

Microsoft Excel jako nástroj při řízení rizik

Roman Skalík

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Roman Skalík
Osobní číslo: A20251
Studijní program: B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia: Prezenční
Téma práce: Microsoft Excel jako nástroj při řízení rizik
Téma práce anglicky: Microsoft Excel as a Risk Management Tool

Zásady pro vypracování

1. Popište a vysvětlete základní pojmy v oblasti řízení a analýzy rizik.
2. Analyzujte jednotlivé kroky řízení rizik.
3. Navrhněte model nástroje, který bude podporovat jednotlivé kroky řízení rizik, identifikaci aktiv, katalogu hrozeb a zranitelností, přehled rizik a odpovědností.
4. Porovnejte nástroj na modelové situaci a zhodnoťte jeho efektivitu v procesu řízení rizik.
5. Vyhodnoťte, jak nástroj usnadňuje proces řízení rizik, a diskutujte jeho možnosti pro praktické využití.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management: [teorie a praxe ochrany majetku a fyzické bezpečnosti]*. Zlín: VeRBuM, 2011-. ISBN 9788087500057.
2. MAREŠ, Miroslav; REKTOŘÍK, Jaroslav a ŠELEŠOVSKÝ, Jan. *Krizový management: případové bezpečnostní studie*. Praha: Ekopress, 2013. ISBN 9788086929927.
3. SMEJKAL, Vladimír a RAIS, Karel. *Řízení rizik. Expert*. Praha: Grada, 2003. ISBN 8024701987.
4. ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. V Tribun EU vyd. 1. *Knihovnicka.cz*. Brno: Tribun EU, 2009. ISBN 9788073997311.
5. TICHONĚ, Pavel. *Excel*. [Praha]: Pavel Tichoně – Individuum ve spolupráci s Pragovka Gallery, [2023]. ISBN 978-80-908879-2-3.

Vedoucí bakalářské práce: **Ing. Lukáš Králík, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **11. prosince 2024**
Termín odevzdání bakalářské práce: **2. června 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 11. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Bakalářská práce se v teoretické části zabývá vymezením základní terminologie v oblasti řízení rizik a popisem jednotlivých kroků procesu, včetně identifikace aktiv, hrozeb a zranitelností. Praktická část je zaměřena pro návrh a implementaci nástroje do softwaru Microsoft Excel s využitím automatizace a vizualizací výstupů. Výstupem práce je vyhodnocení efektivity nástroje procesu řízení rizik.

Klíčová slova: bezpečnost, řízení rizik, analýza rizik, Excel

ABSTRACT

The theoretical part of this bachelor thesis focuses on defining the basic terminology in the field of risk management and describing the individual steps of the process, including the identification of assets, threats, and vulnerabilities. The practical part is aimed at the design and implementation of a tool in Microsoft Excel, utilizing automation and output visualization. The outcome of the thesis is an evaluation of the tool's effectiveness within the risk management process.

Keywords: security, risk management, risk analysis, Excel

Touhle formou bych rád vyjádřil vděk svému vedoucímu práce panu Ing. Lukáši Králíkovi, Ph.D. za odbornou pomoc, rady a ochotu spolupracovat při tvorbě mé bakalářské práce. Další poděkování patří mé rodině, mým spolužákům a kamarádům, kteří mi věřili a podporovali mě ve studiu.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	12
1 ŘÍZENÍ RIZIK.....	13
1.1 AKTIVUM	13
1.2 HROZBA	13
1.3 ZRANITELNOST.....	14
1.4 RIZIKO.....	14
1.5 ZBYTKOVÉ RIZIKO.....	15
1.6 PROTIPATŘENÍ.....	15
1.7 PROCES ŘÍZENÍ RIZIK	15
1.8 ANALÝZA RIZIK.....	16
1.9 METODY ANALÝZY RIZIK	16
1.9.1 Kvalitativní metody.....	16
1.9.2 Kvantitativní metody.....	17
1.9.3 Kombinované metody	17
1.10 HODNOCENÍ RIZIK	17
1.11 REGULOVÁNÍ RIZIK	18
1.11.1 Redukce rizika.....	19
1.11.2 Retence rizika.....	19
2 VYUŽITÍ MICROSOFT EXCEL PRO ŘÍZENÍ RIZIK.....	20
2.1 PŘEHLED FUNKCÍ EXCELU VYUŽITELNÝCH V ŘÍZENÍ RIZIK.....	20
2.1.1 Datové tabulky a seznamy	20
2.1.2 Výpočty a automatizace hodnocení	20
2.1.3 Matice rizik a vizualizace.....	20
2.1.4 Grafické přehledy a dashboardy.....	21
2.2 VÝHODY A OMEZENÍ EXCELU.....	21
2.3 TABULKOVÝ PROCESOR.....	22
2.3.1 Nejrozšířenější tabulkové procesory	22
2.3.2 Srovnání tabulkových procesorů.....	23
II PRAKTICKÁ ČÁST.....	25
3 NÁVRH NÁSTROJE PRO ŘÍZENÍ RIZIK V MICROSOFT EXCEL	26
3.1 PRINCIP NÁSTROJE.....	27
3.2 IDENTIFIKACE DAT	28
3.2.1 Aktiva.....	28
3.2.2 Hrozby.....	28
3.2.3 Zranitelnosti	29

3.3	PROPOJENÍ VSTUPNÍCH DAT A HODNOCENÍ RIZIK	29
3.3.1	Výpočet a hodnocení rizikového skóre	30
3.4	NÁVRH OPATŘENÍ A PŘÍRAZENÍ ODPOVĚDNOSTÍ	30
3.5	VIZUALIZACE DAT A DASHBOARD.....	30
3.6	ROZHODOVÁNÍ O RIZICÍCH (MANAGEMENT)	31
3.7	AKTUALIZACE A MONITORING	31
4	IMPLEMENTACE NÁSTROJE V MICROSOFT EXCEL	33
4.1	ZAPISOVÁNÍ DAT	33
4.1.1	Princip zapisování dat přes makro.....	33
4.1.2	Katalog aktiv	33
4.1.3	Katalog hrozeb	35
4.1.4	Katalog zranitelností.....	37
4.2	PROPOJENÍ DAT A HODNOCENÍ RIZIK.....	38
4.2.1	Princip propojení	38
4.2.2	Hodnocení rizik	39
4.3	NÁVRH OPATŘENÍ A PŘÍRAZENÍ ODPOVĚDNOSTÍ	40
4.3.1	Výpočet rizikové skóre po zavedení opatření	41
4.4	VIZUALIZACE DAT	43
4.5	ROZHODOVÁNÍ O RIZICÍCH.....	45
4.6	AKTUALIZACE A MONITORING	45
5	POROVNÁNÍ NÁSTROJE NA MODELOVÉ SITUACI.....	46
5.1	MODELOVÁ SITUACE	46
5.2	ZÁKLADNÍ CHARAKTERISTIKA.....	46
5.3	IMPLEMENTACE DAT DO NÁSTROJE.....	47
6	VYHODNOCENÍ A VYUŽITELNOST NÁSTROJE	50
6.1	VYHODNOCENÍ NÁSTROJE	50
6.2	VYUŽITELNOST NÁSTROJE	51
	ZÁVĚR.....	52
	SEZNAM POUŽITÉ LITERATURY	53
	SEZNAM OBRÁZKŮ	55
	SEZNAM TABULEK.....	56
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	57
	SEZNAM PŘÍLOH.....	58

ÚVOD

Bezpečnost a řízení rizik představují důležité oblasti nejenom v průmyslových, ale také i digitálních a administrativních prostředích. Jelikož se neustále vyvíjí hrozby a narůstá komplexita informačních systémů je pro organizace nezbytné pracovat s nástroji, které umožní identifikaci, hodnocení i zvládání rizik.

Cílem této bakalářské práce je navrhnout a implementovat nástroj pro řízení rizik, který je postavený pro velmi dobře dostupnou a rozšířenou platformu – Microsoft Excel. Tento princip umožňuje jak analýzu, tak jednoduchou implementaci i pro organizace s omezeným rozhledem pro specializované softwary.

Teoretická část popisuje základní pojmy v oblasti řízení rizik jako jsou aktivum, hrozba, zranitelnost nebo riziko. Přibližuje chápání samotného procesu řízení rizik a jeho možností. Uvádí postup hodnocení rizik včetně regulování rizik po jejich identifikaci.

Praktická část práce se zaměřuje na vytvoření nástroje v systému Excel, který podporuje vedení katalogů aktiv, hroze a zranitelností, jejich vzájemné propojení a předem automatizované hodnocení rizik. Systém zahrnuje interaktivní zapisování dat do katalogů, výpočty rizikového skóre na základě definovaných parametrů, vizualizaci přehledů a seznam zavedených opatření. Součástí řešení je i logika sledování kontroly termínů a evidence odpovědnosti.

Zvolený přístup prezentuje možnosti, jak lze pomocí běžného softwaru vytvořit přehledné řešení pro řízení rizik. Data v nástroji mohou být snadno upravována díky své flexibilitě a konkrétním preferencím organizace a slouží jako prostředek pro strategické rozhodování a prevenci bezpečnostních incidentů.

I TEORETICKÁ ČÁST

1 ŘÍZENÍ RIZIK

Pro správné pochopení pojmů v bezpečnostním prostředí, je potřeba vysvětlit termíny používané v bakalářské práci, ale také přiblížit řízení rizik a jeho metody. Terminologie je ošemetná věc, proto vymezení pojmů jako riziko, hrozba, zranitelnost nebo aktivum jsou vysvětleny v podkapitole níže.

1.1 Aktivum

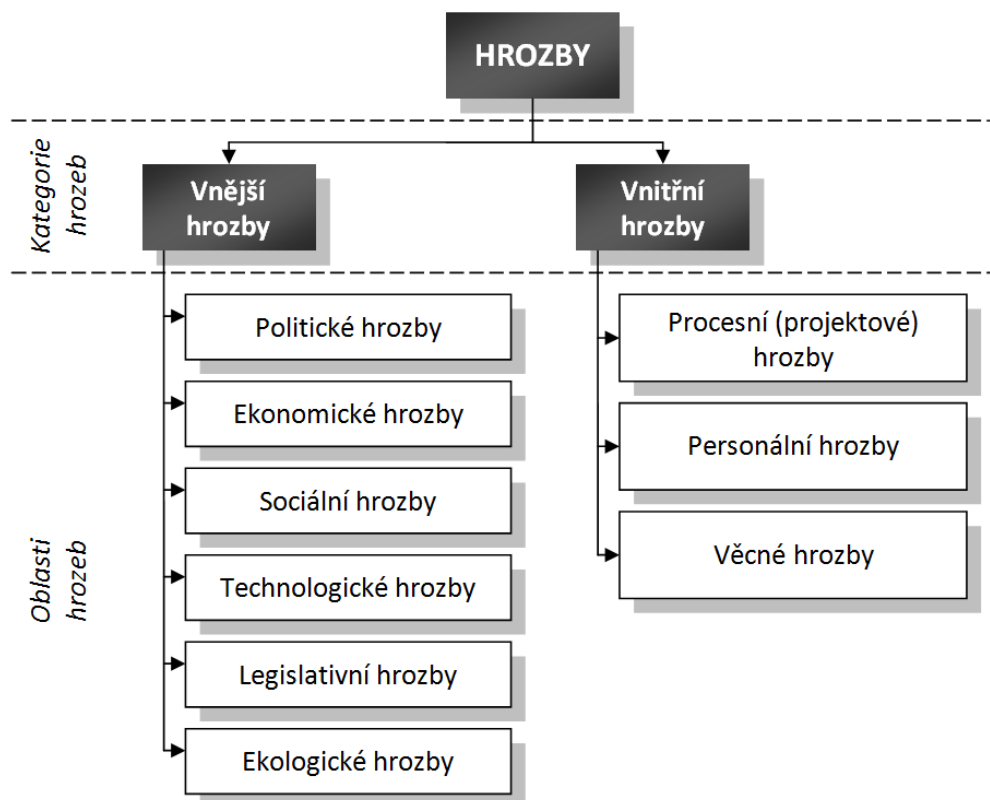
Jedná se o cokoliv, co má pro organizaci hodnotu a tato hodnota může být snížena působením hrozby. Aktiva se dají dělit a nejjednodušší způsob dělení aktiv je na hmotné a nehmotné. Mezi hmotné aktiva se dají považovat fyzické subjekty, například lidi, majetek ale i samotná nemovitost apod. K nehmotným aktivům se dají zařadit informace, know-how apod. [1]

1.2 Hrozba

Podle definice Ministerstva vnitra je hrozba přírodní nebo člověkem podmíněný proces, který představuje potenciál, jinak řečeno schopnost zdroje způsobit škodu. Spouští se buď zcela náhodně, nebo záměrně. V definici je také napsáno: „Hrozba bývá zdrojem rizika.“ [2] Výstižnost hrozby určuje její úroveň, která je hodnocena podle tří možností:

- nebezpečnost – „*schopnost hrozby působit škodu*“,
- přístup – „*možnost, že hrozba získá přístup k aktivu*“,
- motivace – „*zájem iniciovat hrozbu vůči aktivu*“. [3]

Hrozby se dají dělit ze dvou hledisek. První možnost dělení hrozeb je z pohledu úmyslných (které byly naplánované) a neúmyslných (které byly zcela náhodné). Druhá možnost, jak dělit hrozby je z pohledu zdroje na vnitřní a vnější hrozby (Obrázek 1), tedy rozdělení kategorií hrozeb do oblastí hrozeb. [4]



Obrázek 1 Vnější a vnitřní hrozby

(zdroj: [4])

1.3 Zranitelnost

Představuje jev, který vede k nějakému následku/dopadu, tj. stav aktiva, který by mohla hrozba zneužít k uplatnění svých nepříznivých účinků. Ke zranitelnosti dochází v případě interakce mezi aktivem a hrozbou. Hlavní výstižností zranitelnosti je její úroveň, která se hodnotí pomocí dvou faktorů:

- Citlivostí – „*náchylnost aktiva být poškozeno danou hrozbou*“,
- Kritičností – „*důležitost aktiva pro analyzovaný subjekt*“. [3]

1.4 Riziko

Riziko je rozšířený pojem propletený napříč různými odvětvími. Jednotlivé odvětví mohou mít vlastní porozumění pro definici, v oblasti bezpečnosti může být riziko chápáno jako interakce mezi hrozbou a aktivem. Vyjádření rizika se tak používá pravděpodobnost výskytu mimořádné události a dopad na aktivum. [3]

Podle teorie bezpečnosti v publikaci [5] představuje riziko pravděpodobnost negativního působení určité hrozby na referenční objekt. Toto působení může vést k

poškození nebo ohrožení chráněných hodnot, což se projevuje formou újmy, ztráty nebo jiného nežádoucího dopadu. Teorie rizik tedy zdůrazňuje dvě klíčové složky:

- Pravděpodobnost výskytu události (expozice¹ vůči hrozbě)
- Velikost následků této události (dopad na hodnotu)

1.5 Zbytkové riziko

Označení pro takové rizika, které i po zavedení bezpečnostních opatření stále přetrvává. Zbytkové rizika jsou zpravidla velmi nízké a neměly by přesáhnout referenční úroveň (akceptovatelná hranice rizika, která byla stanovena organizací nebo legislativou) aby bylo nutné zavádět bezpečnostní opatření za účelem snížení úrovně rizika. [7]

1.6 Protiopatření

Představuje proces, postup, technický nebo jiný prostředek pro zmírnění působení hrozby (v některých případech úplné odstranění hrozby), snížení zranitelnosti nebo dopadu hrozby. Vyznačuje se dvěma parametry:

- míra efektivity,
- výše nákladů. [3]

Účelem protiopatření je zabránit vzniku škody, nebo pokud již vznikla, usnadnit obnovu následků. [3]

1.7 Proces řízení rizik

Řízení rizik je postup, který se opakuje tak často, jak je to nutné nebo žádoucí. Účelem tohoto postupu je co nejvíce snížit a řídit rizika pomocí různých metod, jak zabránit účinkům nebezpečí, nebo způsoby, jak zmírnit účinky nebezpečí. [4]

Proces většinou probíhá ve třech fázích. První fází je **analýza rizik**, navazující fází je **vyhodnocení rizik** a závěrečnou fází je **zvládání rizik**. Proces analýzy a vyhodnocení rizik se označuje jako hodnocení rizik. [1]

Jelikož se jedná o proces, který je dobré opakovat pravidelně, nebo minimálně hned po vzniku bezpečnostního problému; je důležité velmi dobře znát povahu, prostory a prostředí ve kterém se subjekt nachází k úspěšnému procesu řízení rizik. [1]

¹ „Expozice je vystavení organismu působení faktorů prostředí.“ [6]

1.8 Analýza rizik

Označovaná jako proces, který lze chápat jako: „*definování hrozeb, pravděpodobností jejich uskutečnění a dopadu na aktiva, tedy stanovení rizik a jejich závaznosti*“ [3]. Nejobecnější plán analýzy rizik, kterým se dá řídit může obsahovat:

- identifikaci aktiv – vypsání aktiv, které subjektu náleží;
- stanovení hodnoty aktiv – ohodnocení aktiv a jejich smyslu pro subjekt, vyhodnocení dopadu jejich ztráty nebo poškození vůči chování subjektu;
- identifikaci hrozeb a slabin – vymezení kritických míst subjektu, vymezení činností, které negativně ovlivňují subjekt;
- stanovení závažnosti – stanovení pravděpodobnosti výskytu hrozeb a úrovně zranitelnosti vzhledem k příslušné hrozbě. [8]

Výsledky hodnocení rizik přispějí ke stanovení vhodných opatření, která organizace přijme, stejně jako priorit spojených s řízením rizik a implementací opatření, která zabrání vzniku těchto situací. Proces hodnocení rizik a stanovení kroků může být nutné opakovat vícekrát, aby byly pokryty různé části organizace. [3]

V každém případě je nezbytné určit, do jaké míry mají být analyzovaná rizika snížena. Snaha eliminovat všechna rizika by vedla k nemyslitelným nákladům na realizaci příslušných opatření a v každém případě by mohla negativně ovlivnit funkčnost organizace. [3]

V rámci analýzy rizik jsou zbytková rizika probírána a definována na základě míry jejich hodnocení ve vztahu k hrozbám, míře zranitelnosti a navrhovaným protiopatřením. Na základě toho je volen konkrétní přístup a metoda provádění analýzy rizik. [3]

1.9 Metody analýzy rizik

Jednotlivých metod analýzy rizik je velká spousta ale důležité je, podle kterých faktorů se rozdělují. Těmito faktory se vyznačují kvalitativní a kvantitativní metody. Používají se buď samostatně nebo v kombinacích. [3]

1.9.1 Kvalitativní metody

Kvalitativní metody jsou odvozeny od popisu závažnosti potenciálních následků a pravděpodobnosti, že k události dojde. Charakterizují se vyjádřením rizik definovaným

rozsahem, který může být obodovaný od 1 až do 10, nebo slovním způsobem (malé, střední, velké riziko). Kvalitativní metody jsou označovány za jednodušší i rychlejší ale o to více subjektivní. Problémové v oblasti zvládání rizik, zvažování finančních nákladů nezbytných k eliminaci hrozeb. Hrozby mohou být kvalitativní metodou charakterizovány například jako „nízká, velká, kritická“. [3]

1.9.2 Kvantitativní metody

Kvantitativní metody jsou odvozeny z matematického výpočtu rizika spojeného s četností výskytu hrozby a dopadem, který má. Číselné hodnoty se používají jak v případě pravděpodobnosti výskytu incidentu, tak i při ocenění dopadu. Obvykle popisují dopad v peněžním vyjádření, například „tisíce Kč“. Riziko se obvykle vyjadřuje jako očekávaná roční ztráta (annualized loss expectancy – ALE), která je vyjádřena jako peněžní hodnota. Kvantitativní metody jsou přesnější než kvalitativní metody, jejich implementace je sice časově náročnější, ale poskytují finanční popis rizik, který je pro jejich řízení výhodnější. [3]

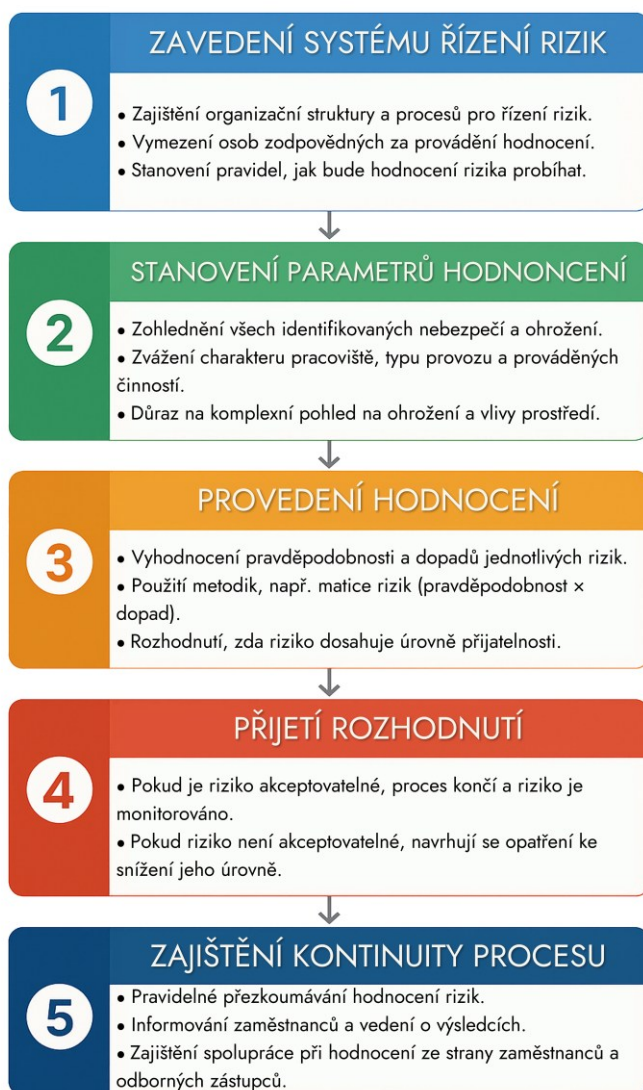
1.9.3 Kombinované metody

Kombinované metody využívají číselné informace. Kvalitativní přístup nám však umožňuje získat bližší vztah k hypotézám, které jsou založeny na kvantitativních metodách. Je však důležité si uvědomit, že data použitá v kvalitativních metodách nejsou nutně přímým důkazem pravděpodobnosti událostí nebo jejich dopadu, ale mohou být ovlivněna měřítkem použitým v konkrétní metodě. [3]

1.10 Hodnocení rizik

Důležitá fáze procesu analýzy rizik, která rozhoduje o dalším postupu organizace při zajišťování bezpečnosti. Cílem hodnocení rizik je určit, zda jsou existující rizika akceptovatelná, nebo zda je nutné přijmout další opatření ke snížení jejich dopadu nebo pravděpodobnosti výskytu. [3][5]

Postup hodnocení rizik v publikaci [5] je uveden jako „plán“, který by měl obsahovat body uvedené na obrázku č.2.



Obrázek 2 Postup hodnocení rizik

(zdroj: upraveno z [5])

Na základě výsledků hodnocení se rozhoduje o přijatelnosti rizika. Pokud je riziko nepřijatelné, navrhuje se opatření pro jeho regulaci. [5]

1.11 Regulování rizik

Regulace rizik představuje fázi řízení rizik, která následuje po jejich identifikaci, analýze a hodnocení. Hlavním cílem regulace rizik je zmírnit hrozby plynoucí z rizikových situací, minimalizovat škody nebo zabránit vzniku škod vůbec. Regulace znamená rozhodování o způsobu, jak se bude s konkrétním rizikem nakládat. [3][5]

Jednotlivé přístupy k regulaci rizik lze rozdělit do několika kategorií. Tato kapitola se zaměřuje na dvě z nich – redukci rizika a retenci rizika.

1.11.1 Redukce rizika

Redukce rizika je jedním z nejčastějších opatření při regulaci rizik. Cílem je snížit pravděpodobnost vzniku rizikové události nebo zmírnit její následky, pokud by k ní došlo. Redukce může být dosaženo jak preventivními opatřeními, tak reaktivními činnostmi zaměřenými na zmírnění dopadů rizika. [3][5]

Formy redukce rizika:

- Technická opatření – zavedení nových technologií, bezpečnostních systémů, modernizace výrobních zařízení.
- Organizační opatření – revize pracovních postupů, zajištění školení zaměstnanců, zvýšení bezpečnostní kultury.
- Bezpečnostní politika – zavedení norem, interních předpisů a pravidel v oblasti řízení bezpečnosti. [3][5]

1.11.2 Retence rizika

Retence rizika (též akceptace nebo přijetí rizika) znamená vědomé ponechání rizika bez zavedení dalších opatření ke zmírnění. Tato strategie se využívá, pokud:

- Riziko je hodnoceno jako přijatelné.
- Náklady na preventivní nebo ochranná opatření by byly vyšší než potenciální škody způsobené realizací rizika.
- Organizace je schopna nést důsledky, které by mohly z realizace rizika vyplynout. [3][5]

Retence je často kombinována s jinými opatřeními, například monitoringem a kontrolou vývoje rizika. Důležité podmínky retence rizika:

- Pravidelné sledování retencovaných rizik.
- Přezkum a vyhodnocení aktuálnosti rozhodnutí o ponechání rizika. [3][5]

2 VYUŽITÍ MICROSOFT EXCEL PRO ŘÍZENÍ RIZIK

Efektivní řízení rizik představuje systematický přístup k identifikaci, hodnocení a minimalizaci rizik, která mohou ohrozit cíle organizace [3]. Pro tento proces se často využívají specializované softwarové nástroje. Nicméně v mnoha případech, zejména v malých a středních organizacích, se jako dostupná a flexibilní alternativa nabízí Microsoft Excel [9]. Excel disponuje širokou škálou funkcionalit, které umožňují vytvářet propracované systémy pro řízení rizik, aniž by bylo nutné pořizovat nákladné softwarové řešení [10].

2.1 Přehled funkcí Excelu využitelných v řízení rizik

Pro řízení rizik je možné využít celou řadu funkcionalit, které Excel poskytuje. Mezi nejvýznamnější patří datové tabulky a seznamy, výpočty a automatizace hodnocení a grafický přehled.

2.1.1 Datové tabulky a seznamy

Základní prvek systému pro řízení rizik tvoří přehledné a strukturované tabulky. Ty slouží pro evidenci aktiv, hrozeb, zranitelností, opatření a výsledků analýzy rizik [3]. Pomocí datové validace lze zajistit konzistenci dat, např. omezením vstupů na definované hodnoty (pravděpodobnost 1–5, dopad 1–5) [9].

2.1.2 Výpočty a automatizace hodnocení

Excel umožňuje realizovat výpočty pomocí vzorců a funkcí (např. IF, VLOOKUP, INDEX/MATCH), což umožňuje automatizovat proces hodnocení rizik [10]:

- Výpočet rizikového skóre jako součin pravděpodobnosti a dopadu.
- Automatické přiřazení rizika do příslušné kategorie (nízké, střední, vysoké) pomocí podmíněných funkcí.

2.1.3 Matice rizik a vizualizace

Pro vizualizaci výsledků analýzy rizik lze využít matice rizik (Risk Matrix), která zobrazuje vztah mezi pravděpodobností výskytu a závažností dopadu. Pomocí podmíněného formátování lze vytvořit barevné kódování (např. zelená – nízké riziko, žlutá – střední, červená – vysoké) [11].

2.1.4 Grafické přehledy a dashboardy

K efektivnímu přehledu nad riziky lze využít kontingenční tabulky a grafy, které umožňují rychlé filtrování a agregaci dat [9]. Pro sledování vývoje rizik v čase a stavů opatření je možné vytvořit dashboard, kde jsou zobrazovány klíčové ukazatele (počet otevřených rizik, stav opatření, zbytková rizika apod.) [10].

2.2 Výhody a omezení Excelu

Microsoft Excel je často volen pro řízení rizik zejména díky následujícím výhodám:

- Dostupnost a uživatelská znalost: Excel je běžnou součástí kancelářských balíků a většina uživatelů má základní znalosti jeho používání [9].
- Flexibilita a přizpůsobitelnost: Umožňuje vytvářet vlastní modely a šablony podle specifických potřeb organizace [10].
- Nákladová efektivita: Ve srovnání s dedikovanými softwarovými řešeními je nasazení Excelu finančně nenáročné [12].
- Možnost vizualizace dat: Excel nabízí nástroje pro vytváření grafů, dashboardů a vizualizací, které usnadňují analýzu a interpretaci dat [11].

Ačkoliv je Excel efektivním a univerzálním nástrojem, jeho použití má i svá omezení:

- Obtížná správa velkého množství dat – při rozsáhlejších projektech může být Excel pomalejší a méně přehledný [9].
- Bezpečnostní rizika – při práci s citlivými daty může být nutné zajistit dodatečné zabezpečení souborů (šifrování, hesla) [12].
- Závislost na uživateli – kvalita a správnost dat závisí na pečlivosti a znalostech uživatele [3].

2.3 Tabulkový procesor

Tabulkový procesor je softwarová aplikace navržená k usnadnění práce s daty, zejména ve formě tabulek, které obsahují buňky uspořádané do řádků a sloupců. Hlavním účelem těchto nástrojů je provádění výpočtů, analýz dat, tvorba grafů, tabulek a reportů, a umožnění efektivního zpracování a vizualizace informací [9].

Tabulkové procesory byly původně vyvinuty pro potřeby účetnictví a finančních výpočtů, avšak v současné době se jejich využití rozšířilo do celé řady dalších oblastí, například:

- plánování a rozpočtování,
- analýza dat a vizualizace,
- modelování a simulace,
- sběr a třídění dat a
- podpora rozhodování v řízení rizik, projektovém managementu či kvalitě. [12]

Tabulkový procesor umožňuje nejen manuální zadávání dat, ale také jejich zpracování pomocí vzorců, funkcí a logických operací. Pokročilejší nástroje navíc podporují práci s databázemi, automatizaci (skripty a makra), dynamické vizualizace a analýzy scénářů. [10]

2.3.1 Nejrozšířenější tabulkové procesory

Úplný základ tabulkových procesorů tvoří právě nejvýznamnější „offline“ software Microsoft Excel, a naopak mezi „online“ verzi se může řadit software od společnosti Google – Sheets. Na trhu je i více tabulkových procesorů, které nemusí být tak rozšířené, přesto můžou disponovat mnoha unikátními funkcemi. Mezi méně známé se řadí LibreOffice Calc nebo Apple Numbers.

Microsoft Excel

- Výrobce: Microsoft
- Platformy: Windows, macOS, mobilní verze (iOS, Android), webová aplikace

Microsoft Excel je považován za nejvýznamnější tabulkový procesor současnosti. Nabízí širokou škálu funkcí, které pokrývají pokročilé datové analýzy, modelování a vizualizaci dat [9]. Dále podporuje programování vlastních skriptů pomocí VBA a integraci s dalšími nástroji, např. Power BI. [10]

Google Sheets (Tabulky Google)

- Výrobce: Google
- Platformy: Webové rozhraní, mobilní aplikace

Google Sheets je cloudový tabulkový procesor, který se stal populárním zejména díky svým možnostem spolupráce více uživatelů v reálném čase [13]. Je zdarma a nabízí jednoduché rozhraní s podporou skriptování přes Google Apps Script.

LibreOffice Calc

- Výrobce: The Document Foundation
- Platformy: Windows, macOS, Linux

LibreOffice Calc je open-source alternativou k Excelu. Nabízí základní funkce, které jsou dostačující pro běžnou práci s daty, avšak v oblasti pokročilé analýzy a vizualizace zaostává za konkurencí [14].

Apple Numbers

- Výrobce: Apple Inc.
- Platformy: macOS, iOS

Apple Numbers se zaměřuje na jednoduchost a přehlednost. Nabízí intuitivní rozhraní a podporuje iCloud synchronizaci, ale jeho možnosti pokročilé analýzy dat jsou omezené [15].

2.3.2 Srovnání tabulkových procesorů

Tabulkové procesory jsou univerzální nástroje pro práci s daty, analýzy a vizualizace. Každý z nástrojů má své přednosti a slabiny, které jsou obecně uvedeny v tabulce č.1., přičemž Microsoft Excel dominuje v oblasti pokročilých funkcí a automatizace, což jej předurčuje k využití při řízení rizik. Pro tuto práci byl Microsoft Excel zvolen především pro svou robustnost, možnosti analytického zpracování dat, dostupnost pokročilých funkcí a rozšířenosti skrze trh.

Tabulka 1 Porovnání tabulkových procesorů

Nástroj	Platforma	Cena	Pokročilé funkce	Spolupráce v reálném čase	Automatizace
Microsoft Excel	Windows, macOS, web	Placená	Ano (Power Query, VBA)	Omezená (desktop), dobrá (online)	VBA, Power Automate
Google Sheets	Web, iOS, Android	Zdarma / placené v rámci Google Workspace	Omezené (chybí Power Pivot)	Výborná	Google Apps Script
LibreOffice Calc	Windows, macOS, Linux	Zdarma	Omezené	Ano (sdílení souboru)	LibreOffice Basic
Apple Numbers	macOS, iOS	Zdarma	Základní	Dobrá (iCloud)	Omezené skripty

(zdroj: upraveno z [9]-[15])

II PRAKTICKÁ ČÁST

3 NÁVRH NÁSTROJE PRO ŘÍZENÍ RIZIK V MICROSOFT EXCEL

Samotná kapitola obsahující proces navrhování nástroje, popis funkčnosti a rozbor jednotlivých kroků navrhování nástroje. Ke snadnějšímu procesu navrhování bylo nutné znát alespoň pár základních požadavků, které funkce by měl nástroj obsahovat. Požadavky byly rozděleny na funkcionální a nefunkcionální. Funkcionální požadavky prezentovaly ty, které má nástroj umět vykonávat, mezi ně patří:

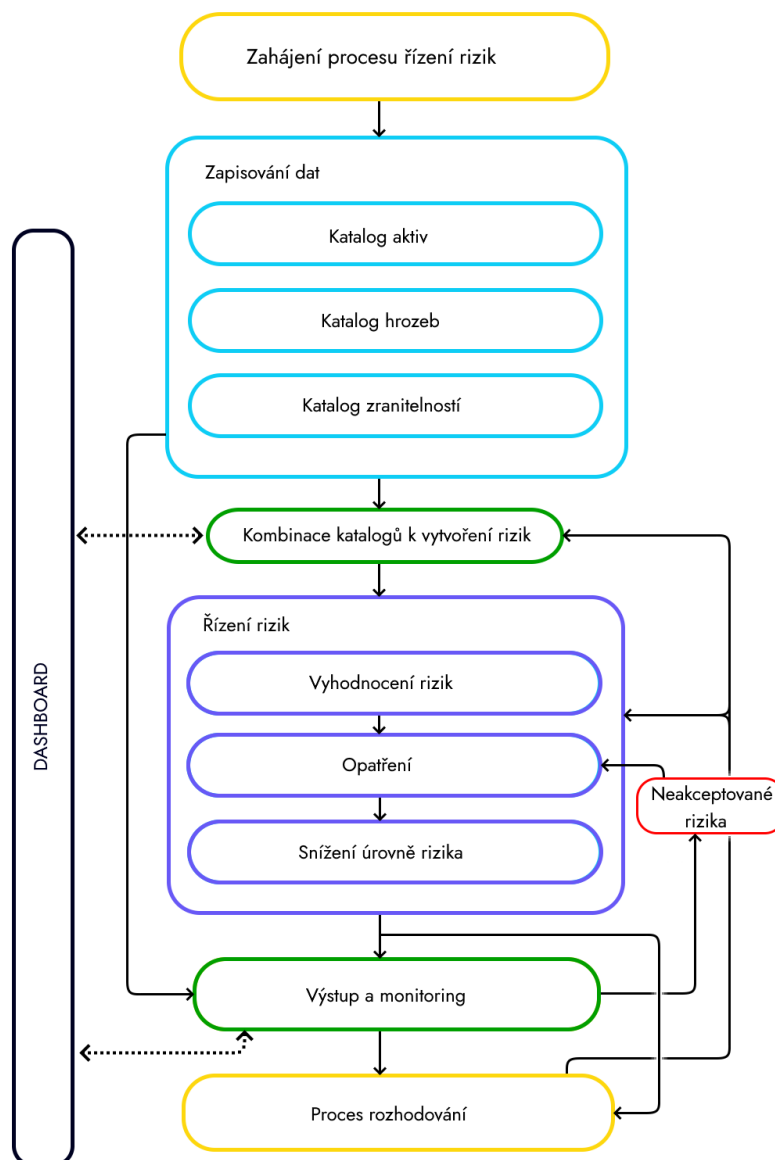
- evidence aktiv, hrozeb a zranitelností;
- automatizovaný zápis dat;
- propojení vstupních dat do rizik;
- výpočet rizikového skóre;
- určení úrovně rizika podle skóre;
- návrh a evidence opatření;
- přehledový dashboard a vizualizace;
- možnost filtrování a sledování stavu;
- modularita.

Nefunkcionální požadavky měly za úkol popsat vlastnosti nebo omezení, které nástroj vystihují nejlépe. Do seznamu byly zařazeny tyto možnosti:

- dostupnost bez potřeby dalšího softwaru;
- jednoduchost a přehlednost;
- automatizace procesů;
- nízké nároky na hardware;
- flexibilita a upravitelnost;
- bezpečnost dat v rámci souboru;
- kompatibilita.

3.1 Princip nástroje

Jakým stylem byla funkčnost nástroje pojata, je ukázkově načrtnuta obrázkem č.3.



Obrázek 3 Diagram funkčnosti nástroje

Nástroj byl postaven na cyklickém procesu, který začíná zahájením procesu řízení rizik. Navazuje se vyplňováním jednotlivých položek katalogů aktiv, hrozeb i zranitelností. Z vytvořených seznamů se skládají kombinace, které představují rizika vyvozené z katalogů.

Po kombinování se zapsaná rizika vyhodnocují a navrhuje se k nim opatření, které by měly způsobit snížení úrovně rizika. Výstupem jsou dokončené (potvrzené) opatření, které určují úroveň rizika. Pokud je riziko vyhodnoceno jako neakceptovatelné, nástroj umožňuje

návrat k návrhu opatření a jeho opětovné vyhodnocení po implementaci změn. Akceptovatelná rizika jsou dále pouze monitorována.

Celý proces byl doplněn o přehledový dashboard, který podporuje dílčí části systému a poskytuje uživateli kontrolu a přehled nad aktuálním stavem řízení rizik. Výstupem je monitoring rizik a opatření, který slouží v rozhodování vedení o bezpečnostním prostředí organizace.

3.2 Identifikace dat

V postupu řízení rizik bude potřeba identifikovat všechna důležitá data, mezi které se řadí:

- **aktiva,**
- **hrozby a**
- **zranitelnost.**

Tato data budou tvořit základ pro propojení mezi jednotlivými bezpečnostními prvky, jejich vyhodnocení a následné rozhodování o opatřeních. Pro efektivní implementaci v prostředí Microsoft Excel budou data rozdělena do tří samostatných listů.

3.2.1 Aktiva

Aktiva představují to, co chceme chránit. Může jít o fyzické objekty, informační systémy, databáze nebo lidské zdroje. Každé aktivum bude v nástroji popsáno:

- názvem,
- podrobným popisem,
- hodnocením hodnoty (na stupnici 1–5),
- kategorií (např. HW, SW, Data, Personál, Služba a jiné).

Tato tabulka bude tvořit referenční seznam všech aktiv, na které se budou později vázat hrozby a zranitelnosti.

3.2.2 Hrozby

Hrozby popisují události, které mohou negativně ovlivnit chráněná aktiva. Mohou mít charakter fyzický, lidský nebo technický. Pro každou hrozbu bude možno evidovat:

- název hrozby,

- popis hrozby,
- typ hrozby (např. fyzická, lidská, technická a profesní),
- pravděpodobnost (hodnocení 1–5 s významem od "téměř vyloučené" po "téměř jisté"),
- dopad (hodnocení 1–5 od "téměř neznatelný" po "katastrofický").

Tato data budou sloužit jako vstup pro výpočet rizikového skóre.

3.2.3 Zranitelnosti

Zranitelnosti jsou slabá místa v systému, která mohou být zneužita hrozbou. Každá zranitelnost se bude zaznamenávat s atributy:

- název,
- popis,
- typ zranitelnosti (technická, procesní, lidská, fyzická),
- hodnota (1–5, kde 5 značí nejzávažnější slabinu).

Tímto způsobem dochází k vytvoření tří jasně definovaných vstupních tabulek, které tvoří základ pro další kroky v řízení rizik. Všechny tabulky mají vlastní vstupní rozhraní přímo v dashboardu nástroje pro lepší přehlednost a jednoduchost používání.

3.3 Propojení vstupních dat a hodnocení rizik

Po identifikaci vstupních údajů následuje propojení těchto dat, které tvoří základní logiku řízení rizik. Pomocí samostatné tabulky bude možné vytvářet kombinace jednotlivých aktiv, hrozeb a zranitelností. Každá kombinace reprezentuje jedno potenciální riziko, které bude dále hodnoceno.

Pro propojení se bude používat unikátní identifikátor, ke kterému jsou přiřazeny:

- ID aktiva,
- ID hrozby,
- ID zranitelnosti.

Na základě tohoto propojení bude možné následně pomocí vzorců automaticky doplňovat:

- název aktiva, hrozby i zranitelnosti,
- hodnoty pravděpodobnosti a dopadu hrozby,
- hodnotu rizika (rizikové skóre).

3.3.1 Výpočet a hodnocení rizikového skóre

Rizikové skóre bude vypočítáváno jako součin pravděpodobnosti a dopadu:

- $Riziko = Pravděpodobnost \times Dopad$

Tento výpočet umožňuje kvantifikovat jednotlivá rizika a následně je porovnávat mezi sebou podle závažnosti. Hodnota skóre může být doplněna i o kategorii úrovně rizika (např. nízké, střední, vysoké) na základě definovaných prahových hodnot.

Hodnocení rizik tímto způsobem přináší strukturovaný pohled na bezpečnostní situaci organizace. Umožňuje zacílit pozornost a zdroje na oblasti s nejvyšší mírou ohrožení, což přispívá k efektivnímu řízení rizik.

3.4 Návrh opatření a přiřazení odpovědností

Po vyhodnocení rizik bude nezbytné navrhnout odpovídající bezpečnostní opatření pro jejich snížení, eliminaci nebo přijetí. V rámci nástroje budou tato opatření zadávána do samostatné tabulky, ve které bude možné evidovat:

- popis navrženého opatření,
- typ opatření (technické, organizační, procesní apod.),
- přiřazená osoba odpovědná za realizaci,
- termín realizace,
- stav plnění.

Tato část nástroje bude sloužit jako aktivní výstup řízení rizik a umožňuje organizaci řídit plnění nápravných opatření v čase. Může být také využita pro kontrolu plnění a hlášení pro vedení společnosti.

3.5 Vizualizace dat a dashboard

Pro zajištění přehlednosti a podkladů pro rozhodování bude důležitou součástí nástroje přehledná vizualizace dat. Pomocí funkcí Microsoft Excel lze připravit:

- kontingenční tabulky pro dynamické přehledy,
- sloupcové, koláčové a spojnicové grafy pro jednotlivé oblasti (např. četnost hrozeb, rozložení rizik podle úrovně apod.),
- barevné zvýraznění pomocí podmíněného formátování (např. heatmapa rizikového skóre).

Centrálním prvkem bude **dashboard**, který bude spojovat klíčové ukazatele a umožní:

- zobrazit počet identifikovaných rizik podle kategorie nebo závažnosti,
- sledovat stav opatření (plněno/neplněno),
- vizualizovat distribuci hrozeb, aktiv a zranitelností,
- filtrovat podle odpovědných osob nebo kategorií aktiv.

Dashboard bude navržen tak, aby byl snadno ovladatelný a intuitivní pro management a pracovníky odpovědné za bezpečnost. Jeho cílem je zrychlit a zpřehlednit orientaci v datech bez nutnosti procházet jednotlivé tabulky manuálně.

3.6 Rozhodování o rizicích (Management)

Na základě výsledků analýzy a zobrazení dat na dashboardu dochází k rozhodovacímu procesu. Management organizace bude moci využívat výstupy z nástroje pro:

- určení prioritních rizik,
- schválení nebo zamítnutí navržených opatření,
- rozhodnutí o přijetí rizika v případě nízkého skóre.

3.7 Aktualizace a monitoring

Rizika nejsou statická – s časem se mění technologie, procesy i hrozby. Z toho důvodu je nutné umožnit pravidelnou aktualizaci dat v nástroji:

- aktualizace aktiv, hrozeb a zranitelností (např. přidání nového zařízení, nové typy útoků),
- přehodnocení pravděpodobnosti a dopadu (např. po zavedení opatření),
- sledování změn v opatřeních a jejich stav.

Nástroj bude navržen tak, aby umožňoval pružné doplňování a úpravy dat, a tím udržoval celý systém řízení rizik aktuální a spolehlivý.

4 IMPLEMENTACE NÁSTROJE V MICROSOFT EXCEL

Pro implementaci funkcí a funkčnosti nástroje do Microsoft Excel byl připraven návrh, podle kterého se v této kapitole bude postupovat. Prvním a zásadním krokem, aby nástroj mohl fungovat bylo důležité zapisování dat.

4.1 Zapisování dat

Aktiva, hrozby i zranitelnosti jsou vedeny v samostatných listech. Zapisování probíhá přes centrální dashboard, ve kterém jsou tři jednoduché formuláře pro vyplnění. Každý formulář odpovídá obsahem hlaviček pro aktiva, hrozby i zranitelnost, tak aby seděly informace do jejich tabulek.

Zapsaná data jsou odesílána z dashboardu přímo na listy určené pro aktiva, hrozby i zranitelnost pomocí maker. Princip makra byl vysvětlen v kapitole 4.1.1 pouze pro list *Aktiva*, pro *Hrozby* a *Zranitelnost* se princip makra v ničem nelišil.

4.1.1 Princip zapisování dat přes makro

Makro bylo důležité pro odesílání dat z jednoho listu (dashboardu) do ostatních listů (aktiva, hrozby, zranitelnost...). Rozbor byl proveden pouze pro jeden list (aktiva), zbylá makra fungují totožně.

Na začátku makra, které je v příloze PI, se definuje list, ze kterého se budou data přebírat a do kterého cílového listu se budou data zapisovat. Vstupní hodnoty jsou definovány jako obsah buněk ve formuláři na dashboardu a z možnosti pro kritičnost se odesílá pouze číselná hodnota, která je nezbytná pro následné výpočty. Načtené hodnoty se odesílají do listu *Aktiva* a makro vyhledá poslední (cílový) řádek, do kterého data přepíše. Poté se data zapisují v pořadí, ve kterém byly do formuláře zapsány a přidá se automaticky vygenerované ID. Jakmile makro přepíše všechna data do listu *Aktiva*, všechna data ve formuláři na dashboardu se vymažou, aby byl formulář připraven pro další přidání záznamu.

4.1.2 Katalog aktiv

Aktiva byla vedena velmi jednoduchým, až tím úplně nejzákladnějším, způsobem. V tabulce pro aktiva jsou parametry

- ID aktiva,
- název aktiva,

- kategorie a
- kritičnost.

Číslování aktiv bylo navrženo tak, aby šlo poznat, že jde o ID aktiva. Označením s předponou „A“ která značí aktivum a číselným označením, např. A001, A002 atd.

Kategorizování bylo rozděleno do základních typů jako jsou například hardware, software, služby, lidé nebo data a další. Kategorie byly využívány především ke třídění. Obrázek č. 4. znázorňuje orientační zobrazení obsahu listu *Aktiva*.

ID Aktiva	Název	Kategorie	Kritičnost (hodnota)
A001	Firemní databáze klientů	Informační	5
A002	Servery	Technologické	5
A003	Přístupové karty	Fyzické	3
A004	Kamerový systém	Bezpečnostní technologie	4
A005	Zálohovací systém	Technologické	4
A006	Osobní údaje zaměstnanců	Informační	5
A007	Hlavní budova společnosti	Fyzické	4
A008	Firemní plakáty	Fyzické	1
A009	Tiskárny	Technologické	2
A010	Kávovar v kuchyňce	Fyzické	1

Obrázek 4 Rozložení katalogu aktiv

Tabulka č.2 definuje kritičnost aktiva v organizaci, nikoliv obecně pro dané aktivum. Slovní popis usnadňuje lepší pochopení významu kritičnosti a jejího použití v nástroji.

Tabulka 2 Kritičnost aktiva

KRITIČNOST		
HODNOTA	SLOVNÍ VYJÁDŘENÍ	POPIS
5	Kritická	Aktivum je naprosto nezbytné. Jeho ztráta nebo výpadek by znamenal okamžité ohrožení fungování organizace, finanční ztráty nebo právní dopady.
4	Vysoká	Aktivum je zásadní pro provoz klíčových procesů. Výpadek by měl vážný dopad, vyžaduje rychlou reakci.
3	Střední	Aktivum podporuje důležité procesy, ale existují alternativy nebo zálohy. Výpadek způsobí zdržení, ale ne kritické škody.
2	Nízká	Aktivum je využíváno okrajově. Jeho výpadek je nepříjemný, ale neohroží běžné fungování.
1	Zanedbatelná	Aktivum nemá významný vliv na chod organizace. Je snadno nahraditelné, případně má nulový dopad při výpadku.

4.1.3 Katalog hrozeb

Katalog hrozeb je více obsáhlý oproti katalogu aktiv a zapisovat se do něj můžou data jako

- ID hrozeb,
- název,
- kategorie,
- četnost výskytu a
- dopad.

Značení hrozeb je nastaveno stejným principem jako u všech ostatních tabulek, tedy předponou pro značení hrozeb „H“ a číselným označením, např. H001, H002 atd.

Do katalogu hrozeb bylo důležité dostat číselné hodnoty pro dopad a četnost výskytu hrozby. Hodnoty těchto dvou parametrů byly klíčové k výpočtu rizikového skóre. Vyjádření a popis úrovní pro četnost výskytu hrozby, v tabulce č.3, zlepšují pochopení pro snadnější ohodnocení hrozby.

Tabulka 3 Četnost výskytu hrozby

ČETNOST VÝSKYTU		
HODNOTA	SLOVNÍ VYJÁDŘENÍ	POPIS
5	téměř jisté	vyskytne se skoro vždy
4	pravděpodobné	pravděpodobně se vyskytne
3	možné	někdy se může vyskytnout
2	nepravděpodobné	vyskytnout se může, ale nemusí také vůbec
1	téměř vyloučené	vyskytuje se pouze ve výjimečných případech

(upraveno z [16])

K chápání, jakým stylem byl pojat dopad hrozby pro užívání v nástroji, slouží tabulka č.4.

Tabulka 4 Dopad hrozby

DOPAD HROZBY		
HODNOTA	SLOVNÍ VYJÁDŘENÍ	POPIS
5	katastrofický	ztráta majetku, dat, porušení legislativy, dlouhodobé reputační a finanční ztráty
4	velmi významný	vážný dopad na provoz, výpadky, závažné narušení bezpečnosti nebo produktivity
3	významný	vyžaduje okamžité řešení situace
2	drobný	ovlivňuje pouze dílčí aktivity
1	téměř neznatelný	neovlivňuje znatelně fungování

(upraveno z [16])

Ukázka naplněné tabulky v nástroji pro hrozby je znázorněna na obrázku č.5, data v tabulce jsou pouze příkladové.

ID Hrozby	Název	Kategorie	Četnost výskytu	Dopad
H001	Kybernetický útok (ransomware)	Digitální	4	5
H002	Požár v serverovně	Fyzická	2	5
H003	Selhání hardwaru	Technologická	3	4
H004	Neoprávněný přístup do systému	Digitální	3	4
H005	Krádež zařízení	Fyzická	3	3
H006	Chyba v softwaru	Technologická	3	3
H007	Ztráta kancelářských potřeb	Fyzické	3	1
H008	Chyba v prezentaci	Informační	2	2
H009	Zpoždění doručení toneru	Technologické	2	1
H010	Lidská chyba (mazání dat)	Personální	4	3

Obrázek 5 Rozložení katalogu hrozeb

4.1.4 Katalog zranitelností

Pro evidence zranitelností byl taky vytvořen samostatný list *Zranitelnost*, ve kterém jsou uvedeny informace jako

- ID zranitelnosti,
- název,
- kategorie a
- míra.

Značení zranitelností je stejným způsobem jako v předchozích případech u aktiv a hrozeb, kdy „Z“ označuje zranitelnost a číslo číselné označení. Definování míry zranitelnosti je vyjádřené v tabulce č. 5, kde jsou popsány všechny stupně.

Tabulka 5 Míra zranitelnosti

MÍRA ZRANITELNOSTI		
MÍRA	SLOVNÍ VYJÁDŘENÍ	POPIS
5	katastrofická	aktivní zneužívání nebo veřejně známá zranitelnost
4	vysoká	slabiny jsou snadno zneužitelné
3	střední	známé slabiny ale zneužitelné za daných podmínek
2	nízká	těžko zneužitelné slabiny
1	zanedbatelná	téměř žádné zneužitelné slabiny

Vyobrazení celé navrhnuté tabulky pro katalog zranitelností slouží obrázek č.6, data v tabulce jsou příkladové.

ID Zranitelnosti	Název	Kategorie	Míra
Z001	Neaktuální antivirový software	Technologická	4
Z002	Slabé heslo	Digitální	5
Z003	Nedostatečné školení personálu	Personální	4
Z004	Chybějící zálohování dat	Technologická	5
Z005	Otevřené porty v síti	Digitální	4
Z006	Fyzický přístup bez dohledu	Fyzická	4
Z007	Nepřítomnost UPS systému	Technologická	3
Z008	Chybějící monitoring systémů	Technologická	3
Z009	Nedostatek kapacit v IT	Personální	3
Z010	Nezajištěné zásuvky a kabeláž	Fyzická	2

Obrázek 6 Rozložení katalogu zranitelností

4.2 Propojení dat a hodnocení rizik

Seskupení dat a vypisování rizik byl nezbytný krok pro fungování. V nástroji jsou rizika spojována jako průsečík aktiv, zranitelností a hrozeb. Pro přehlednější orientaci byl vytvořen formulář, zobrazen na obrázku č.7.

PŘIDÁNÍ RIZIKA

Název aktiva	Název hrozby	Název zranitelnosti

Zapsat Propojení

Obrázek 7 Formulář zapisování propojení

4.2.1 Princip propojení

Propojení bylo zavedeno do dashboardu, ve kterém je k dispozici formulář pro vyplnění. Ve formuláři jsou k dispozici všechny katalogy a jejich obsah, který je k dispozici pro vytváření rizik. Ve formuláři se vyplní aktivum, přiřadí se k němu odpovídající hrozba a zranitelnost a následně se data odešlou do listu *Rizika*.

Struktura tabulky v listu *Rizika* je následovná:

- ID rizika,
- Aktivum,
- Hrozba,
- Zranitelnost,
- Četnost výskytu hrozby,
- Míra zranitelnosti,
- Výsledná četnost výskytu,
- Dopad,
- Rizikové skóre a
- Úroveň rizika.

Makro, které způsobuje odesílání dat do listu *Rizika*, je v příloze P IV. Kód si přebere vybrané položky z katalogů ve formuláři, převezme jejich názvy a hodnoty se kterými pracuje a vypočítává navržené rizikové skóre.

4.2.2 Hodnocení rizik

Rizikové skóre v nástroji je vypočítáváno jako *výsledná četnost výskytu* $\times$ *dopad*. K výpočtu výsledné četnosti výskytu byla potřeba hodnota pro četnost výskytu hrozby a míra zranitelnosti. Z těchto dvou hodnot bylo vytvořené maximum pomocí funkce `max()`, tímto způsobem je riziko zvyšováno nejhorším faktorem. Hodnota dopadu je vyjádřena jako maximální hodnota dopadu hrozby a kritičnosti aktiva, což umožňuje vliv obou veličin na rizikové skóre.

Pro určení úrovně rizika byl zvolen postup rizikové matice, která je zobrazena na obrázku č.8. Matice má 4 úrovně rizika:

- Nízké,
- Střední,
- Vysoké a
- Kritické.

Škála úrovní byla stanovena jako 1-4 nízká rizika, 5-11 střední rizika, 12-19 vysoká rizika a 20-25 kritická rizika.

Dopad	1	2	3	4	5
Výsledná četnost výskytu	1	2	3	4	5
1	nízké	nízké	nízké	nízké	střední
2	nízké	nízké	střední	střední	střední
3	nízké	střední	střední	vysoké	vysoké
4	nízké	střední	vysoké	vysoké	kritické
5	střední	střední	vysoké	kritické	kritické

Obrázek 8 Riziková matice

4.3 Návrh opatření a přiřazení odpovědností

Návrhy pro opatření byly přidány jako další samostatný list, který má v sobě data jako přidělené riziko (to riziko, kterého se opatření týká), samotný název opatření, odpovědnost, termín realizace, stav opatření a účinnost.

Každý proces musí mít svého vlastníka a další účastníky, kteří mají dílčí odpovědnosti. Proto byla použita odpovědnostní matice – RACI [17], která by měla mít strukturu:

- R – Responsible -> osoba odpovědná za celý proces (nejčastěji vlastník procesu), přiděluje úkoly v rámci procesu
- A – Accountable -> osoba odpovědná za dílčí činnost/aktivitu v rámci procesu, většinou se jedná o osobu, která je zodpovědná za rozhodnutí v rámci zmíněné aktivity. Často bývá kombinace R+A.
- C – Consulted -> osoba se kterou musí být konzultováno každé rozhodnutí (typicky DPO) odpovědnou osobou (A)

- I – Informed -> osoba která musí být informovaná o rozhodnutí nebo provedené aktivitě

Sloupec odpovědnost byl rozdělen do těchto kategorií, do kterých se vepisují příslušné osoby nebo role. Na základě rozdělení je pak možné vytvářet výstup např. kdo má nejvíce odpovědností jako R (Responsible).

Termín realizace byl přidán pro určení, do jakého termínu by mělo být realizováno opatření. Slouží zejména pro osobu nebo skupinu lidí, která opatření realizuje. K termínu realizace byla přiřazena podmínka, která doporučuje realizovat opatření pro riziko s rizikovou úrovní „Kritické“ do 30 dnů. Pokud je zadaný termín realizace delší než 30 dnů, zobrazí se doporučení na jeho zkrácení. Termín je nutné zadávat ve formátu „den, měsíc, rok“ a všechno v číselném vyjádření odděleno tečkami (příklad: 26.7.2025).

Stav opatření byl nastavený na základní hodnotu „Navrženo“, tudíž opatření je zapsáno v systému, ale ještě není řešené. Stav se dá upravovat podle tří stavů. Opatření, které je řešeno dostává stav „V řešení“, pro realizované opatření existuje možnost „Dokončeno“ a zamítnuté nebo nerealizovatelné stavy můžou být označeny stavem „Odmítnuto“.

U každého zavádění opatření je důležitá poslední kolonka „Účinnost opatření“. Osoba nebo skupina lidí, které realizovali dané opatření přidělí hodnotu účinnosti podle efektivity opatření. Hodnota pak dále reflektuje rizikové skóre po přijetí opatření.

Celý proces zapisování dat přes formulář do listu Opatření, je vyobrazen v příloze P V.

4.3.1 Výpočet rizikové skóre po zavedení opatření

Každým správným zavedením opatření by se měla snížit hodnota rizika, kterého se opatření týká. V nástroji byl zvolen princip postupného snižování rizika pomocí účinnosti opatření. Jelikož může být zavedeno více opatření pro jedno riziko, muselo se počítat i s takovými případy, kde je pro jedno riziko více opatření.

Každé opatření může riziko pouze snížit, ne však eliminovat. Výsledné riziko je zapotřebí vnímat jako zbytkové, které lze dále řídit. [3]

Snižování zbytkového rizika probíhalo tak, že původní riziko bylo násobeno zbývajícím účinností opatření:

- Zbytkové riziko = původní rizikové skóre $\times$ (1 – účinnost prvního opatření) $\times$ (1 – účinnost druhého opatření) $\times$ atd...

Způsob výpočtu zabraňuje chybné interpretaci při součtu účinností, které by vedly k nerealistickým hodnotám snížení rizika.

Celý výpočet byl implementován přes makro v příloze P VI. Makro připraví proměnné a listy se kterými má pracovat, zároveň vytváří dynamický slovní *dict*, který slouží k dočasnému uložení opatření přiřazené každému rizikům. Cyklem *For* projde všechny řádky v tabulce *Opatření* a:

- získá **ID rizika, název opatření, stav opatření a účinnost;**
- zpracuje jen opatření se stavem „Dokončeno“;
- ověří, že u všech dokončených opatření je vyplněná účinnost – pokud ne, upozorní uživatele a opatření nepřevede.

Pro každé riziko se vytváří „vnořený slovník“ *dict*, který obsahuje:

- seznam názvů všech opatření;
- seznam účinnosti pro výpočet.

Funkce *AppendToArray* pomáhá přidat čísla do pole (VBA neumí dynamicky zvětšovat *Array()* jako ostatní jazyky)

Přepočet rizikového skóre se provádělo podle logiky popsané výš v kapitole 4.3.1. Pro každý přechod cyklem se zapsalo původní skóre, vypočítal se kumulativní faktor (zbývající riziko) vynásobený zbývající účinností opatření. Proces se opakoval do té doby, dokud se neprošla všechna opatření, nebo dokud nechyběla zapsaná účinnost pro opatření, které bylo označeno stavem „Dokončeno“. V takovém případě se zobrazila hláška, že opatření chybí zapsaná účinnost a přepočítání se neuskutečnilo.

Makro disponuje funkcí automatického přiřazení úrovně rizika podle nového vypočítaného rizikového skóre. Škála rizikového skóre se nezměnila a pořadí se vychází z rizikové matice podle obrázku č.8.

Automatizována byla i možnost přiřazení přijatelnosti rizika. Rizika s nízkou úrovní byla automaticky akceptována, rizika s kritickou úrovní byla automaticky neakceptována. Zbytek se dá upravovat ručně odpovědnou osobou.

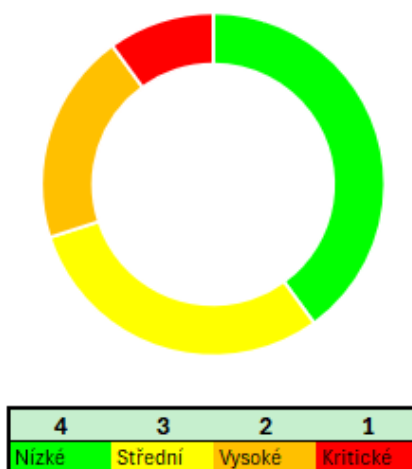
4.4 Vizualizace dat

Nedílnou součástí fungování nástroje je přehlednost a uživatelská manipulace. Hlavním prvkem pro ovládání nástroje je dashboard, do kterého byly přidány veškeré formuláře pro snadnější doplňování tabulek. Jedná se o formuláře:

- zapisování aktiv,
- zapisování hrozeb,
- zapisování zranitelností,
- přidání rizika a
- zavedení opatření.

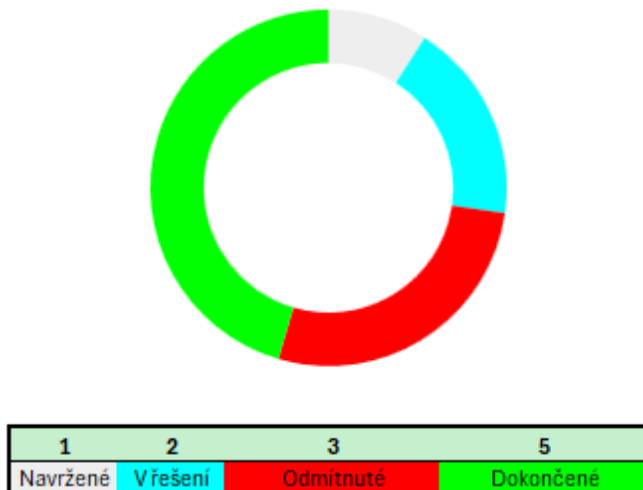
Každý formulář je interaktivní a nabízí seznam možností které lze doplnit, například pro kategorie ke všem katalogům, nebo nápovědu pro možnosti kritičnosti aktiv, četnost výskytu a dopadu hrozby nebo míry zranitelnosti. Formulář pro přidání rizika je plně interaktivní, na výběr jsou všechny možnosti z každého katalogu pro lepší přehled a vytváření rizik.

Do dashboardu byly zahrnuty i důležité přehledy, které mohou snadněji vyvodit výsledky analýzy. Jedná se o grafy pro zobrazení rizik před analýzou, které jsou v „surovém“ stavu přidány do systému. Pro porovnání byl zde přidán i graf pro rizika po zavedení opatření. Oba grafy znázorňují počet rizik v dané úrovni rizika. Graf pro zobrazení rizik po zavedení opatření je vyobrazen obrázkem č.9.



Obrázek 9 Grafické znázornění počtu úrovní rizik po zavedení opatření

Pro snadnější kontrolu opatření byl přidán graf zobrazující počet opatření podle stavu opatření. Graf tak umožňuje lépe pochopit kolik opatření je například v řešení, nebo kolik opatření teprve čeká na zahájení řešení. Obrázek č.9., znázorňuje grafické zobrazení počtu opatření podle stavu opatření.



Obrázek 10 Grafické znázornění počtu opatření v kategorii stav opatření

S dokončením opatření se neaktualizuje tabulka s riziky automaticky, je potřeba manuálně stisknout tlačítko, které bylo přidáno do dashboardu hned pod formulář „Zavedení opatření“ aby bylo lehce dostupné a nepřekáželo ostatním výstupům.

Každá tabulka byla doplněna o možnost filtrování skrz kategorie a seřazení výstupů. Pro katalog aktiv, hrozeb a zranitelností byl použit stejný filtr i seřazení, a to stylem filtrování podle vybrané kategorie nebo seřazení do kategorií k sobě. Pro seřazení bylo do navigačního panelu přidáno tlačítko „Seřadit“, pro filtrování bylo připraveno tlačítko „Filtrovat“ a v poslední řadě bylo přidáno tlačítko pro vrácení tabulky do původního stavu díky tlačítku „Vymazat filtry“. Všechny makra pro třídění, filtrování a resetování filtru jsou v příloze P VII. Makra jsou uvedena pouze pro aktiva, hrozby a zranitelnosti mají odlišný kód pouze v názvu a pojmenování listu. Stejným principem byla přidána možnost filtrování a seřazení rizik, a to jak v listu *Rizika*, tak i v listu *RizikaPoOpatření*. Kdy se rizika dala filtrovat a třídit podle úrovně. Náhled kódů pro třídění, filtr a vymazání filtru rizik je k nahlédnutí v příloze P VIII. Poslední filtrování proběhlo pro list *Opatření*, kde byl systém pojat trošičku jinak. Filtrování a seřazení bylo vytvořeno podle stavu opatření, kdy se po seřazení vypíší nahoře záznamy, které mají stav „Navrženo“ poté „V řešení“ a nakonec „Dokončeno“ a „Odmítnuté“. Tohle pořadí bylo zvolené z důvodu priority pro nedokončené opatření.

Důležitý byl také termín realizace, který se dá třídit podle nejbližšího termínu realizace. Náhledy pro kódy jsou v příloze P IX.

Po aktualizaci všech rizik, je možné nyní sledovat počet akceptovaných a neakceptovaných rizik. Jejich počet byl přidán do dashboardu pro lepší přehlednost místo zmatečného hledání v samotném listu *RizikaPoOpatření*.

4.5 Rozhodování o rizicích

Pro management organizace, který bude rozhodovat o přijatelnosti rizik nebo rozhodování stavu opatření, byla připravená navigace v hlavním panelu v horní části nástroje. Možnosti pro přepínání na důležité listy jako jsou *Opatření* nebo *RizikaPoOpatření*, ve kterých jsou možnosti pro rozhodování o stavu opatření, nebo možnosti stanovit přijatelnost rizika.

4.6 Aktualizace a monitoring

Data v nástroji se dají aktualizovat dvěma způsoby. Manuálně přejít do katalogů a upravovat data přímo v tabulkách, nebo používat formuláře na dashboardu. Přepisování hodnot, pokud se uživatel spletl, je možné přímo v katalogu. Je vhodné brát v potaz, že každé nové přidání záznamu do katalogu se zobrazí na konci seznamu.

Sledování změn například po zavedení opatření bylo umožněno přímo v dashboardu, jsou zde grafy pro rizika před a po zavedení opatření včetně sledování počtu opatření dle jednotlivých stavů. Uživatel tedy vidí, kolik opatření bylo navrženo a může se přejít do procesu řešení daného opatření.

Navíc byl zaveden monitoring všech opatření, kterým skončila platnost a stále jejich stav nebyl změněný na „Dokončeno“ nebo „Odmítnuto“. Tahle možnost umožňuje managementu rychle jednat.

5 POROVNÁNÍ NÁSTROJE NA MODELOVÉ SITUACI

Po implementaci nástroje do prostředí Microsoft Excel bylo přistoupeno k porovnání nástroje na modelové situaci a zhodnocení jeho efektivity v procesu řízení rizik. Cílem této části je poukázat na praktickou využitelnost řešení a popsat, jak efektivně nástroj dokáže identifikaci a řízení rizik v simulovaném prostředí.

5.1 Modelová situace

Modelová situace byla navržena stylem, aby obsáhla širokou škálu aktiv, hrozeb i zranitelností a umožnila vyhodnocení výstupů nástroje.

Organizace, které se proces řízení rizik týkal, pro demonstraci funkčnosti nástroje byla zvolena středně velká humanitární nezisková organizace, která se specializuje na poskytování pomoci v České republice. Její činnosti zahrnují distribuci potravin, léků, krizového vybavení a poskytování základní sociální nebo zdravotní podpory v postižených oblastech.

5.2 Základní charakteristika

Stručná charakteristika organizace byla rozdělena na hlavní informace, počet zaměstnanců, technologické vybavení, informační aktiva, fyzická aktiva a bezpečnostní prvky.

Hlavní sídlo organizace se nachází v krajském městě, areál asi o velikosti 800 m², skládající se z:

- centrální kanceláře,
- skladovacích prostor,
- zasedací místnosti,
- technické místnosti pro servery a IT infrastrukturu.

Počet zaměstnanců byl odhadován na cca 35 interních pracovníků (vedení, administrativa, IT, logistika, účetnictví), cca 20 terénních pracovníků, kteří působí v regionech a stabilní síť až 50 registrovaných dobrovolníků, aktivovaných podle potřeby.

Mezi vybavení organizace se řadí technologické, informační a fyzické věci. U technologické vybavenosti jde především o:

- Vlastní emailový server,

- Účetní a dárcovský software,
- Interní dokumentový a školící systém,
- Dárcovský portál a veřejné webové stránky.

Do informačních aktiv spadají databáze, zdravotní dokumentace klientů, vnitřní směrnice, záznamy z porad, smlouvy a kontakty. Zásoby potravin, vody, léků, přenosné stany a krizové přístřešky, notebooky, zálohovací disky, tiskárny a periferie se řadí do seznamu fyzických aktiv organizace.

Mezi bezpečnostní prvky, kterými organizace disponuje jsou například přístupové čipy nebo kamerový systém.

Organizace má jednoduchou organizační strukturu, tvoří ji:

- Ředitel organizace,
- Vedoucí jednotlivých oddělení (IT, logistika, personální)
- Právník nebo koordinátor bezpečnosti.

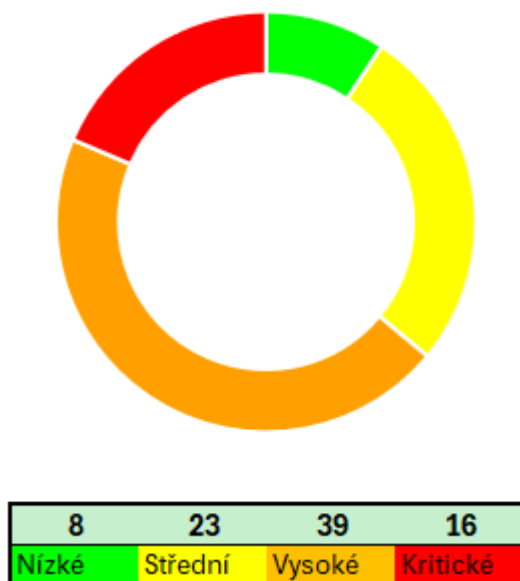
Organizace operuje v hybridním režimu, kdy část pracovníků pracují v terénu a část v kancelářích. Pro zajištění provozu používá organizace cloudové služby, ale hodně citlivých dat uchovává lokálně z důvodu bezpečnosti.

5.3 Implementace dat do nástroje

Data do systému byla vkládána přes formuláře na dashboardu, díky kterému bylo možné vložit aktivum rovnou s hrozbou i zranitelností. Tohle řešení umožňuje zapsat všechny možnosti systematicky. Seznam všech dat v katalozích aktiv, hrozeb i zranitelností, které byly k modelové organizaci vymyšleny jsou k nahlédnutí v přílohách P X až P XII.

Po vypsání všech potřebných informací do katalogů nastal důležitý moment, kdy se výstupy začnou přetvářet do rizik. K dispozici byl formulář, ve kterém se tvořily propojení a který automaticky po zapsání určoval hodnotu a úroveň rizika. Nahlédnutí pro kompletní seznam rizik je v příloze P XIII.

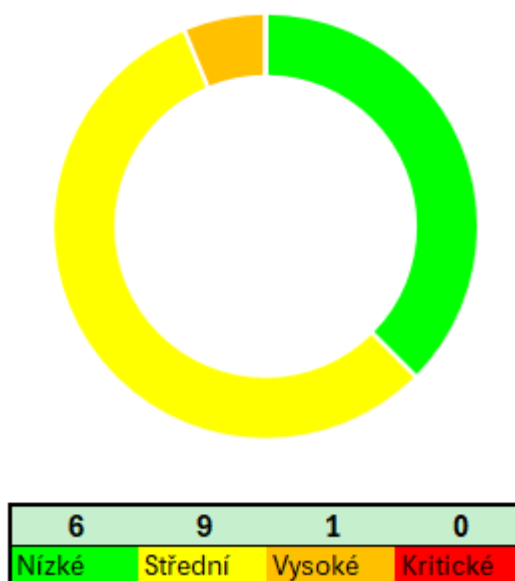
V tento moment bylo možné pozorovat změny grafiky na dashboardu, protože se pomaličku začaly propisovat úrovně rizik do grafu, viz. obrázek č.11.



Obrázek 11 Grafický přehled rizik modelové organizace

Pro zjevné výsledky implementace dat do nástroje pro řízení rizik byl zvolen přístup návrhu opatření pouze k rizikům s úrovní vysokou nebo kritickou. Pro přehlednější vkládání opatření sloužil formulář, ve kterém byla možnost rozbalovacího seznamu pro rizika, ve kterém bylo možné vidět i úroveň rizika.

Po vymyšlení a zapsání všech opatření k rizikům začínal proces rozhodování. Proces rozhodování vyplýval z datumu realizace a vyhodnocení důležitosti zavedených opatření. Uživatel nástroje byl schopný měnit stav opatření podle aktuálního zavedení do organizace. Všechny opatření, které byly dokončené musel uživatel ohodnotit podle toho, jak moc účinné ve vazbě pro dané riziko byly. Podle téhle logiky se rizika na žádost uživatele přepočítaly a výsledky byly zaznamenány do dashboardu viz. příloha P XIV. Graf počtu rizik po zavedení některých opatření je znázorněný na obrázku č.12.



Obrázek 12 Grafické znázornění počtu rizik po zavedení opatření

Nástroj v tenhle moment čekal na další změny, které mohl uživatel provést. Jednalo se o změny typu:

- změnit stav u opatření, aby mohl vyhodnotit snížení rizika;
- zapsání nového opatření;
- rozhodnutí o přijetí nebo odmítnutí rizika;

Tímhle se využil plný potenciál, kterým nástroj disponoval.

6 VYHODNOCENÍ A VYUŽITELNOST NÁSTROJE

Tato kapitola cílí na vyhodnocení funkčnosti nástroje a využitelnost vytvořeného nástroje pro řízení rizik. Úkolem bylo posoudit do jaké míry nástroj splňuje požadavky, které byly stanoveny v návrhu nástroje a podporu rozhodování při řízení bezpečnosti. Zároveň je také představena uplatitelnost systému v reálném prostředí.

6.1 Vyhodnocení nástroje

Vyhodnocení probíhalo testováním hlavních oblastí, kterými byly především správná funkce jednotlivých maker, tedy spolehlivost, uživatelská přehlednost, přívětivost zápisu dat, logika výpočtu rizikového skóre a schopnost nástroje podpořit orientaci v datech při reálném použití. Testování probíhalo autorem práce na modelovém příkladu neziskové humanitární organizaci, a přitom byl simulován proces analýzy rizik od identifikace aktiv až po zavedení opatření a vyhodnocení účinnosti opatření.

Z pohledu funkčních požadavků se dá říct, že všechny klíčové funkce, které byly sepsány při navrhování nástroje, byly splněny. Nástroj disponuje evidencí dat jako jsou aktiva, zranitelnosti i hrozby a jejich následné propojení do přehledu rizik pomocí formuláře a automatizovaného zápisu. Pomocí VBA (Visual Basic for Application) – programovací jazyk pro Microsoft Office, se provádí výpočet rizikového skóre na základě určených vstupních dat a zároveň se vyhodnotí úroveň rizika. Výsledky jsou přehledně vyobrazeny na dashboardu. Jednotlivě pro každé riziko lze zaznamenat i více návrhů opatření včetně odpovědností podle RACI matice a následně sledovat nebo spravovat jejich stav i účinnost. Nechybí možnost seřazení ani filtrování dat dle různých kritérií, tím je zajištěna snadná orientace a flexibilita při používání nástroje.

Nástroj obstál i z pohledu nefunkčních požadavků. Implementace do prostředí Microsoft Excel představuje dostupnost široké veřejnosti vzhledem k rozšířenosti balíčku Microsoft Office na trhu. To zajišťuje dostupnost bez nutnosti dalšího softwaru a také nízké nároky na hardware, kdy Microsoft Excel se nejvíce jeví jako hardwarově náročný program. Uživatelské rozhraní nástroje je přehledné, logicky rozřazené a ovladatelné i pro méně zkušené uživatele. Automatizace hlavních činností pomocí maker usnadňuje práci a snižuje chybovost. Nástroji chybí flexibilita, pro určení úrovně rizika je pevně daná hodnotící škála rozsahu. Bezpečnost dat není nijak speciálně modifikovaná, nástroj se spoléhá na politiku prostředí Microsoft Excel. Při hromadném zapisování dat do nástroje může být nevýhodou přepisování dat z externích zdrojů, kdy proces se může časově prodloužit. Dále se ukázalo,

že výpočty rizika a opatření nejsou dostupné mimo vstupy z formuláře. Nástroj vypadá modulárně, ale podle názoru autora plně nevyhovuje této vlastnosti. Tyhle nedostatky by mohly být brány v potaz při dalším vývoji nástroje.

6.2 Využitelnost nástroje

Vytvořený nástroj pro řízení rizik je díky své struktuře a zvolenému prostředí využitelný skrz široké množství organizací. Byl navržen tak aby splňoval jednoduchost, přehlednost a dostupnost, což umožňuje jeho používání i v prostředí, kde není možnost specializovaného softwaru. Vzhledem ke zpracování v Microsoft Excel jej lze snadno využívat na většině běžných pracovištích.

Nástroj se osvědčil v příkladu neziskové organizace, a proto je vhodný i pro menší organizace, kde bude možná jeho uplatitelnost. Podporuje systematické vedení katalogů aktiv, hrozeb i zranitelností, přehledů rizik, opatření i odpovědností, čímž vystihuje proces řízení rizik v souladu s běžně uznávanými postupy a metodami. Automatizace usnadňuje proces rozhodování o prioritách a zavedených opatřeních. Možnost filtrovat data, sledovat přehledový dashboard přispívají ke vhodné prezentaci výsledků vedení organizace. Díky modularitě prostředí Microsoft Excel lze nástroj upravovat potřebám organizace pro spolehlivější proces. Pro organizace, které hledají základní nástroj řízení rizik bez nutnosti nákladných profesionálních softwarů, představuje tento nástroj ideálně dostupnou variantu.

ZÁVĚR

Cílem bakalářské práce bylo navrhnout a implementovat nástroj vhodný pro řízení rizik v prostředí Microsoft Excel. Tento cíl se podařil naplnit vytvořením funkčního, jednoduchého a přehledného nástroje, který umožňuje evidenci aktiv, hrozeb, zranitelností a opatření s odpovědnostmi, včetně automatizace výpočtů rizikového skóre a sledování úrovně rizik nebo stavu navrhnutých opatření.

Při testování nástroje na modelovém příkladu neziskové organizace se potvrdila skutečnost, že navržená makra plní funkci spolehlivě a nástroj tak může být využíván i uživateli bez hlubšího smyslu chápání programování. Řešení disponuje velmi silnou stránkou jako je dostupnost, přehlednost nebo nízké systémové nároky na používání Microsoft Excelu. Mezi vhodné možnosti pro zlepšení nástroje lze považovat např. podporu výpočtů mimo formulářové vstupy nebo možnost individuální konfigurace škály úrovně rizika nebo kategorií.

Práce mi umožnila propojit teoretické znalosti z oblasti řízení rizik a praktickými znalostmi kancelářských aplikací. Během tvorby nástroje jsem rozšířil své dovednosti zejména v oblasti tvorby maker, složitějších funkcí ale také i v oblasti uvažování nad použitelností a uživatelskou přívětivostí řešení. Věřím, že vytvořený nástroj může sloužit jako základ pro vedení rizik organizacím, které hledají jednoduchý způsob, jak začít systematicky řešit řízení rizik bez nutnosti investování do drahého profesionálního softwaru.

SEZNAM POUŽITÉ LITERATURY

- [1] ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. V Tribunu EU vyd. 1. Knihovnicka.cz. Brno: Tribun EU, 2009. ISBN 9788073997311.
- [2] Terminologický slovník – krizové řízení a plánování obrany státu. Ministerstvo vnitra České republiky [online]. Praha: Odbor bezpečnostní politiky a prevence kriminality, c2022, 8. června 2016 [cit. 2025-2-9]. Dostupné z: <https://www.mvcr.cz/clanek/terminologicky-slovník-krizove-řízení-a-planování-obrany-státu.aspx>.
- [3] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 9788024746449.
- [4] KOTKOVÁ, Dora. *Krizové plánování a řízení, Řízení rizik*. Zlín, 2022. Přednáška pro studenty oboru BTSM. [cit. 2025-2-9].
- [5] LUKÁŠ, Luděk. *Teorie bezpečnosti I*. Zlín: Radim Bačuvčík – VeRBuM, 2017. ISBN 978-80-87500-89-7.
- [6] WIKISKRYPTA. *Expozice v pracovním prostředí* [online]. [cit. 2025-03-15]. Dostupné z: https://www.wikiskripta.eu/w/Expozice_v_pracovním_prostředí
- [7] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II*. Zlín: Radim Bačuvčík – VeRBuM, 2012. ISBN 978-80-87500-19-4.
- [8] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I*.
- [9] PECINOVSKÝ, Josef. *Microsoft Excel 2019: Podrobný průvodce*. Brno: Computer Press, 2019. ISBN 978-80-251-5172-2.
- [10] ALEXANDER, Michael a Richard KUSLEIKA. *Microsoft Excel 2021 Bible*. Hoboken: Wiley, 2021. ISBN 978-1-119-83710-6.
- [11] GOLDMEIER, Jordan a Purnachandra DUGGIRALA. *Dashboard Design in Excel*. Birmingham: Packt Publishing, 2015. ISBN 978-1785286341.
- [12] LAM, James. *Enterprise Risk Management: From Incentives to Controls*. Hoboken: Wiley, 2014. ISBN 978-1118414143.
- [13] GOOGLE. *Google Sheets Help*. [online]. 2024. [cit. 2025-03-19]. Dostupné z: <https://support.google.com/docs/>

- [14] THE DOCUMENT FOUNDATION. *LibreOffice Calc Guide 7.5*. [online]. 2023. [cit. 2025-03-19]. Dostupné z: <https://documentation.libreoffice.org>
- [15] APPLE INC. *Numbers User Guide for Mac*. [online]. Apple Support, 2024. [cit. 2025-03-19]. Dostupné z: <https://support.apple.com/numbers>
- [16] Brain tools. *Brain tools* [online]. Olomouc: BRAIN TOOLS GROUP, c2014-2025 [cit. 2025-04-12]. Dostupné z: <https://www.braintools.cz/toolbox/zvladani-rizik/jak-analyzovat-rizika.htm>
- [17] KRÁLÍK, Lukáš. Administrativní bezpečnost, Information Security Management System – ISMS. Zlín, 2022. Přednáška pro studenty oboru BTSM. [cit. 2025-5-19].

SEZNAM OBRÁZKŮ

Obrázek 1 Vnější a vnitřní hrozby	14
Obrázek 2 Postup hodnocení rizik	18
Obrázek 3 Diagram funkčnosti nástroje	27
Obrázek 4 Rozložení katalogu aktiv	34
Obrázek 5 Rozložení katalogu hrozeb	37
Obrázek 6 Rozložení katalogu zranitelností	38
Obrázek 7 Formulář zapisování propojení.....	38
Obrázek 8 Riziková matice.....	40
Obrázek 9 Grafické znázornění počtu úrovní rizik po zavedení opatření	43
Obrázek 10 Grafické znázornění počtu opatření v kategorii stav opatření.....	44
Obrázek 11 Grafický přehled rizik modelové organizace	48
Obrázek 12 Grafické znázornění počtu rizik po zavedení opatření.....	49

SEZNAM TABULEK

Tabulka 1 Porovnání tabulkových procesorů.....	24
Tabulka 2 Kritičnost aktiva.....	35
Tabulka 3 Četnost výskytu hrozby.....	36
Tabulka 4 Dopad hrozby.....	36
Tabulka 5 Míra zranitelnosti.....	37

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ALE annualized loss expectancy

VBA Visual Basic for Application

RACI (R) Responsible, (A) Accountable, (C) Consulted, (I) Informed

SEZNAM PŘÍLOH

Příloha P I:	Zapisování do katalogu aktiv
Příloha P II:	Zapisování do katalogu hrozeb
Příloha P III:	Zapisování do katalogu zranitelností
Příloha P IV:	Propojení katalogů
Příloha P V:	Zapsání opatření
Příloha P VI:	Zpracování dokončených opatření
Příloha P VII:	Třídění, filtr a vymazání filtru katalogů
Příloha P VIII:	Třídění, filtr a vymazání filtru rizik
Příloha P IX:	Třídění, filtr a vymazání filtru opatření
Příloha P X:	Katalog aktiv modelové organizace
Příloha P XI:	Katalog hrozeb modelové organizace
Příloha P XII:	Katalog zranitelností modelové organizace
Příloha P XIII:	Přehled rizik modelové organizace
Příloha P XIV:	Ukázka dashboardu

PŘÍLOHA P I: ZAPISOVÁNÍ DO KATALOGU AKTIV

```
Sub ZapsatAktivum()  
    Dim wsZdroj As Worksheet, wsCil As Worksheet  
    Set wsZdroj = ThisWorkbook.Sheets("Dashboard")  
    Set wsCil = ThisWorkbook.Sheets("Aktiva")  
  
    ' Načtení dat z formuláře  
    Dim Nazev As String, Kategorie As String, kriticnost As String  
    Nazev = wsZdroj.Range("B16").Value  
    Kategorie = wsZdroj.Range("D16").Value  
    kriticnost = wsZdroj.Range("F16").Value  
  
    If Nazev = "" Or Kategorie = "" Or kriticnost = "" Then  
        MsgBox "Vyplň prosím všechna pole pro zapsání aktiva.", vbExclamation  
        Exit Sub  
    End If  
  
    ' Získání čísla kritičnosti  
    Dim KriticnostCislo As String  
    KriticnostCislo = Trim(Split(kriticnost, "-")(0))  
  
    ' Najdi poslední řádek tabulky pod hlavičkou (B10:F10)  
    Dim posledniRadek As Long  
    posledniRadek = wsCil.Cells(wsCil.Rows.Count, "B").End(xlUp).Row  
    Dim cilovyRadek As Long  
  
    If posledniRadek < 10 Then  
        cilovyRadek = 11  
    Else  
        cilovyRadek = posledniRadek + 1  
    End If  
  
    ' Zapsání dat do tabulky (sloupce B-F = 2-6)  
    wsCil.Cells(cilovyRadek, 2).Value = "A" & Format(cilovyRadek - 10, "000") ' ID Aktiva  
    wsCil.Cells(cilovyRadek, 3).Value = Nazev  
    wsCil.Cells(cilovyRadek, 4).Value = Kategorie  
    wsCil.Cells(cilovyRadek, 5).Value = KriticnostCislo  
  
    ' Vyčištění formuláře  
    wsZdroj.Range("B16").MergeArea.ClearContents  
    wsZdroj.Range("D16").MergeArea.ClearContents  
    wsZdroj.Range("F16").MergeArea.ClearContents  
  
    MsgBox "Aktivum bylo uloženo do tabulky na listu 'Aktiva'.", vbInformation  
End Sub
```

PŘÍLOHA P II: ZAPISOVÁNÍ DO KATALOGU HROZEB

```
Sub ZapsatHrozbu()  
    Dim wsZdroj As Worksheet, wsCil As Worksheet  
    Set wsZdroj = ThisWorkbook.Sheets("Dashboard")  
    Set wsCil = ThisWorkbook.Sheets("Hrozby")  
  
    ' Načtení dat  
    Dim Nazev As String, Kategorie As String, cetnost As String, dopad As String  
    Nazev = wsZdroj.Range("I16").Value  
    Kategorie = wsZdroj.Range("K16").Value  
    cetnost = wsZdroj.Range("M16").Value  
    dopad = wsZdroj.Range("O16").Value  
  
    If Nazev = "" Or Kategorie = "" Or cetnost = "" Or dopad = "" Then  
        MsgBox "Vyplň prosím všechna pole pro zapsání hrozby.", vbExclamation  
        Exit Sub  
    End If  
  
    Dim CetnostCislo As String, DopadCislo As String  
    CetnostCislo = Trim(Split(cetnost, "-")(0))  
    DopadCislo = Trim(Split(dopad, "-")(0))  
  
    ' Najdi poslední řádek tabulky pod hlavičkou (B10:G10)  
    Dim posledniRadek As Long, cilovyRadek As Long  
    posledniRadek = wsCil.Cells(wsCil.Rows.Count, "B").End(xlUp).Row  
  
    If posledniRadek < 10 Then  
        cilovyRadek = 11  
    Else  
        cilovyRadek = posledniRadek + 1  
    End If  
  
    ' Zápis do tabulky  
    wsCil.Cells(cilovyRadek, 2).Value = "H" & Format(cilovyRadek - 10, "000")  
    wsCil.Cells(cilovyRadek, 3).Value = Nazev  
    wsCil.Cells(cilovyRadek, 4).Value = Kategorie  
    wsCil.Cells(cilovyRadek, 5).Value = CetnostCislo  
    wsCil.Cells(cilovyRadek, 6).Value = DopadCislo  
  
    ' Vyčištění vstupních polí  
    wsZdroj.Range("I16").MergeArea.ClearContents  
    wsZdroj.Range("K16").MergeArea.ClearContents  
    wsZdroj.Range("M16").MergeArea.ClearContents  
    wsZdroj.Range("O16").MergeArea.ClearContents  
  
    MsgBox "Hrozba byla uložena do listu 'Hrozby'.", vbInformation  
End Sub
```

PŘÍLOHA P III: ZAPISOVÁNÍ KATALOGU ZRANITELNOSTÍ

```
Sub ZapsatZranitelnost()  
    Dim wsZdroj As Worksheet, wsCil As Worksheet  
    Set wsZdroj = ThisWorkbook.Sheets("Dashboard")  
    Set wsCil = ThisWorkbook.Sheets("Zranitelnost")  
  
    ' Načtení dat  
    Dim Nazev As String, Kategorie As String, Mira As String  
    Nazev = wsZdroj.Range("R16").Value  
    Kategorie = wsZdroj.Range("T16").Value  
    Mira = wsZdroj.Range("V16").Value  
  
    If Nazev = "" Or Kategorie = "" Or Mira = "" Then  
        MsgBox "Vyplň prosím všechna pole pro zapsání zranitelnosti.", vbExclamation  
        Exit Sub  
    End If  
  
    Dim MiraCislo As String  
    MiraCislo = Trim(Split(Mira, "-")(0))  
  
    ' Najdi poslední řádek tabulky pod hlavičkou (B10:F10)  
    Dim posledniRadek As Long, cilovyRadek As Long  
    posledniRadek = wsCil.Cells(wsCil.Rows.Count, "B").End(xlUp).Row  
  
    If posledniRadek < 10 Then  
        cilovyRadek = 11  
    Else  
        cilovyRadek = posledniRadek + 1  
    End If  
  
    ' Zápis do tabulky  
    wsCil.Cells(cilovyRadek, 2).Value = "Z" & Format(cilovyRadek - 10, "000")  
    wsCil.Cells(cilovyRadek, 3).Value = Nazev  
    wsCil.Cells(cilovyRadek, 4).Value = Kategorie  
    wsCil.Cells(cilovyRadek, 5).Value = MiraCislo  
  
    ' Vyčištění vstupních polí  
    wsZdroj.Range("R16").MergeArea.ClearContents  
    wsZdroj.Range("T16").MergeArea.ClearContents  
    wsZdroj.Range("V16").MergeArea.ClearContents  
  
    MsgBox "Zranitelnost byla uložena do listu 'Zranitelnost'.", vbInformation  
End Sub
```

PŘÍLOHA P IV: PROPOJEJÍ KATALOGŮ

```
Sub ZapsatRizikoDoTabulky()  
    Dim wsDash As Worksheet, wsAktiva As Worksheet, wsHrozby As Worksheet  
    Dim wsZranitelnost As Worksheet, wsRizika As Worksheet  
    Dim nazevA As String, nazevH As String, nazevZ As String  
    Dim cetnost As Long, dopad As Long, zranitelnost As Long, kriticitnost As Long  
    Dim vyslednaCetnost As Long, vyslednyDopad As Long, skore As Long  
    Dim uroven As String, radekRizik As Long  
  
    Set wsDash = ThisWorkbook.Sheets("Dashboard")  
    Set wsAktiva = ThisWorkbook.Sheets("Aktiva")  
    Set wsHrozby = ThisWorkbook.Sheets("Hrozby")  
    Set wsZranitelnost = ThisWorkbook.Sheets("Zranitelnost")  
    Set wsRizika = ThisWorkbook.Sheets("Rizika")  
  
    ' Přímé názvy z formuláře (bez dělení)  
    nazevA = wsDash.Range("Y16").Value  
    nazevH = wsDash.Range("AB16").Value  
    nazevZ = wsDash.Range("AE16").Value  
  
    If nazevA = "" Or nazevH = "" Or nazevZ = "" Then  
        MsgBox "Vypĺíte prosim všechny položky formuláře.", vbExclamation  
        Exit Sub  
    End If  
  
    ' Načtení číselných hodnot z tabulek podle názvů  
    cetnost = Application.WorksheetFunction.XLookup(nazevH, wsHrozby.Range("C11:C1000"), wsHrozby.Range("E11:E1000"))  
    dopad = Application.WorksheetFunction.XLookup(nazevH, wsHrozby.Range("C11:C1000"), wsHrozby.Range("F11:F1000"))  
    kriticitnost = Application.WorksheetFunction.XLookup(nazevA, wsAktiva.Range("C11:C1000"), wsAktiva.Range("E11:E1000"))  
    zranitelnost = Application.WorksheetFunction.XLookup(nazevZ, wsZranitelnost.Range("C11:C1000"), wsZranitelnost.Range("E11:E1000"))  
  
    ' Výpočty  
    vyslednaCetnost = Application.WorksheetFunction.Max(cetnost, zranitelnost)  
    vyslednyDopad = Application.WorksheetFunction.Max(dopad, kriticitnost)  
    skore = vyslednaCetnost * vyslednyDopad  
  
    ' Určení úrovně rizika podle škály  
    Select Case skore  
        Case 1 To 4: uroven = "Nizké"  
        Case 5 To 10: uroven = "Střední"  
        Case 11 To 16: uroven = "Vysoké"  
        Case 17 To 25: uroven = "Kritické"  
        Case Else: uroven = "Neurčeno"  
    End Select  
  
    ' Najdi poslední řádek  
    radekRizik = wsRizika.Cells(wsRizika.Rows.Count, 2).End(xlUp).Row  
    If radekRizik < 10 Then radekRizik = 10  
    radekRizik = radekRizik + 1  
  
    ' Zápis do tabulky  
    With wsRizika  
        .Cells(radekRizik, 2).Value = "R" & Format(radekRizik - 10, "000")  
        .Cells(radekRizik, 3).Value = nazevA  
        .Cells(radekRizik, 4).Value = nazevH  
        .Cells(radekRizik, 5).Value = nazevZ  
        .Cells(radekRizik, 6).Value = cetnost  
        .Cells(radekRizik, 7).Value = zranitelnost  
        .Cells(radekRizik, 8).Value = vyslednaCetnost  
        .Cells(radekRizik, 9).Value = vyslednyDopad  
        .Cells(radekRizik, 10).Value = skore  
        .Cells(radekRizik, 11).Value = uroven  
    End With  
  
    ' Vyděštění formuláře  
    wsDash.Range("Y16").MergeArea.ClearContents  
    wsDash.Range("AB16").MergeArea.ClearContents  
    wsDash.Range("AE16").MergeArea.ClearContents  
  
    MsgBox "Riziko bylo úspěšně zapsáno do tabulky.", vbInformation  
End Sub
```

PŘÍLOHA P V: ZAPSÁNÍ OPATŘENÍ

```
Sub ZapsatOpatreni()  
    Dim wsDash As Worksheet, wsRizika As Worksheet, wsOpatreni As Worksheet  
    Dim rizikoVstup As String, rizikoID As String, urovenRizika As String  
    Dim nazevOpatreni As String, rOdp As String, aOdp As String, cOdp As String, iOdp As String  
    Dim termin As String, vystraha As String  
    Dim radekOpatreni As Long, dnes As Date, zadaneDatum As Date  
    Dim zprava As String  
    Dim aktivum As String, hrozba As String, zranitelnost As String  
  
    Set wsDash = ThisWorkbook.Sheets("Dashboard")  
    Set wsRizika = ThisWorkbook.Sheets("Rizika")  
    Set wsOpatreni = ThisWorkbook.Sheets("Opatření")  
  
    ' Vstupy z dashboardu  
    rizikoVstup = wsDash.Range("Y26").value  
    nazevOpatreni = wsDash.Range("AB26").value  
    rOdp = wsDash.Range("AE27").value  
    aOdp = wsDash.Range("AE28").value  
    cOdp = wsDash.Range("AE29").value  
    iOdp = wsDash.Range("AE30").value  
    termin = wsDash.Range("AG26").value  
  
    ' Kontrola povinných vstupů  
    If rizikoVstup = "" Or nazevOpatreni = "" Or termin = "" Then  
        MsgBox "Vypĺň prosim všechna požadovaná pole (riziko, název, termin).", vbExclamation  
        Exit Sub  
    End If  
  
    rizikoID = Trim(Split(rizikoVstup, " - ")(1))  
  
    ' Načti riziko z tabulky Rizika  
    On Error Resume Next  
    urovenRizika = Application.WorksheetFunction.XLookup(rizikoID, wsRizika.Range("B11:B1000"), wsRizika.Range("K11:K1000"))  
    aktivum = Application.WorksheetFunction.XLookup(rizikoID, wsRizika.Range("B11:B1000"), wsRizika.Range("C11:C1000"), "")  
    hrozba = Application.WorksheetFunction.XLookup(rizikoID, wsRizika.Range("B11:B1000"), wsRizika.Range("D11:D1000"), "")  
    zranitelnost = Application.WorksheetFunction.XLookup(rizikoID, wsRizika.Range("B11:B1000"), wsRizika.Range("E11:E1000"), "")  
    On Error GoTo 0  
  
    vystraha = ""  
    dnes = Date  
    If IsDate(termin) Then zadaneDatum = CDate(termin)  
  
    If Trim(LCase(urovenRizika)) = "kritické" And zadaneDatum > DateAdd("d", 30, dnes) Then  
        vystraha = "Doporučeno do 30 dnů!"  
    End If  
  
    ' Najdi volný řádek  
    radekOpatreni = wsOpatreni.Cells(wsOpatreni.Rows.Count, 2).End(xlUp).Row  
    If radekOpatreni < 11 Then radekOpatreni = 11  
    radekOpatreni = radekOpatreni + 1  
  
    With wsOpatreni  
        .Cells(radekOpatreni, 2).value = "O" & Format(radekOpatreni - 11, "000")  
        .Cells(radekOpatreni, 3).value = rizikoID  
        .Cells(radekOpatreni, 4).value = aktivum & ", " & Chr(10) & hrozba & ", " & Chr(10) & zranitelnost & ", "  
        .Cells(radekOpatreni, 4).WrapText = True  
        .Cells(radekOpatreni, 5).value = nazevOpatreni  
        .Cells(radekOpatreni, 6).value = rOdp  
        .Cells(radekOpatreni, 7).value = aOdp  
        .Cells(radekOpatreni, 8).value = cOdp  
        .Cells(radekOpatreni, 9).value = iOdp  
        .Cells(radekOpatreni, 10).value = CDate(termin)  
        .Cells(radekOpatreni, 10).NumberFormat = "dd.mm.yyyy"  
        .Cells(radekOpatreni, 11).value = vystraha  
        .Cells(radekOpatreni, 12).value = "Navrženo"  
  
        If vystraha <> "" Then  
            .Cells(radekOpatreni, 11).Interior.Color = RGB(255, 0, 0)  
            .Cells(radekOpatreni, 11).Font.Color = RGB(255, 255, 255)  
        End If  
    End With  
  
    wsDash.Range("Y26").MergeArea.ClearContents  
    wsDash.Range("AB26").MergeArea.ClearContents  
    wsDash.Range("AE27").MergeArea.ClearContents  
    wsDash.Range("AE28").MergeArea.ClearContents  
    wsDash.Range("AE29").MergeArea.ClearContents  
    wsDash.Range("AE30").MergeArea.ClearContents  
    wsDash.Range("AG26").MergeArea.ClearContents  
  
    zprava = "Opatření bylo úspěšně zapsáno do tabulky."  
    If vystraha <> "" Then  
        zprava = zprava & vbCrLf & vbCrLf & "!!UPOZORNĚNÍ!! Pro kritické riziko bylo přidáno doporučení."  
    End If  
  
    MsgBox zprava, vbInformation  
End Sub
```

PŘÍLOHA P VI: ZPRACOVÁNÍ DOKONČENÝCH OPATŘENÍ

```
Sub GenerovatRizikaPoOpatreni()
    Dim wsOpatreni As Worksheet, wsRizika As Worksheet, wsVystup As Worksheet
    Dim dict As Object
    Dim i As Long, radekVystup As Long
    Dim rizikoID As String, opatreniStav As String, opatreniNazev As String
    Dim ucinnostRaw As Variant, ucinnost As Double
    Dim skorePuvodni As Double, skoreVysledne As Double
    Dim rizikoUroven As String
    Dim ucinnosti() As Double

    Set wsOpatreni = ThisWorkbook.Sheets("Opatřeni")
    Set wsRizika = ThisWorkbook.Sheets("Rizika")
    Set wsVystup = ThisWorkbook.Sheets("RizikaPoOpatřeni")
    Set dict = CreateObject("Scripting.Dictionary")

    ' Sbírej opatření (stav "Dokončeno" nebo "Odmítnuto") podle ID rizika (sloupec 3)
    For i = 12 To wsOpatreni.Cells(wsOpatreni.Rows.Count, 2).End(xlUp).Row
        rizikoID = Trim(wsOpatreni.Cells(i, 3).value)
        opatreniStav = Trim(wsOpatreni.Cells(i, 12).value) ' sloupec Stav
        opatreniNazev = wsOpatreni.Cells(i, 5).value ' sloupec Název opatření
        ucinnostRaw = wsOpatreni.Cells(i, 13).value ' sloupec Účinnost opatření

        If opatreniStav = "Dokončeno" Or opatreniStav = "Odmítnuto" Then
            If Not dict.Exists(rizikoID) Then
                Dim podDict As Object
                Set podDict = CreateObject("Scripting.Dictionary")
                podDict("název") = opatreniNazev
                podDict("účinnosti") = Array()
                Set dict(rizikoID) = podDict
            Else
                dict(rizikoID)("název") = dict(rizikoID)("název") & ", " & opatreniNazev
            End If

            ' Účinnost
            If Trim(ucinnostRaw & "") <> "" And IsNumeric(ucinnostRaw) Then
                ucinnost = CDBl(ucinnostRaw)
            ElseIf opatreniStav = "Odmítnuto" Then
                ucinnost = 0
            Else
                MsgBox "U opatření '" & opatreniNazev & "' (řádek " & i & ") není vyplněna účinnost.", vbExclamation
                GoTo Skip
            End If

            dict(rizikoID)("účinnosti") = AppendToArray(dict(rizikoID)("účinnosti"), ucinnost)
        End If
    Next i

    Skip:
    ' Výstup do RizikaPoOpatření
    radekVystup = 11
    For i = 11 To wsRizika.Cells(wsRizika.Rows.Count, 2).End(xlUp).Row
        rizikoID = wsRizika.Cells(i, 2).value
        If dict.Exists(rizikoID) Then
            With wsVystup
                .Cells(radekVystup, 2).value = rizikoID
                .Cells(radekVystup, 3).value = wsRizika.Cells(i, 3).value ' Aktivum
                .Cells(radekVystup, 4).value = wsRizika.Cells(i, 4).value ' Hrozba
                .Cells(radekVystup, 5).value = wsRizika.Cells(i, 5).value ' Zranitelnost
                .Cells(radekVystup, 6).value = dict(rizikoID)("název")

                If IsNumeric(wsRizika.Cells(i, 10).value) Then
                    skorePuvodni = CDBl(wsRizika.Cells(i, 10).value)
                Else
                    skorePuvodni = 0
                End If

                Dim faktor, kumulativniFaktor As Double
                kumulativniFaktor = 1
                For Each faktor In dict(rizikoID)("účinnosti")
                    kumulativniFaktor = kumulativniFaktor * (1 - faktor)
                Next faktor

                skoreVysledne = Round(skorePuvodni * kumulativniFaktor, 1)
                .Cells(radekVystup, 7).value = skoreVysledne

                Select Case skoreVysledne
                    Case Is <= 4: rizikoUroven = "Nizké"
                    Case 5 To 11: rizikoUroven = "Střední"
                    Case 12 To 19: rizikoUroven = "Vysoké"
                    Case Is >= 20: rizikoUroven = "Kritické"
                End Select

                .Cells(radekVystup, 8).value = rizikoUroven

                If rizikoUroven = "Nizké" Then
                    .Cells(radekVystup, 9).value = "Akceptovatelné"
                ElseIf rizikoUroven = "Kritické" Then
                    .Cells(radekVystup, 9).value = "Neakceptovatelné"
                End If
            End With
            radekVystup = radekVystup + 1
        End If
    Next i

    MsgBox "Rizika byla úspěšně přegenerována z dokončených i odmítnutých opatření.", vbInformation
End Sub
```

```
Function AppendToArray(arr As Variant, value As Double) As Variant
    Dim temp() As Double, i As Long
    ReDim temp(UBound(arr) + 1)
    For i = 0 To UBound(arr)
        temp(i) = arr(i)
    Next i
    temp(UBound(temp)) = value
    AppendToArray = temp
End Function
```

PŘÍLOHA P VII: TŘÍDĚNÍ, FILTR A VYMAZÁNÍ FILTRU KATALOGŮ

```
Sub FiltrovatAktiva()  
    Dim ws As Worksheet  
    Set ws = ThisWorkbook.Sheets("Aktiva")  
  
    Dim kategorie As String  
    kategorie = InputBox("Zadej název kategorie pro filtrování:" & vbCrLf & _  
        "- Informační" & vbCrLf & _  
        "- Technologické" & vbCrLf & _  
        "- Fyzické" & vbCrLf & _  
        "- Bezpečnostní" & vbCrLf & _  
        "- Personální" & vbCrLf & _  
        "- Právní" & vbCrLf & _  
        "- Jiné", "Filtr kategorie")  
  
    If kategorie = "" Then Exit Sub  
  
    With ws  
        .Range("All").AutoFilter Field:=3, Criteria:=kategorie  
    End With  
End Sub  


---

  
Sub SeraditAktiva()  
    Dim ws As Worksheet  
    Dim posledniRadek As Long  
    Dim customOrder As String  
    Dim rozsahTabulky As Range  
  
    Set ws = ThisWorkbook.Sheets("Aktiva")  
    posledniRadek = ws.Cells(ws.Rows.Count, 2).End(xlUp).Row  
    customOrder = "Informační, Technologické, Fyzické, Bezpečnostní, Personální, Právní, Jiné"  
    If ws.AutoFilterMode Then ws.AutoFilter.ShowAllData  
    Set rozsahTabulky = ws.Range("B10:E" & posledniRadek)  
    ws.Sort.SortFields.Clear  
    ws.Sort.SortFields.Add _  
        Key:=ws.Range("D11:D" & posledniRadek), _  
        SortOn:=xlSortOnValues, Order:=xlAscending, DataOption:=xlSortNormal  
  
    With ws.Sort  
        .SetRange rozsahTabulky  
        .Header = xlYes  
        .MatchCase = False  
        .Orientation = xlTopToBottom  
        .SortFields(1).customOrder = customOrder  
        .Apply  
    End With  
End Sub  


---

  
Sub ResetovatAktiva()  
    Dim ws As Worksheet  
    Dim posledniRadek As Long  
    Dim rozsahTabulky As Range  
  
    Set ws = ThisWorkbook.Sheets("Aktiva")  
    posledniRadek = ws.Cells(ws.Rows.Count, 2).End(xlUp).Row  
    If ws.AutoFilterMode Then ws.AutoFilter.ShowAllData  
    Set rozsahTabulky = ws.Range("B10:E" & posledniRadek)  
    ws.Sort.SortFields.Clear  
    ws.Sort.SortFields.Add _  
        Key:=ws.Range("B11:E" & posledniRadek), _  
        SortOn:=xlSortOnValues, Order:=xlAscending, DataOption:=xlSortNormal  
    With ws.Sort  
        .SetRange rozsahTabulky  
        .Header = xlYes  
        .MatchCase = False  
        .Orientation = xlTopToBottom  
        .Apply  
    End With  
End Sub
```

PŘÍLOHA P VIII: TRŽDĚNÍ, FILTR A VYMAZÁNÍ FILTRU RIZIK

```
Sub FiltrovatRizika()  
    Dim ws As Worksheet  
    Dim uroven As String  
  
    Set ws = ThisWorkbook.Sheets("Rizika")  
  
    uroven = InputBox("Zadej úroveň rizika pro filtrování:" & vbCrLf & _  
        "- Kritické" & vbCrLf & _  
        "- Vysoké" & vbCrLf & _  
        "- Střední" & vbCrLf & _  
        "- Nízké", _  
        "Filtr úrovně rizika")  
  
    If uroven = "" Then Exit Sub  
  
    ws.Range("B10:K10").AutoFilter Field:=10, Criteria:=uroven  
End Sub
```

```
Sub SeraditRizika()  
    Dim ws As Worksheet  
    Dim posledniRadek As Long  
    Dim customOrder As String  
    Dim rozsah As Range  
  
    Set ws = ThisWorkbook.Sheets("Rizika")  
    posledniRadek = ws.Cells(ws.Rows.Count, 2).End(xlUp).Row  
    customOrder = "Kritické,Vysoké,Střední,Nízké"  
    Set rozsah = ws.Range("B10:K" & posledniRadek)  
    If ws.AutoFilterMode Then ws.AutoFilter.ShowAllData  
    ws.Sort.SortFields.Clear  
    ws.Sort.SortFields.Add  
        Key:=ws.Range("K11:K" & posledniRadek), _  
        SortOn:=xlSortOnValues, Order:=xlAscending, DataOption:=xlSortNormal  
    With ws.Sort  
        .SetRange rozsah  
        .Header = xlYes  
        .MatchCase = False  
        .Orientation = xlTopToBottom  
        .SortFields(1).customOrder = customOrder  
        .Apply  
    End With  
End Sub
```

```
Sub ResetovatRizika()  
    Dim ws As Worksheet  
    Dim posledniRadek As Long  
    Dim rozsah As Range  
  
    Set ws = ThisWorkbook.Sheets("Rizika")  
    posledniRadek = ws.Cells(ws.Rows.Count, 2).End(xlUp).Row  
    If ws.AutoFilterMode Then ws.AutoFilter.ShowAllData  
    Set rozsah = ws.Range("B10:K" & posledniRadek)  
    ws.Sort.SortFields.Clear  
    ws.Sort.SortFields.Add  
        Key:=ws.Range("B11:B" & posledniRadek), _  
        SortOn:=xlSortOnValues, Order:=xlAscending, DataOption:=xlSortNormal  
    With ws.Sort  
        .SetRange rozsah  
        .Header = xlYes  
        .MatchCase = False  
        .Orientation = xlTopToBottom  
        .Apply  
    End With  
End Sub
```

PŘÍLOHA P IX: TŘÍDĚNÍ, FILTR A VYMAZÁNÍ FILTRU OPATŘENÍ

```
Sub FiltrovatOpatreniPodleStavu()  
    Dim ws As Worksheet  
    Dim stav As String  
  
    Set ws = ThisWorkbook.Sheets("Opatřeni")  
  
    stav = InputBox("Zadej stav opatření pro filtrování:" & vbCrLf & _  
        "- Navrženo" & vbCrLf & "- V řešení" & vbCrLf & "- Dokončeno" & vbCrLf & "- Odmítnuto", _  
        "Filtr stavu opatření")  
  
    If stav = "" Then Exit Sub  
  
    ws.Range("B11:M11").AutoFilter Field:=11, Criteria1:=stav  
End Sub
```

```
Sub SeraditOpatreniPodleStavu()  
    Dim ws As Worksheet  
    Dim posledniRadek As Long  
    Dim rozsah As Range  
    Dim customOrder As String  
  
    Set ws = ThisWorkbook.Sheets("Opatřeni")  
    posledniRadek = ws.Cells(ws.Rows.Count, 2).End(xlUp).Row  
    Set rozsah = ws.Range("B10:M" & posledniRadek)  
    customOrder = "Navrženo,V řešení,Dokončeno,Odmítnuto"  
    If ws.AutoFilterMode Then ws.AutoFilter.ShowAllData  
    ws.Sort.SortFields.Clear  
    ws.Sort.SortFields.Add  
        Key:=ws.Range("L12:L" & posledniRadek), _  
        SortOn:=xlSortOnValues, Order:=xlAscending, DataOption:=xlSortNormal  
    With ws.Sort  
        .SetRange rozsah  
        .Header = xlYes  
        .MatchCase = False  
        .Orientation = xlTopToBottom  
        .SortFields(1).customOrder = customOrder  
        .Apply  
    End With  
End Sub
```

```
Sub SeraditOpatreniPodleTerminu()  
    Dim ws As Worksheet  
    Dim posledniRadek As Long  
    Dim rozsah As Range  
  
    Set ws = ThisWorkbook.Sheets("Opatřeni")  
    posledniRadek = ws.Cells(ws.Rows.Count, 2).End(xlUp).Row  
    Set rozsah = ws.Range("B10:M" & posledniRadek)  
    If ws.AutoFilterMode Then ws.AutoFilter.ShowAllData  
    ws.Sort.SortFields.Clear  
    ws.Sort.SortFields.Add  
        Key:=ws.Range("J12:J" & posledniRadek), _  
        SortOn:=xlSortOnValues, Order:=xlAscending, DataOption:=xlSortNormal  
    With ws.Sort  
        .SetRange rozsah  
        .Header = xlYes  
        .MatchCase = False  
        .Orientation = xlTopToBottom  
        .Apply  
    End With  
End Sub
```

```

Sub ResetovatOpatreni()
    Dim ws As Worksheet
    Dim posledniRadek As Long
    Dim rozsah As Range

    Set ws = ThisWorkbook.Sheets("Opatřeni")
    posledniRadek = ws.Cells(ws.Rows.Count, 2).End(xlUp).Row
    Set rozsah = ws.Range("B10:M" & posledniRadek)
    If ws.AutoFilterMode Then ws.AutoFilter.ShowAllData
    ws.Sort.SortFields.Clear
    ws.Sort.SortFields.Add _
        Key:=ws.Range("B12:B" & posledniRadek), _
        SortOn:=xlSortOnValues, Order:=xlAscending, DataOption:=xlSortNormal
    With ws.Sort
        .SetRange rozsah
        .Header = xlYes
        .MatchCase = False
        .Orientation = xlTopToBottom
        .Apply
    End With
End Sub

```

PŘÍLOHA P X: KATALOG AKTIV MODELOVÉ ORGANIZACE

ID Aktiva	Název	Kategorie	Kritičnost (hodnota)
A001	Databáze dárců	Informační	5
A002	E-mailový server	Technologické	4
A003	Notebook projektového manažera	Technologické	4
A004	Starý nábytek v kanceláři	Fyzické	1
A005	Kávovar	Fyzické	1
A006	Smlouvy s partnery	Právní	5
A007	Terenní pracovníci	Personální	5
A008	Centrální kancelář	Fyzické	4
A009	Mobilní telefon koordinátora	Technologické	3
A010	Účetní software	Technologické	4
A011	Dekorace v zasedací místnosti	Fyzické	1
A012	Dárcovský webový portál	Technologické	3
A013	Bezpečnostní kamery v kanceláři	Bezpečnostní	3
A014	Plány evakuace	Bezpečnostní	4
A015	Vnitřní směrnice organizace	Informační	3
A016	Dobrovolníci	Personální	4
A017	Seznam příjemců pomoci	Informační	4
A018	Smlouvy o pojištění	Právní	4
A019	Přístupové čipy ke kancelářím	Bezpečnostní	3
A020	Zásoby potravin pro distribuci	Fyzické	4
A021	Označení místností	Informační	2
A022	Kancelářské potřeby	Fyzické	2
A023	Zálohovací disk serveru	Technologické	4
A024	Databáze zaměstnanců	Informační	4
A025	Webové stránky organizace	Technologické	2
A026	Zdravotní dokumentace klientů	Informační	5
A027	Léky pro humanitární zásahy	Fyzické	5
A028	Finanční rezerva	Jiné	5
A029	Přenosné stany a přístřešky	Fyzické	3
A030	Router a síťová infrastruktura	Technologické	4
A031	Náhradní periferie	Fyzické	2
A032	Seznam kontaktů na krizové složky	Informační	2
A033	Přístupové údaje k bankovnímu účtu	Informační	5
A034	Interní školící materiály	Informační	3
A035	Zápisy z porad	Informační	3
A036	Regulérní zaměstnanci	Fyzické	5
A037	Záznamy o školení zaměstnanců	Informační	3
A038	Stany pro krizové ubytování	Fyzické	4
A039	Zásoby vody	Fyzické	4
A040	Loga a grafické podklady	Informační	2

PŘÍLOHA XI: KATALOG HROZEB MODELOVÉ ORGANIZACE

ID Hrozby	Název	Kategorie	Četnost výskytu	Dopad
H001	Zneužití osobních údajů dárců	Informační	3	5
H002	Únik dat v důsledku kybernetického útoku	Technologické	4	5
H003	Ztráta databáze kvůli chybě zálohování	Technologické	2	4
H004	Výpadek serveru	Technologické	3	3
H005	Phishingový útok na uživatele	Informační	3	4
H006	Ztráta e-mailové komunikace	Technologické	2	3
H007	Krádež notebooku s důvěrnými daty	Fyzické	3	4
H008	Poškození nebo ztráta dat	Technologické	2	4
H009	Neautorizovaný přístup k citlivým dokumentům	Informační	3	4
H010	Úraz zaměstnance způsobený nestabilním nábytkem	Fyzické	2	2
H011	Zkrat nebo únik vody způsobující škodu	Fyzické	2	2
H012	Ztráta důležitých smluv	Právní	2	4
H013	Porušení smluvních podmínek třetí stranou	Právní	2	3
H014	Neplatné nebo neaktuální smlouvy	Právní	2	4
H015	Nepokrytí specifických rizik v pojištění	Právní	2	3
H016	Požár nebo záplava	Fyzické	2	5
H017	Vniknutí nepovolané osoby	Bezpečnostní	2	3
H018	Výpadek elektřiny omezující provoz	Technologické	3	2
H019	Ztráta nebo krádež telefonu s citlivými daty	Fyzické	3	4
H020	Nevymazaná data při změně zařízení	Technologické	2	3
H021	Ztráta účetních dat kvůli softwarové chybě	Technologické	2	4
H022	Neoprávněná manipulace s účetními záznamy	Technologické	2	3
H023	Překážka evakuačnímu průchodu	Fyzické	2	2
H024	DDoS útok omezující přístup	Technologické	3	4
H025	Únik platebních informací	Technologické	2	5
H026	Změna obsahu po útoku	Technologické	2	4
H027	Selhání záznamového zařízení	Technologické	2	3
H028	Zneužití záznamů k porušení soukromí	Bezpečnostní	2	4
H029	Zastaralé nebo chybné evakuační plány	Bezpečnostní	2	3
H030	Nedostupné plány v době incidentu	Bezpečnostní	2	4
H031	Zastaralé interní postupy	Informační	3	2
H032	Nedodržování interních předpisů	Informační	2	3
H033	Zneužití pravomocí dobrovolníkem	Personální	2	4
H034	Nedostatečné zaškolení	Personální	3	3
H035	Neprofesionální chování vůči klientovi	Personální	2	2
H036	Únik údajů o příjemcích	Informační	3	5
H037	Ztráta informací kvůli technické chybě	Technologické	2	4
H038	Duplikace přístupového média	Bezpečnostní	2	3
H039	Ztráta čipu bez zablokování přístupu	Bezpečnostní	3	3
H040	Zkažení zásob	Fyzické	2	3
H041	Krádež potravin ze skladu	Fyzické	2	3
H042	Nedodání zásilky včas	Fyzické	2	2
H043	Nesrozumitelné značení bránící evakuaci	Informační	2	3
H044	Neaktuální označení kanceláří	Informační	2	2
H045	Nedostatek spotřebního materiálu	Fyzické	2	2
H046	Zpoždění dodávky při potřebě	Fyzické	2	1
H047	Selhání zálohovacího procesu	Technologické	2	4
H048	Poškození nebo ztráta disku	Technologické	2	3
H049	Neautorizovaný přístup k osobním údajům	Informační	3	4
H050	Ztráta informací o pracovnících	Informační	2	3

H051	Hacknutí webu a zveřejnění nevhodného obsahu	Technologické	3	4
H052	Výpadek webu	Technologické	3	3
H053	Zveřejnění zdravotních záznamů	Informační	2	5
H054	Ztráta nebo smazání lékařských údajů	Informační	2	5
H055	Nevhodné skladování ovlivňující účinnost	Fyzické	2	4
H056	Ztráta zásilký během přepravy	Fyzické	2	3
H057	Zneužití prostředků	Právní	2	4
H058	Nevhodné investování rezervy	Právní	2	3
H059	Poškození materiálu v důsledku počasí	Fyzické	2	2
H060	Nesprávné uskladnění	Fyzické	2	2
H061	Neautorizovaný přístup do sítě	Technologické	3	4
H062	Přetížení sítě vlivem útoku	Technologické	3	3
H063	Nepoužitelnost zařízení při potřebě	Fyzické	2	2
H064	Poškození bez zálohy	Technologické	2	3
H065	Zastaralé nebo chybné kontakty	Informační	2	2
H066	Nedostupnost seznamu během incidentu	Informační	2	3
H067	Přístup třetí strany k účtu	Informační	2	5
H068	Zneužití přihlašovacích údajů	Informační	2	5
H069	Zastaralý obsah	Informační	2	2
H070	Neautorizovaná změna školících dokumentů	Informační	2	2
H071	Nedodržení pracovních povinností	Personální	2	3
H072	Etické pochybení	Personální	2	3
H073	Ztráta záznamu ovlivňující audit	Informační	2	3
H074	Nesprávná evidence absolvovaných školení	Informační	2	2
H075	Nedostatečné vybavení během nasazení	Fyzické	2	3
H076	Poškození stanů kvůli nesprávnému skladování	Fyzické	2	2
H077	Kontaminace vody	Fyzické	2	4
H078	Nedostatek v době potřeby	Fyzické	2	3
H079	Zneužití loga třetí stranou	Informační	2	3
H080	Zveřejnění nevhodného grafického obsahu	Informační	2	3

PŘÍLOHA XII: KATALOG ZRANITELNOSTÍ MODELOVÉ ORGANIZACE

ID Zranitelnosti	Název	Kategorie	Míra
Z001	Nešifrovaná databáze	Technologické	5
Z002	Nezabezpečené Wi-Fi připojení	Technologické	4
Z003	Nepravidelné zálohování	Technologické	4
Z004	Zastaralý operační systém	Technologické	5
Z005	Chybějící školení uživatelů o phishingu	Personální	3
Z006	Chybějící záloha	Technologické	4
Z007	Neuzamčené místnosti	Fyzické	5
Z008	Nedostatečná údržba běžného vybavení	Technologické	2
Z009	Slabé nebo opakovaně používané hesla	Technologické	3
Z010	Neexistence pravidelné kontroly vybavení	Fyzické	2
Z011	Nezajištěný elektrický přívod	Fyzické	2
Z012	Nedodržení lhůt pro uchovávání dokumentace	Právní	3
Z013	Smlouvy neobsahují doložky o odpovědnosti	Právní	4
Z014	Chybějící havarijní plán	Bezpečnostní	4
Z015	Neexistující politika přístupových práv	Bezpečnostní	5
Z016	Absence záložního napájení	Technologické	3
Z017	Chybějící možnost vzdáleného smazání	Technologické	4
Z018	Neexistence procesu pro výmaz dat při převodu zařízení	Technologické	3
Z019	Zastaralý software bez záloh	Technologické	4
Z020	Chybějící logování přístupu	Technologické	3
Z021	Špatné rozmístění nábytku a dekorací	Fyzické	2
Z022	Používání nevhodných elektrických zařízení	Fyzické	3
Z023	Nenakonfigurovaná síťová ochrana	Technologické	4
Z024	Chybějící šifrování datových přenosů	Technologické	4
Z025	Nezabezpečený redakční systém webu	Technologické	4
Z026	Zastaralý hardware bez záloh	Technologické	3
Z027	Zneužití přístupových oprávnění	Bezpečnostní	4
Z028	Neexistence pravidelné revize plánů	Bezpečnostní	3
Z029	Fyzické plány nejsou snadno přístupné	Bezpečnostní	2
Z030	Neexistence revizí směrnic	Informační	3
Z031	Slabý dohled nad implementací pravidel	Informační	2
Z032	Dobrovolníci nemají ověřenou bezúhonnost	Personální	4
Z033	Neexistující školící plán	Personální	3
Z034	Neexistující etický kodex	Personální	3
Z035	Nešifrované uchovávání osobních údajů	Informační	5
Z036	Neaktuální seznam zákonných povinností	Právní	2
Z037	Chybějící právní přezkum smluv	Právní	3
Z038	Chybějící systém pro deaktivaci přístupů	Bezpečnostní	3
Z039	Neexistující správa vydaných čipů	Bezpečnostní	3
Z040	Nevhodné skladovací podmínky	Fyzické	3

Z041	Slabé fyzické zabezpečení skladu	Fyzické	3
Z042	Chybějící plán logistiky a sledování dodávek	Fyzické	3
Z043	Nevýrazné značení místností	Fyzické	1
Z044	Nepřehledná evidence rozmístění kanceláří	Informační	2
Z045	Neexistence monitoringu zásob	Fyzické	2
Z046	Chybějící smlouvy s dodavateli	Právní	2
Z047	Zálohování není pravidelně testováno	Technologické	3
Z048	Nechráněné fyzické umístění disku	Fyzické	3
Z049	Chybějící řízení oprávnění	Informační	4
Z050	Nezabezpečená administrace webu	Technologické	4
Z051	Nedostatek serverových prostředků	Technologické	3
Z052	Chybějící kontrola teploty	Fyzické	4
Z053	Nesledovaná logistika	Fyzické	3
Z054	Chybějící vnitřní finanční kontrola	Právní	4
Z055	Neexistence investičních pravidel	Právní	3
Z056	Neexistence kontrolního systému skladu	Fyzické	3
Z057	Router bez nastaveného firewallu	Technologické	4
Z058	Chybějící síťové monitorování	Technologické	3
Z059	Nepravidelná kontrola funkčnosti zařízení	Fyzické	2
Z060	Neexistence náhradních komponent	Fyzické	3
Z061	Neexistence aktualizacího procesu kontaktů	Informační	2
Z062	Papírová forma není dostupná elektronicky	Informační	2
Z063	Sdílené přihlašovací údaje	Informační	4
Z064	Uložení hesel v otevřeném formátu	Technologické	4
Z065	Školící materiály nejsou revidovány	Informační	2
Z066	Neexistence řízení verzí dokumentů	Informační	2
Z067	Chybějící přístupová kontrola k zápisům	Informační	2
Z068	Chybějící kontrolní mechanismy výkonu	Personální	3
Z069	Chybné zaznamenávání dat do systému	Informační	2
Z070	Nevytvořený kontrolní seznam vybavení	Fyzické	3
Z071	Sklad bez regulace teploty a vlhkosti	Fyzické	3
Z072	Chybějící sledování zásob vody	Fyzické	2
Z073	Loga nejsou chráněna autorským právem	Informační	2
Z074	Chybějící kontrola nad publikacemi	Informační	2

PŘÍLOHA P XIII: PŘEHLED RIZIK MODELOVÉ ORGANIZACE

ID Rizika	Aktivum	Hrozba	Zranitelnost	Četnost výskytu hrozby	Míra zranitelnosti	Výsledná četnost výskytu	Dopad	Rizikové skóre	Úroveň rizika
R001	Databáze dárců	Zneužití záznamů k porušení soukromí	Nešifrovaná databáze	2	5	5	5	25	Kritické
R002	Databáze dárců	Únik dat v důsledku kybernetického útoku	Nezabezpečené Wi-Fi připojení	4	4	4	5	20	Kritické
R003	Databáze dárců	Ztráta databáze kvůli chybě zálohování	Nepravidelné zálohování	2	4	4	5	20	Kritické
R004	E-mailový server	Vypadek serveru	Zastaralý operační systém	3	5	5	4	20	Kritické
R005	E-mailový server	Phishingový útok na uživatele	Chybějící školení uživatelů o phishingu	3	3	3	4	12	Vysoké
R006	E-mailový server	Ztráta e-mailové komunikace	Chybějící záloha	2	4	4	4	16	Vysoké
R007	Notebook projektového manažera	Krádež notebooku s důvěrnými daty	Neuzašifrované místnosti s citlivým vybavením	3	5	5	4	20	Kritické
R008	Notebook projektového manažera	Poškození nebo ztráta dat	Nedostatečná údržba běžného vybavení	2	2	2	4	8	Střední
R009	Notebook projektového manažera	Neautorizovaný přístup k citlivým dokumentům	Slabé nebo opakovaně používané hesla	3	3	3	4	12	Vysoké
R010	Starý nábytek v kanceláři	Úraz zaměstnance způsobený nestabilním nábytkem	Neexistence pravidelné kontroly vybavení	2	2	2	2	4	Nízké
R011	Kávovar	Zkrat nebo únik vody způsobující škodu	Nezajištěný elektrický přívod	2	2	2	2	4	Nízké
R012	Smlouvy s partnery	Ztráta důležitých smluv	Nedodržení lhůt pro uchovávání dokumentace	2	3	3	5	15	Vysoké
R013	Smlouvy s partnery	Porušení smluvních podmínek třetí stranou	Smlouvy neobsahují doložky o odpovědnosti	2	4	4	5	20	Kritické
R014	Smlouvy s partnery	Neplatné nebo neaktuální smlouvy	Chybějící právní přezkum smluv	2	3	3	5	15	Vysoké
R015	Smlouvy o pojištění	Neplatné nebo neaktuální smlouvy	Neaktuální seznam zákonných povinností	2	2	2	4	8	Střední
R016	Centrální kancelář	Požár nebo záplava	Chybějící havarijní plán	2	4	4	5	20	Kritické
R017	Centrální kancelář	Vniknutí nepovolané osoby	Neexistující politika přístupových práv	2	5	5	4	20	Kritické
R018	Centrální kancelář	Vypadek elektřiny omezující provoz	Absence záložního napájení	3	3	3	4	12	Vysoké
R019	Mobilní telefon koordinátora	Ztráta nebo krádež telefonu s citlivými daty	Chybějící možnost vzdáleného smazání	3	4	4	4	16	Vysoké
R020	Mobilní telefon koordinátora	Nemazaná data při změně zařízení	Neexistence procesu pro výmaz dat při převodu zařízení	2	3	3	3	9	Střední
R021	Účetní software	Ztráta účetních dat kvůli softwarové chybě	Zastaralý software bez záloh	2	4	4	4	16	Vysoké
R022	Účetní software	Neoprávněná manipulace s účetními záznamy	Chybějící logování přístupu	2	3	3	4	12	Vysoké
R023	Dekorace v zasedací místnosti	Překážka evakuačnímu průchodu	Špatné rozmístění nábytku a dekorací	2	2	2	2	4	Nízké
R024	Dekorace v zasedací místnosti	Požár nebo záplava	Používání nevhodných elektrických zařízení	2	3	3	5	15	Vysoké
R025	Dekorace v zasedací místnosti	Požár nebo záplava	Neexistence pravidelné kontroly vybavení	2	2	2	5	10	Střední
R026	Dekorace v zasedací místnosti	Požár nebo záplava	Nezajištěný elektrický přívod	2	2	2	5	10	Střední
R027	Dárcovský webový portál	DDoS útok omezující přístup	Nena konfigurovaná síťová ochrana	3	4	4	4	16	Vysoké
R028	E-mailový server	DDoS útok omezující přístup	Nena konfigurovaná síťová ochrana	3	4	4	4	16	Vysoké
R029	Dárcovský webový portál	Únik platebních informací	Chybějící šifrování datových přenosů	2	4	4	5	20	Kritické
R030	Dárcovský webový portál	Změna obsahu po útoku	Nezabezpečený redakční systém webu	2	4	4	4	16	Vysoké

R031	Bezpečnostní kamery v kanceláři	Selhání záznamového zařízení	Zastaralý hardware bez záloh	2	3	3	9	Sřední
R032	Bezpečnostní kamery v kanceláři	Zneužití záznamů k porušení soukromí	Zneužití přístupových oprávnění	2	4	4	16	Vysoké
R033	Plány evakuace	Zastaralé nebo chybné evakuační plány	Neexistence pravidelné revize plánů	2	3	4	12	Vysoké
R034	Plány evakuace	Nedostupné plány v době incidentu	Fyzické plány nejsou snadno přístupné	2	2	4	8	Sřední
R035	Vnitřní směrnice organizace	Zastaralé interní postupy	Neexistence revizí směrnic	3	3	3	9	Sřední
R036	Vnitřní směrnice organizace	Nedodržování interních předpisů	Slabý dohled nad implementací pravidel	2	2	3	6	Sřední
R037	Dobrovolníci	Zneužití pravomocí dobrovolníkem	Dobrovolníci nemají ověřenou bezúhonnost	2	4	4	16	Vysoké
R038	Dobrovolníci	Nedostatečné zaškolení	Neexistující školicí plán	3	3	4	12	Vysoké
R039	Dobrovolníci	Neprofesionální chování vůči klientovi	Neexistující etický kodex	2	3	4	12	Vysoké
R040	Seznam příjemců pomoci	Únik údajů o příjemcích	Nešifrované uchovávání osobních údajů	3	5	5	25	Kritické
R041	Seznam příjemců pomoci	Ztráta informací kvůli technické chybě	Chybějící záloha	2	4	4	16	Vysoké
R042	Přístupové čipy ke kancelářím	Duplikace přístupového média	Neexistující správa vydaných čipů	2	3	3	9	Sřední
R043	Přístupové čipy ke kancelářím	Ztráta čipu bez zablokování přístupu	Chybějící systém pro deaktivaci přístupu	3	3	3	9	Sřední
R044	Zásoby potravin pro distribuci	Zkažení zásob	Nevhodné skladovací podmínky	2	3	4	12	Vysoké
R045	Zásoby potravin pro distribuci	Krádež potravin ze skladu	Slabé fyzické zabezpečení skladu	2	3	4	12	Vysoké
R046	Zásoby potravin pro distribuci	Nedodání zásilků včas	Chybějící plán logistiky a sledování dodávek	2	3	4	12	Vysoké
R047	Označení místností	Nesrozumitelné značení bránící evakuaci	Nevýrazné značení místností	2	1	3	6	Sřední
R048	Označení místností	Neaktuální označení kanceláří	Nepřehledná evidence rozmístění kanceláří	2	2	2	4	Nízké
R049	Kancelářské potřeby	Nedostatek spotřebního materiálu	Neexistence monitoringu zásob	2	2	2	4	Nízké
R050	Kancelářské potřeby	Zpoždění dodávky při potřebě	Chybějící smlouvy s dodavateli	2	2	2	4	Nízké
R051	Zálohovací disk serveru	Selhání zálohovacího procesu	Zálohování není pravidelně testováno	2	3	4	12	Vysoké
R052	Zálohovací disk serveru	Poškození nebo ztráta disku	Nechráněné fyzické umístění disku	2	3	4	12	Vysoké
R053	Databáze zaměstnanců	Ztráta informací o pracovnících	Chybějící záloha	2	4	4	16	Vysoké
R054	Databáze zaměstnanců	Neautorizovaný přístup k osobním údajům	Chybějící řízení oprávnění	3	4	4	16	Vysoké
R055	Webové stránky organizace	Hacknutí webu a zveřejnění nevhodného obsahu	Nezabezpečená administrace webu	3	4	4	16	Vysoké
R056	Webové stránky organizace	Výpadek webu	Nedostatek serverových prostředků	3	3	3	9	Sřední
R057	Zdravotní dokumentace klientů	Zveřejnění zdravotních záznamů	Zneužití přístupových oprávnění	2	4	5	20	Kritické
R058	Zdravotní dokumentace klientů	Ztráta nebo smazání lékařských údajů	Chybějící záloha	2	4	5	20	Kritické
R059	Léky pro humanitární zásahy	Nevhodné skladování ovlivňující účinnost	Chybějící kontrola teploty	2	4	5	20	Kritické
R060	Léky pro humanitární zásahy	Ztráta zásilků během přepravy	Nestedovaná logistika	2	3	5	15	Vysoké

R061	Finanční rezerva	Zneužití prostředků	Chybějící vnitřní finanční kontrola	2	4	4	5	20	Kritické
R062	Finanční rezerva	Nevhodné investování rezervy	Neexistence investičních pravidel	2	3	3	5	15	Vysoké
R063	Přenosné stany a přístřešky	Poškození materiálu v důsledku počasí	Nevhodné skladovací podmínky	2	3	3	3	9	Střední
R064	Přenosné stany a přístřešky	Nesprávné uskladnění	Neexistence kontrolního systému skladu	2	3	3	3	9	Střední
R065	Router a síťová infrastruktura	Neautorizovaný přístup do sítě	Router bez nastaveného firewallu	3	4	4	4	16	Vysoké
R066	Router a síťová infrastruktura	Přetřetí sítě vlivem útoku	Chybějící síťové monitorování	3	3	3	4	12	Vysoké
R067	Náhradní periferie	Nepoužitelnost zařízení při potřebě	Nepřávidelná kontrola funkčnosti zařízení	2	2	2	2	4	Nízké
R068	Náhradní periferie	Poškození bez zálohy	Neexistence náhradních komponent	2	3	3	3	9	Střední
R069	Seznam kontaktů na krizové složky	Zastaralé nebo chybné kontakty	Neexistence aktualizací procesu kontaktů	2	2	2	2	4	Nízké
R070	Seznam kontaktů na krizové složky	Nedostupnost seznamu během incidentu	Papírová forma není dostupná elektronicky	2	2	2	3	6	Střední
R071	Přístupové údaje k bankovnímu účtu	Přístup třetí strany k účtu	Sdílené přihlašovací údaje	2	4	4	5	20	Kritické
R072	Přístupové údaje k bankovnímu účtu	Zneužití přihlašovacích údajů	Uložení hesel v otevřeném formátu	2	4	4	5	20	Kritické
R073	Interní školící materiály	Zastaralý obsah	Školící materiály nejsou revidovány	2	2	2	3	6	Střední
R074	Interní školící materiály	Neautorizovaná změna školících dokumentů	Neexistence řízení verzí dokumentů	2	2	2	3	6	Střední
R075	Zápisy z porad	Poškození nebo ztráta dat	Chybějící záloha	2	4	4	4	16	Vysoké
R076	Zápisy z porad	Neautorizovaný přístup k citlivým dokumentům	Chybějící přístupová kontrola k zápisům	3	2	3	4	12	Vysoké
R077	Regulérní zaměstnanci	Nedodržení pracovních povinností	Chybějící kontrolní mechanismy výkonu	2	3	3	5	15	Vysoké
R078	Regulérní zaměstnanci	Etické pochybení	Neexistující etický kodex	2	3	3	5	15	Vysoké
R079	Záznamy o školení zaměstnanců	Ztráta záznamu ovlivňující audit	Chybějící záloha	2	4	4	3	12	Vysoké
R080	Záznamy o školení zaměstnanců	Nesprávná evidence absolvovaných školení	Chybné zaznamenávání dat do systému	2	2	2	3	6	Střední
R081	Stany pro krizové ubytování	Nedostatečné vybavení během nasazení	Nevytvořený kontrolní seznam vybavení	2	3	3	4	12	Vysoké
R082	Stany pro krizové ubytování	Poškození stanů kvůli nesprávnému skladování	Sklad bez regulace teploty a vlhkosti	2	3	3	4	12	Vysoké
R083	Zásoby vody	Kontaminace vody	Nevhodné skladovací podmínky	2	3	3	4	12	Vysoké
R084	Zásoby vody	Nedostatek v době potřeby	Chybějící sledování zásob vody	2	2	2	4	8	Střední
R085	Loga a grafické podklady	Zneužití loga třetí stranou	Loga nejsou chráněna autorským právem	2	2	2	3	6	Střední
R086	Loga a grafické podklady	Zveřejnění nevhodného grafického obsahu	Chybějící kontrola nad publikacemi	2	2	2	3	6	Střední

PŘÍLOHA P XIV: UKÁZKA DASBOARDU

DASHBOARD

Přidání záznamu

AKTIVA		
Název	Kategória	Kritičnosť

Zapsat aktivum

HROZBY			
Název	Kategorie	Četnost výskytu	Dopad

Zapsat hrozbu

ZRANITELNOSTI	
Název	Mira zranitelnosti

Zapsat zranitelnost

PŘIDÁNÍ RIZIKA		
Název aktiva	Název hrozby	Název zranitelnosti

apsat propoiení

Přehled rizik

Bez opatření



8	23	39	16
Nízké	Sřední	Vysoké	Kritické

Po zavedení opatření



6	9	1	0
Nízké	Střední	Vysoké	Kritické

Přehled opatření



20	20	2	16
Navržené	Vřešín	Odmítnuté	Dokončené

ZAVEDENÍ OPATŘENÍ

Riziko	Název opatření	Odpovědnosti	Termín realizace
	Osoba/rola, která opatření realizuje	(R) →	
	Osoba/rola, která za výsledek odpovídá	(A) →	
	Konzultant, specialista	(C) →	
	Kdo má být informován	(I) →	

Zapsat opatření

Možnost aktualizace rizik po přidání opatření

řegenerovat rizika z dokončených opatření

5 Opatření po splatnosti: Zavedení bezpečnostních směrnic a školení
Zavedení plánu logistiky, proškolení zaměstnanců
Zavedení zálohování a pravidelné zálohování
Zabezpečení sítě
Zabezpečení sítě