin Novotný)	ředitelka odboru podpory (Renata Malá)	ne	Zákon o certifikaci	ano	ano
P2	Rozhodnutí	P2: Rozhodnutí	informace	Výsledné rozhodnutí certifikačního procesu - negativní i pozitivní	náměstek sekce certifikací (Martin Novotný)	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)	ano	Zákon o certifikaci, zákon č. 500/2004 Sb., správní řád	ano	ano
P3	Žádosti, technická dokumentace	P3: Žádosti, technická dokumentace	informace	Technická dokumentace a žádost o certifikaci, kterou zasílají jednotliví výrobci ke svým senzorům	náměstek sekce certifikací (Martin Novotný)	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)	ano	Zákon o certifikaci	ano	ano
P4	Informace o průběhu certifikace	P4: Informace o průběhu certifikace	informace	Informace o průběhu certifikace - kdo rozhodl, kdy došla žádost, průběh certifikace atd.	náměstek sekce certifikací (Martin Novotný)	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)	ano	Zákon o certifikaci, zákon č. 500/2004 Sb., správní řád	ano	ano
...	...	...: ...	...	...	...	...	...	...	...	...

Tabulky | Matice dopadu | Katalog primárních aktiv | Vazby prim. aktiv | S1 | P1 | P2 | P3 | P4


Evidence vazeb
mezi aktivy

	A	B	C	D	E	F	G	H
1	Vazby mezi primárními aktivy		S1	P1	P2	P3	P4	Komentář
2			Služba certifikace senzorů	Seznam certifikovaných senzorů	Rozhodnutí	Žádosti, technická dokumentace	Informace o průběhu certifikace	
3	S1	Služba certifikace senzorů		x	x	x	x	Primární aktivum S1 pracuje se všemi inf agendovém systému. Hodnoty služby cer senzorů jsou nejvyšší hodnoty, které byly pro jednotlivá primární aktiva P1-P4.
4	P1	Seznam certifikovaných senzorů	x					
5	P2	Rozhodnutí	x					
6	P3	Žádosti, technická dokumentace	x					
7	P4	Informace o průběhu certifikace	x					
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								


Evidence aktiv

Název primárního aktiva:	Služba certifikace senzorů
Gestor primárního aktiva:	náměstek sekce certifikací (Martin Novotný)
Garant primárního aktiva:	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru ce
Datum hodnocení:	02.11.2021

Výsledné hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	
Dostupnost	3
Ztráta	4
Důvěrnost	3
Integrita	3

Oblasti dopadu	**Dostupnost**									**Ztráta**									**Důvěrnost**			**Integrita**	
	Nedostupnost 15 min	Nedostupnost 1 h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 1den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více	Ztráta dat od zálohy (15 min)	Ztráta dat od zálohy (1 h)	Ztráta dat od zálohy (4 h)	Ztráta dat od zálohy (8 h)	Ztráta dat od zálohy (1 den)	Ztráta dat od zálohy (2 dny)	Ztráta dat od zálohy (1 týden)	Ztráta dat od zálohy (14 dní)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu
Ochrana osobních údajů - dopady na subjekty osobních údajů	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2
Ochrana osobních údajů - finanční újma subjektů údajů	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2
Obchodní tajemství																							
Zákonné a smluvní povinnosti	1	1	1	1	1	2	2	2	3	1	1	1	1	1	2	2	2	2	2	3	3	3	3
Narušení vnitřních řídících a kontrolních činností	1	1	1	1	1	2	2	2	3	1	1	1	1	1	2	2	2	2	1	1	1	2	3
Veřejný pořádek																							
Finanční ztráta																							
Zajišťovací prostředky																							
Narušení bezpečnostní politiky																							
Ztráta dat																							
Bezpečnostní incidenty																							
Dopad																							
Mezinárodní sankce																							

Úrovně dopadu	
0	nerelevantní
1	nízká
2	střední
3	vysoká
4	kritická

Název primárního aktiva:	Rozhodnutí
Gestor primárního aktiva:	náměstek sekce certifikací (Martin Novotný)
Garant primárního aktiva:	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)
Datum hodnocení:	19.10.2021
Dostupnost	2

Název primárního aktiva:	Žádosti, technická dokumentace
Gestor primárního aktiva:	náměstek sekce certifikací (Martin Novotný)
Garant primárního aktiva:	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)
Datum hodnocení:	02.11.2021
Dostupnost	3

Jak na analýzu rizik?

B) ONLINE PORTÁLOVÉ ŘEŠENÍ

Reference


MĚSTSKÁ ČÁST
PRAHA 8


Český úřad pro
zkoušení zbraní a
střeliva
www.cuzzs.cz


ÚŘAD PRO CIVILNÍ LETECTVÍ


EOP
ELEKTRÁRNY
OPATOVICE


Karlovarský
kraj


SPRÁVA
ZÁKLADNÍCH
REGISTRŮ


mero
MERO ČR, a.s.


jihočeské
nemocnice


Draslovka


PROGRESSIVE
PSTCLC
LOGISTICS
MITSUI-SOKO GROUP


energy
Energie pro budoucnost a stabilitu


innogy


Evidence aktiv

Navigace
Dashboard
Nastavení
Číselníky
Registr rizik
Definice opatření
Aktiva 45
Mapa aktiv
Hodnocení rizik 87
Hodnocení opatření
Plán zvládání rizik
POA - ZoKB
POA - ISO
Plán kontinuity
Hodnocení dodavatelů
BU / BI
Auditní log

Aktiva

V nástroji jsou **předdefinované dvě kategorie aktiv: primární a podpůrná**.
Primární aktivum je informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém.
Podpůrné aktivum může být technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému.

Import | Exportovat vše | + Vytvořit

Primární aktiva | Aktiva | Katalog aktiv | Správa štítků | Správa vazeb

označené položky:
exportovat | stáhnout karty aktiv | editovat

Název aktiva	Podkategorie	Typ	Garant	Dopad	Schváleno VKB	Štítky
	vyberte	vyberte	vyberte	-	-	vyberte
SPISOVÁ SLUŽBA	VIS	Služba	Jakub Skalický	4/Kritický / 4	✓	Spisová služba
ÚŘEDNÍ DESKA	VIS	Služba	František Janů	4/Kritický / 4	✓	ÚŘEDNÍ DESKA
EMAIL	VIS	Služby	Garant Prinární	4/Kritický / 4	✓	EMAIL
REJSTŘÍK	VIS	Software	Vojtěch Hvězda	4/Kritický / 4	✓	REGISTR

(Položek: 1 - 4 z 4)

25

Navigace
Dashboard
Nastavení
Číselníky
Registr rizik
Definice opatření
Aktiva 45
Mapa aktiv
Hodnocení rizik 88
Hodnocení opatření
Plán zvládání rizik
POA - ZoKB
POA - ISO
Plán kontinuity
Hodnocení dodavatelů
BU / BI
Auditní log
Uzavřít modul

Přehled závislostí pro aktivum SPISOVÁ SLUŽBA

Druhy aktiv

- Ostatní
- Podpůrné
- Primární
- Nezařazeno

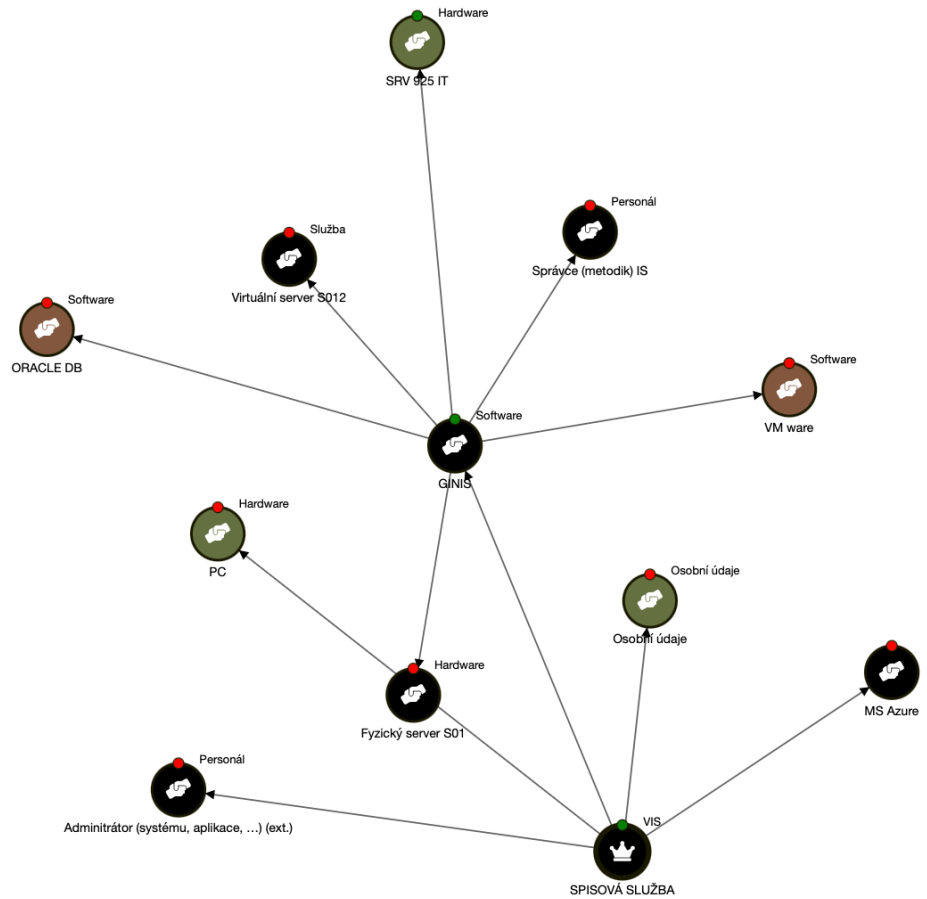
IS KII / KS KII / VIS / ISZS

Štítky

vyberte

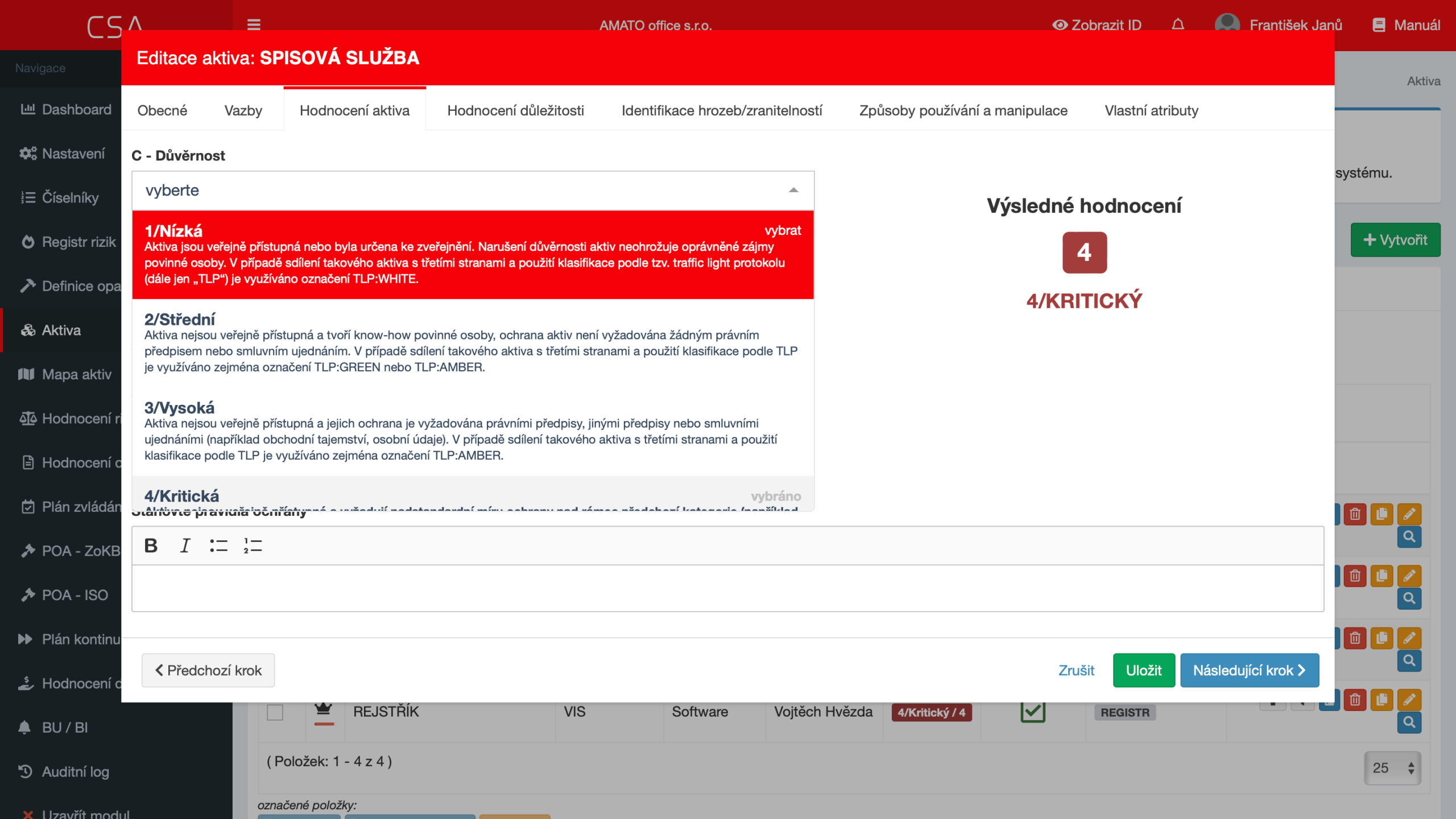
Klasifikace rizik

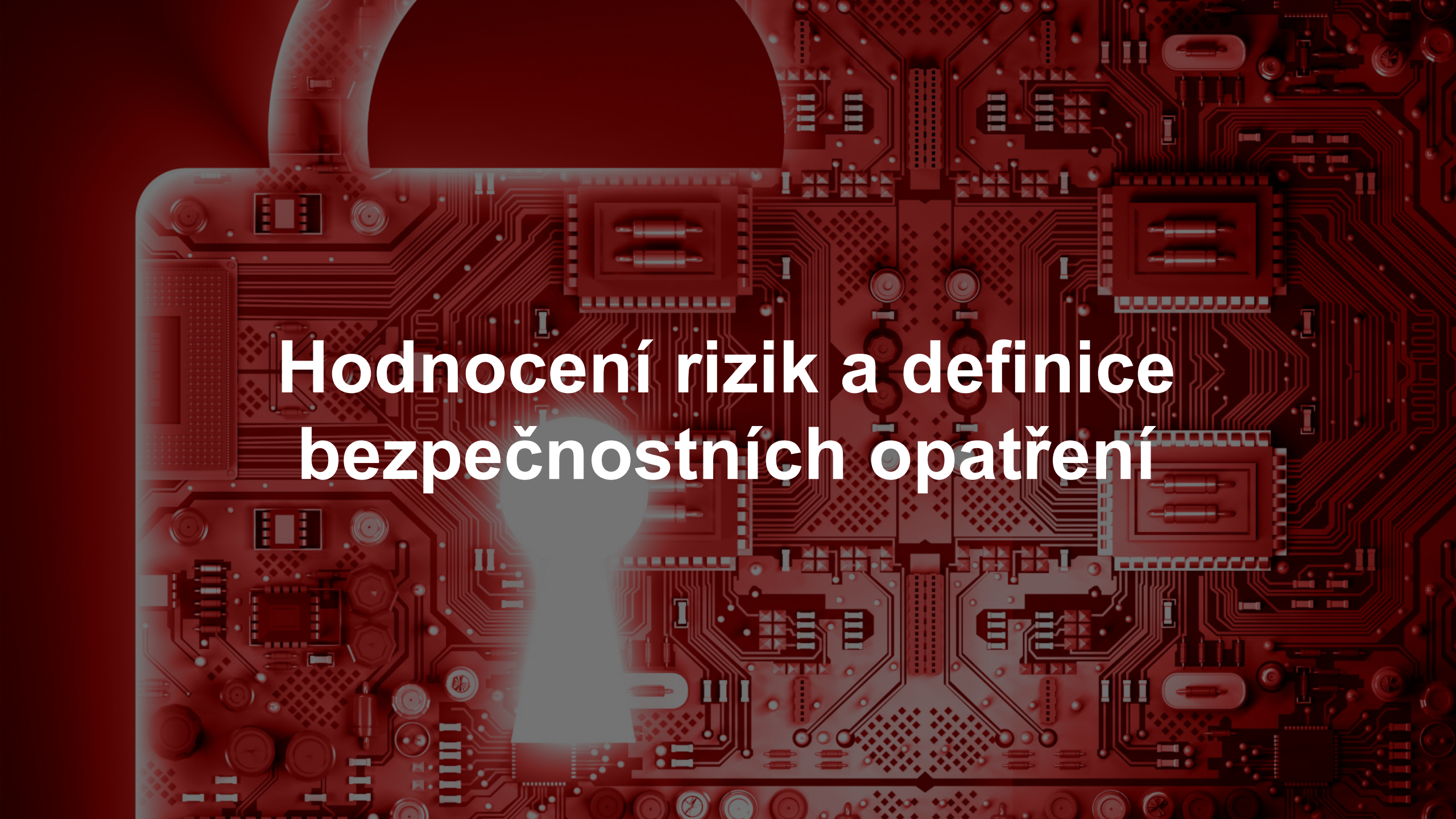
- Nízké
- Střední
- Vysoké
- Kritické
- Neohodnoceno



Zavřít

Hodnocení aktiv


AMATO office s.r.o.
Zobrazit ID
František Janů
Manuál
Navigace
Dashboard
Nastavení
Číselníky
Registr rizik
Definice opa
Aktiva
Mapa aktiv
Hodnocení r
Hodnocení o
Plán zvládán
POA - ZoKB
POA - ISO
Plán kontinu
Hodnocení o
BU / BI
Auditní log
Uzavřít modul
Editace aktiva: SPISOVÁ SLUŽBA
Obecné
Vazby
Hodnocení aktiva
Hodnocení důležitosti
Identifikace hrozeb/zranitelností
Způsoby používání a manipulace
Vlastní atributy
C - Důvěrnost
vyberte
1/Nízká
vybrat
Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP:WHITE.
2/Střední
Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:GREEN nebo TLP:AMBER.
3/Vysoká
Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:AMBER.
4/Kritická
vybráno
Stanovte pravidla ochrany
Výsledné hodnocení
4
4/KRITICKÝ
Předchozí krok
Zrušit
Uložit
Následující krok
Aktiva
systému.
+ Vytvořit
REJSTŘÍK
VIS
Software
Vojtěch Hvězda
4/Kritický / 4
REGISTR
(Položek: 1 - 4 z 4)
25
označené položky:



Hodnocení rizik a definice bezpečnostních opatření

Hodnocení rizik

Přehled identifikovaných rizik pro jednotlivá aktiva/zranitelnosti. Každé riziko je nutné ohodnotit, abyste získali míru daného rizika. V přehledu zároveň vidíte, jaké je aktuální výsledné riziko a cílené riziko, kterého chcete dosáhnout po aplikování všech opatření.

Rizika hodnotíte na každém aktivu/zranitelnosti zvlášť. Výsledné riziko se vypočítává ze tří faktorů:

- **Dopad** - Co by pro vaši organizaci znamenalo, pokud by hrozba nastala? Jaký by měla dopad?
- **Hrozba** - Jak je pravděpodobné, že dojde k realizaci hrozby?
- **Zranitelnost** - Jak je pravděpodobné, že dojde ke zneužití zranitelnosti? Jak moc je zranitelnost závažná?

Aktiva s nejvyšší hodnotou rizika | Rizika

Exportovat vše

označené položky:
exportovat | stáhnout karty rizik | přiřadit opatření

Aktivum	Druh	Garant	Druh hrozby	Druh zranitelnosti	Dopad	Hrozba	Zranitelnost	Riziko	Cílené riziko	Výsledné riziko	Opatření	Akceptováno	
	Podpůrné	vyberte			vyberte	vyberte	vyberte	vyberte	vyberte	vyberte		-	resetovat
Dodávky nepřerušitelného napájení el. energií	Podpůrné	Ondřej Chrást	Narušení fyzické bezpečnosti	Nedostatečná ochrana aktiv	4/Kritický / 4	3/Vysoká / 3	3/Vysoká / 3	Vysoké / 36 (56%)	Nízké / 16 (25%)	Vysoké / 36 (56%)	2 / 1 / 0	ne | a	
Dodávky nepřerušitelného napájení el. energií	Podpůrné	Ondřej Chrást	Pochybení ze strany zaměstnanců	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	4/Kritický / 4	3/Vysoká / 3	3/Vysoká / 3	Vysoké / 36 (56%)	Vysoké / 36 (56%)	Vysoké / 36 (56%)	0 / 0 / 0	ne | a	
Evidence síťových prvků	Podpůrné	Garant Podpůrný	Zneužití oprávnění	Známé chyby v programech	2/Střední / 2	4/Kritická / 4	4/Kritická / 4	Střední / 32 (50%)	Střední / 32 (50%)	Střední / 32 (50%)	0 / 0 / 0	ne | a	
Evidence síťových prvků	Podpůrné	Garant Podpůrný	Nezákonné zpracování dat	Spuštění nepotřebných služeb	2/Střední / 2	4/Kritická / 4	4/Kritická / 4	Střední / 32 (50%)	Nízké / 4 (6%)	Střední / 32 (50%)	1 / 0 / 0	ne | a	

Evidence bezpečnostních opatření

Navigace
Dashboard
Nastavení
Číselníky
Registr rizik
Definice opatření
Aktiva 47
Mapa aktiv
Hodnocení rizik 90
Hodnocení opatření
Plán zvládání rizik
POA - ZoKB
POA - ISO
Plán kontinuity
Hodnocení dodavatelů

Plán zvládání rizik

Plán zvládání rizik slouží pro řízení implementace jednotlivých opatření snižujících riziko dotčených aktiv.

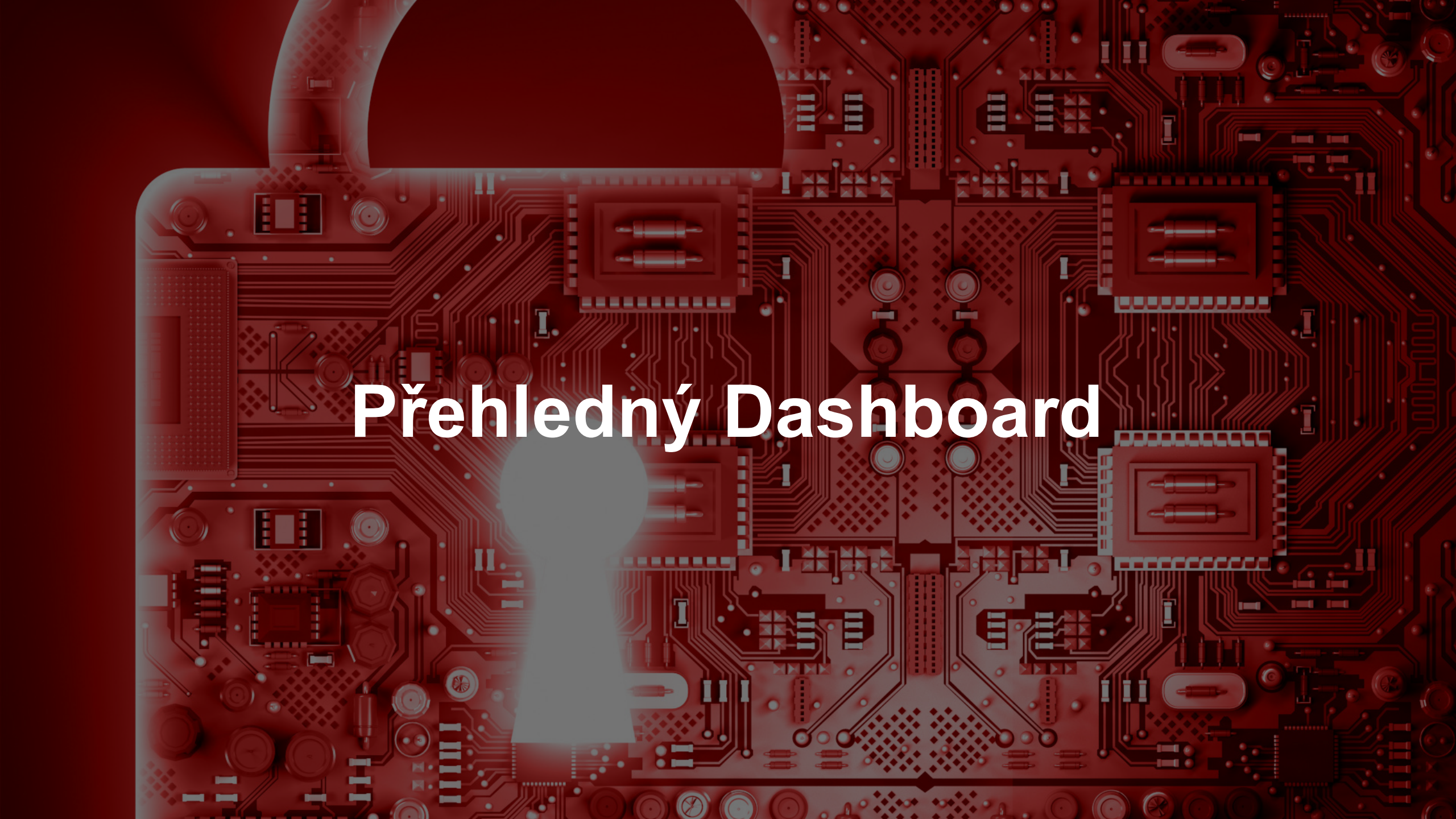
Plány | Aktiva

označené položky:
exportovat

Opatření	Finance	Zahájení	Ukončení	Priorita	Zavedeno
				vyberte	
Úprava smluvních vztahů	6000 Kč				0/1
Definice a vypracování popisu interních postupů	91000 Kč			střední	4/6
Definice rozsahu ISMS	200000 Kč	1. 1. 2021	31. 3. 2021	vysoká	3/5
Pravidelné zálohování	0 Kč				1/1
Omezení přístupu	305000 Kč	30. 11. 2020	21. 1. 2021	vysoká	0/2

(Položek: 1 - 5 z 5)

25


Přehledný Dashboard

- Dashboard
- Nastavení
- Číselníky
- Registr rizik
- Definice opatření
- Aktiva 45
- Mapa aktiv
- Hodnocení rizik 87
- Hodnocení opatření
- Plán zvládání rizik
- POA - ZoKB
- POA - ISO
- Plán kontinuity
- Hodnocení dodavatelů
- BU / BI
- Auditní log
- Uzavřít modul

Dashboard

AKTIVA

Celkem	79
Neohodnoceno	45

BU / BI

Celkem	7
Nevyřešeno	6

DODAVATELÉ

Celkem	6
Oznámení	1

PROVOZOVATELÉ

Celkem	4
Oznámení	3

Primární aktiva

Název aktiva	Garant	Nejvyšší riziko
EMAIL	Garant Prinární	Kritické / 64 (100%)
ÚŘEDNÍ DESKA	František Janů	Kritické / 64 (100%)
REJSTŘÍK	Vojtěch Hvězda	Vysoké / 48 (75%)
SPISOVÁ SLUŽBA	Jakub Skalický	Vysoké / 48 (75%)

Podpůrná aktiva

Název aktiva	Garant	Nejvyšší riziko
Interní procesy	Lucie Juřičková	Kritické / 64 (100%)
Zaměstnanci	Alena Šuhajová	Kritické / 64 (100%)
Service desk	František Janů	Vysoké / 48 (75%)
VM ware		Vysoké / 48 (75%)
GINIS	Jakub Skalický	Vysoké / 48 (75%)
Dodávky nepřerušitelného napájení el. energií	Ondřej Chrást	Vysoké / 36 (56%)
ORACLE DB	Garant Podpůrný	Vysoké / 36 (56%)
Prostory ICT (Servovna)	František Janů	Vysoké / 36 (56%)
ZIS - Zákaznický IS >		Vysoké / 36 (56%)
Kamerový systém	Tomáš	Vysoké / 36 (56%)

Rizika dle kategorie

☐ pouze primární aktiva

Celkem	94
Neošetřená	7
Automaticky akceptovaná	6
Manuálně akceptovaná	1

Rizika dle hrozby a zranitelnosti

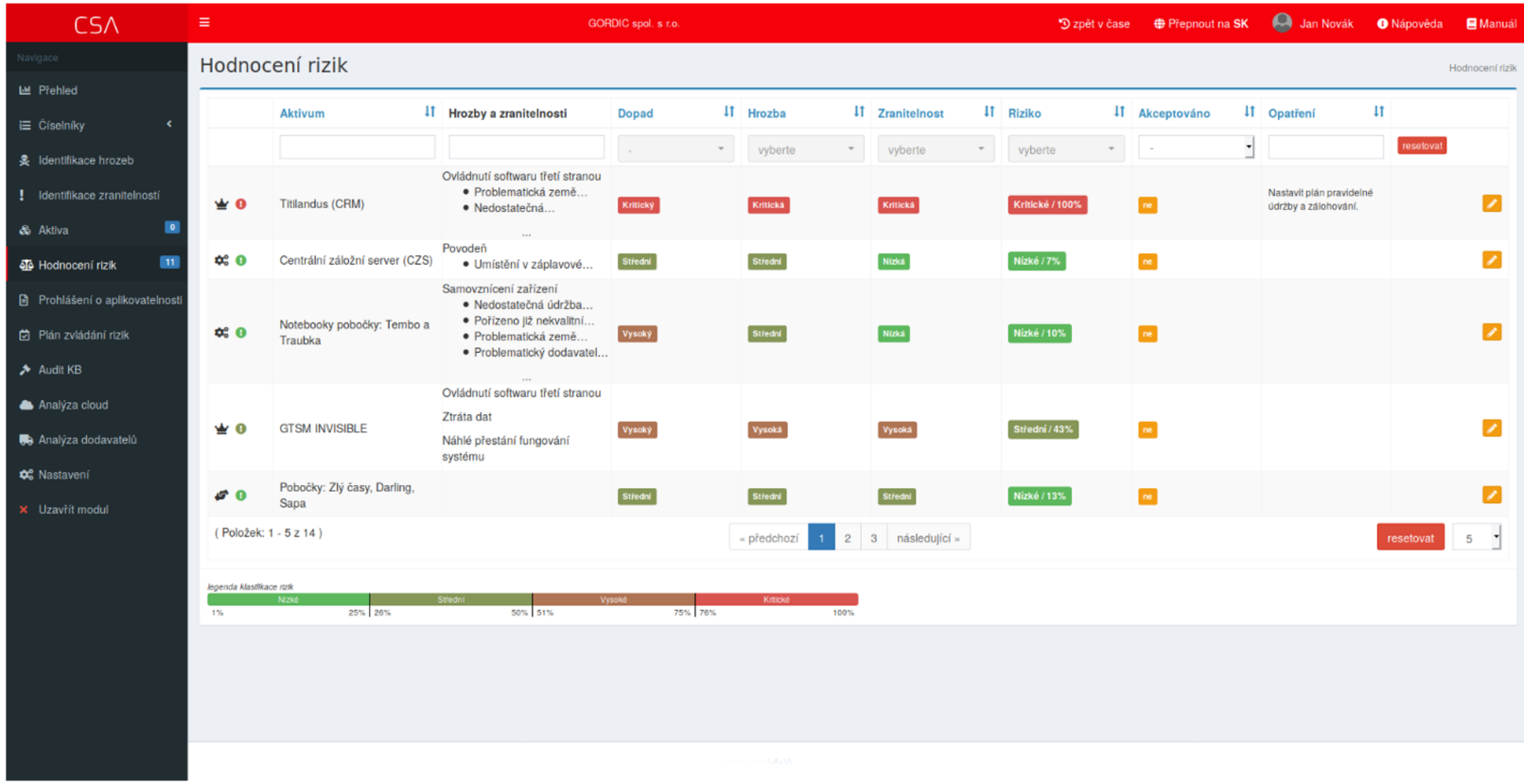
☐ pouze primární aktiva

Hrozby		Zranitelnosti	
neohodnoceno	59	neohodnoceno	64
1/Nízká	4	1/Nízká	3
2/Střední	12	2/Střední	5
3/Vysoká	13	3/Vysoká	13
4/Kritická	6	4/Kritická	9

CSA - Cyber Security Audit

- **ANALÝZA RIZIK A ŘÍZENÍ BEZPEČNOSTI V JEDNOM**

Díky aplikaci CSA zvládnete zpracovat evidenci aktiv, analýzu rizik a budete řídit procesní náležitosti kybernetické bezpečnosti.



GORDIC

www.gordic.cz

Nejdůležitější bezpečnostní opatření

- ***Analýza rizik*** a politiky bezpečnosti informací;
- ***Sběr a vyhodnocení bezpečnostních událostí***, Zvládání incidentů;
- Kontinuita činností (tj. business kontinuita), přičemž směrnice tento okruh ještě rozvádí o příklad zálohování, zotavení (disaster recovery) a krizové řízení;
- Bezpečnost v rámci dodavatelského řetězce;
- Bezpečnost v rámci pořízení, vývoje a údržby systémů;
- Segmentace sítě;
- Praktiky ***základní počítačové hygieny a vzdělávání*** v oblasti kybernetické bezpečnosti;
- Politiky a postupy týkající se využívání kryptografie a tam, kde je to vhodné, také šifrování;
- Bezpečnost lidských zdrojů, řízení přístupů a aktiv, ***Školení informační bezpečnosti;***
- Využívání vícefaktorového ověření identity, bezpečných komunikačních nástrojů a nástrojů pro nouzovou komunikaci.

**zdroj NÚKIB*

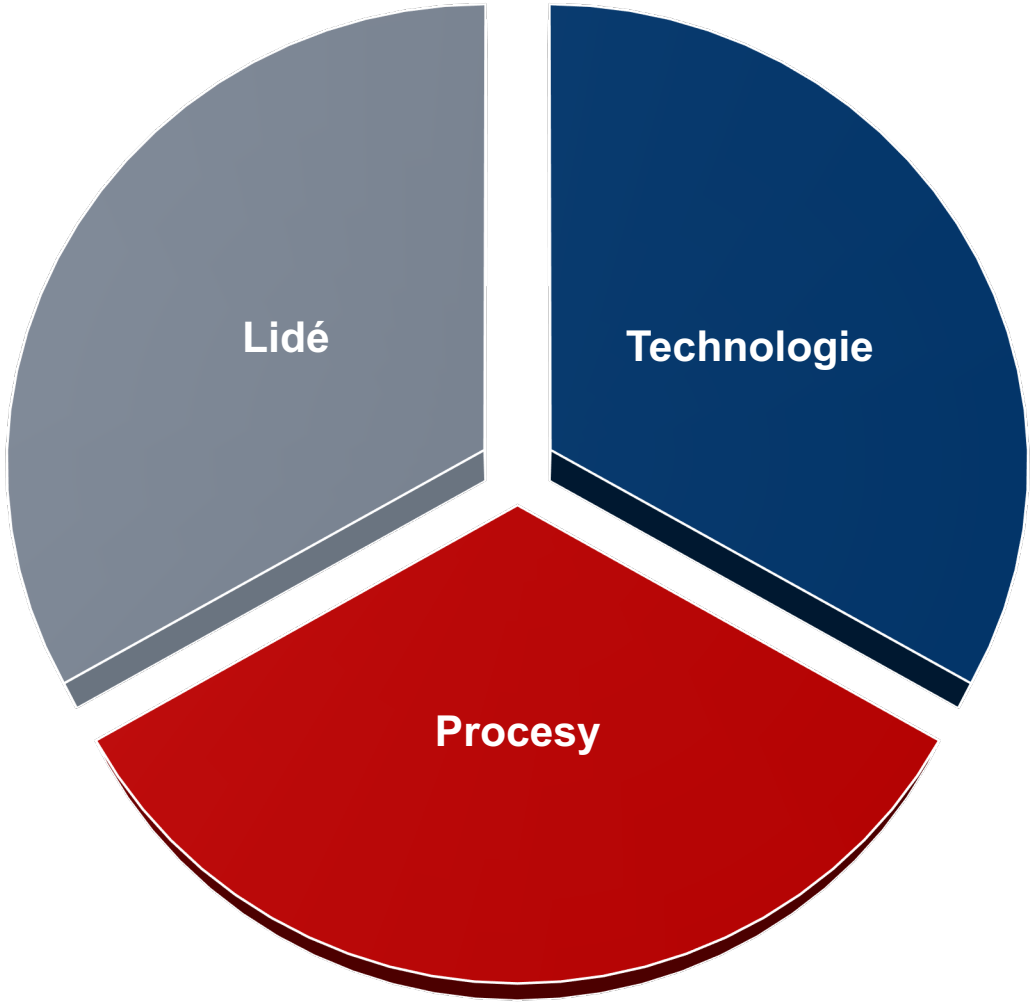
CISO a Ředitel odboru Správa informační bezpečnosti

- celoživotní nadšenec do nových technologií
- 20+ let v oboru informační bezpečnosti
- programátor, IT specialista, forenzní analytik, manažer
- působení v ČS, sIT Solutions, ESET

- vášnivý kutil
- chovatel jedné z nejnebezpečnějších psích ras

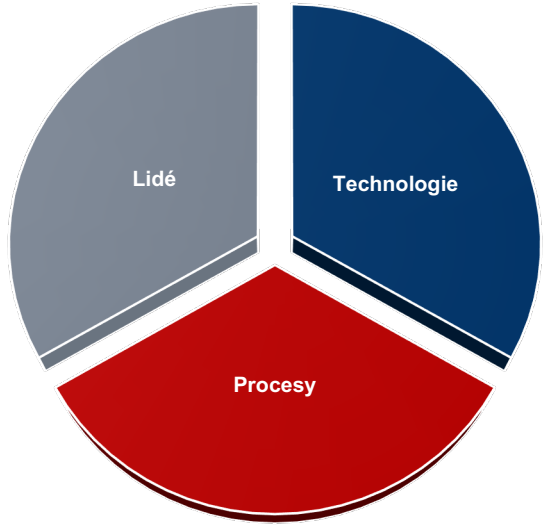
Ing. Miroslav Dvořák

Informační bezpečnost



Redukce plochy pro útok – TOP příklady

- členěte síť na menší celky (segmentace)
- sledujte síťový provoz a zajistěte centralizované a časově synchronizované logování síťových událostí
- důsledně kontrolujte příchozí e-maily
- udržujte aktuální operační systém i aktuální aplikační software
- zaveďte centrální správu uživatelských účtů a oprávnění
- stanovte pravidla pro více faktorovou autentizaci
- vypracujte Incident response plan (IRP) a Disaster recovery plan (DRP)
- zaveďte pravidelná školení informační bezpečnosti pro zaměstnance
- pravidelně provádějte testy sociálního inženýrství



https://www.govcert.cz/cs/informacni-servis/doporuceni/2736-doporuceni-nukib-pro-administratory-verze-4-0/

Co pro vás máme a chystáme a kde vám můžeme pomoci

- Monitorování externí útočné plochy
- Centrální správa bezpečnostních událostí a reakce na ně
- Záplatování aplikací a operačních systémů za běhu
- Školení informační bezpečnosti

Monitorování externí útočné plochy

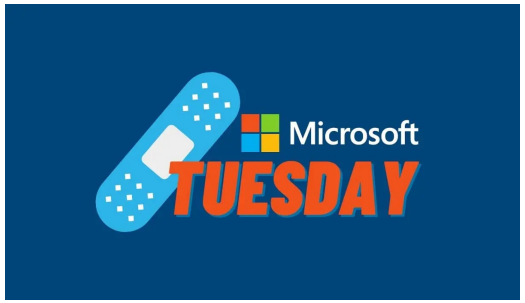
- SaaS / MSSP
- pohled útočníka na vaše informační aktiva dostupná z internetu - OSINT přístup, inventarizace služeb, technologií, DNS, certifikátů, zranitelností, …
- monitorování obsahu tzv. „Dark webu“ – uniklé přihlašovací údaje, kompromitovaná aktiva, integrovaný nákup
- ochrana jména společnosti - podvodné domény, účty na sociálních sítích, integrovaný „takedown“
- TI data – vulnerability, supply chain intelligence, IOC feed, threat hunting rules, …

Centrální správa bezpečnostních událostí a reakce na ně

- SaaS / MSSP
- otevřená platforma sdružující funkce SIEM, E/XDR, SOAR
- využívá stávající bezpečnostní technologie, resp. jejich data
- AI zajišťuje korelace a řetězení bezpečnostních událostí
- funguje jak vůči interní, tak cloudové infrastruktuře

Záplatování aplikací a operačních systémů za běhu

- SaaS / MSSP
- doručení bezpečnostních záplat na kritické systémy v řádu maximálně hodin
- umožnuje záplatovat i již nepodporované aplikace a operační systémy
- bezproblémová koexistence se stávajícími systémy pro záplatování bezpečnostních děr



Anketa

- Pomozte nám se zpětnou vazbou na naši přednášku a navštivte anketu na Slido.com s kódem **#3210** nebo využijte následující QR kód.

- Pokud chcete vědět o některém z témat více, jsme k dispozici na našem stánku nebo nás kontaktujte na e-mailové adrese: obchodpraha@gordic.cz

Děkujeme za pozornost.

František Janů - vedoucí oddělení Služby Cyber Security
Miroslav Dvořák - ředitel odboru Správa informační bezpečnosti