
ANALÝZA RIZÍK ZÁKLADY



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU
UNIVERZITA SLOVENSKEJ
AKADÉMIE VIED A UMBRAN

OBSAH

1. Základné pojmy a definície
2. Právny a normatívny rámec
3. Proces riadenia bezpečnostných rizík
4. Krok 1: Vytváranie súvislostí (Určovanie kontextu)
5. Krok 2: Posudzovanie rizika (Identifikácia, Analýza, Hodnotenie)
6. Krok 3: Ošetrovanie rizík
7. Krok 4: Akceptácia zvyškového rizika
8. Krok 5: Komunikácia a monitorovanie
9. Praktické aspekty a úloha zamestnanca
10. Dôsledky chýbajúcej analýzy rizík
11. Záver a zhrnutie

MANAŽMENT RIZÍK ZÁKLADY



PLÁN [OBNOVY]



Pojem „Riziko“ v historickom kontexte



Rizq vychádza z **arabčiny** a týka všetkého, čo Alah (Boh) poskytuje Svojim stvoreniam. Zahŕňa nielen **materiálne** veci ako **jedlo, peniaze a prístrešie**, ale aj **nemateriálne hodnoty** ako **zdravie, vedomosti, mier a šťastie** priaznivý výsledok

V uzbečtine je to doteraz slovo pre obživu

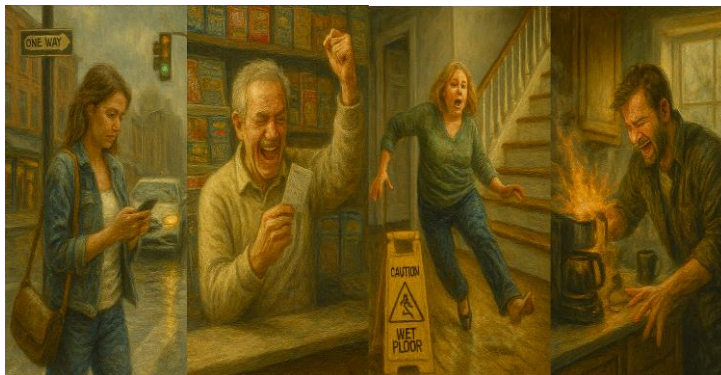
Vo francúzštine risk znamená odvážnosť - čo je priaznivý

Latinsky riscum je spojené s lodnou dopravou a útesmi - nepriaznivými udalosťami a odvahou podstúpiť nebezpečenstvo námorníkov pri plavbách

Dnes prevláda chápanie rizika ako určitého **nebezpečenstva** alebo **možnosti vzniku straty**.

„Riziko“ v bežnom živote

- Bežné životné situácie
- Vnímanie rizika
- Reakcia na riziko



Každý v živote vedome a častokrát podvedome myslí a riadi sa rizikovo. Ráno odchádzame do práce pozrieme na predpoveď počasia alebo von oknom.

S rizika sa stretávame v bežnom živote, sme s nimi oboznamovaní aj v práci napríklad formou BOZP.

Vnímame riziká častokrát podvedome a taktiež tieto riziká podvedome riadime. Niektoré vnímame vedome a vieme s nimi pracovať, vieme sa vedome rozhodovať ako sa s nimi vysporiadame.

Podvedomá reakcia na riziko > častokrát jednoduchá reakcia – strach, únik, útok.

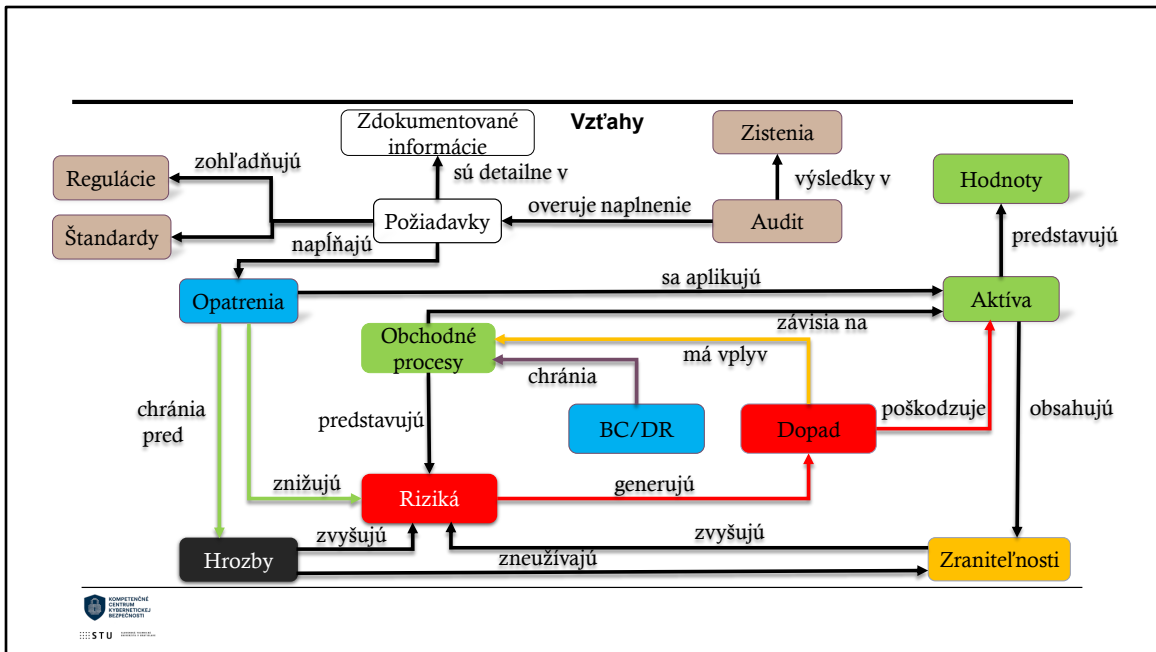
Modelová situácia 1

	Aktívum	Hrozba	Zraniteľnosť	Opatrenie	Riziko
Diery v dáždniku					
Dážď					
Dáždnik					
Búrkové mraky					
Žena					



KLÚČOVÉ POJMY PRE RIADENIE RIZÍK

- **Aktívum (Asset):** Všetko, čo má pre organizáciu definovateľnú hodnotu. Môže byť hmotné (servery, budovy) aj nehmotné (dáta, reputácia, know-how).
- **Hrozba (Threat):** Potenciálna udalosť, ktorá môže poškodiť aktívum. Môže byť spôsobená úmyselne alebo náhodne.
- **Zraniteľnosť (Vulnerability):** Slabé miesto v systéme ochrany, ktoré môže hrozba zneužiť.
- **Dopad (Impact):** Miera alebo výška škody, ktorá nastane, ak hrozba využije zraniteľnosť.
- **Pravdepodobnosť (Likelihood):** Hodnota vyčísľujúca istotu resp. neistotu výskytu určitej udalosti.
- **Riziko (Risk):** Vplyv neistoty na ciele. Je to hodnota vyjadrujúca vzťah medzi pravdepodobnosťou, toho že hrozba zneužije zraniteľnosť, a dopadom, ktorý tým spôsobí.



Modelová situácia 1

	Aktívum	Hrozba	Zraniteľnosť	Opatrenie	Riziko
Diery v dáždniku			x		
Dážď					x
Dáždnik	x			x	
Búrkové mraky		x			
Žena	x				

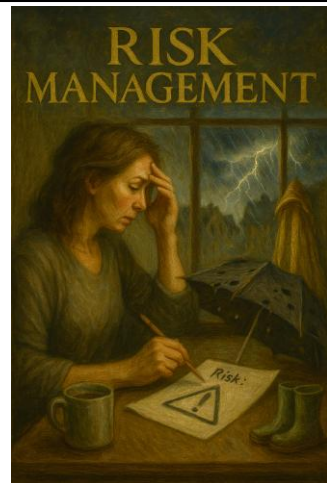


CIELE MANAŽMENTU RIZÍK

1. Znížiť pravdepodobnosť výskytu nežiaducich udalostí
2. Zmierniť dopad, ak sa riziko naplní
3. Zabezpečiť kontinuitu činností a ochranu majetku
4. Zvýšiť bezpečnosť a dôveru
5. Podporiť informované rozhodovanie
6. Využiť príležitosti

Tri kľúčové otázky:

- **Čo chceme chrániť?**
- **Pred kým a pred čím chrániť?**
- **Ako chrániť?**



1. (napr. nehody, finančné straty, technické poruchy)
2. (napr. pripraviť krízový plán, poistenie, záložné systémy)
3. -
4. u občanov, zamestnancov, klientov či obchodných partnerov
5. na základe analýzy rizík
6. niektoré riziká môžu priniesť aj pozitívne efekty, ak sú správne riadené

Proces manažmentu rizík sa zaoberá troma základnými otázkami

ČO sa môže pokaziť?

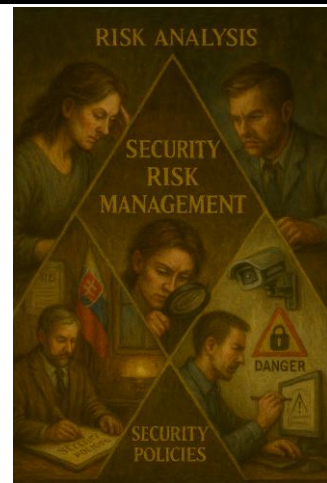
Ako sa to môže pokaziť?

ČO S TÝM UROBÍM?

ZÁKLADNÉ PILIERE RIADENIA RIZÍK

Riadenie bezpečnostných rizík, ak má plniť svoju funkciu, musí zahŕňať nasledujúce činnosti:

1. **Analýza bezpečnostných rizík**
2. **Tvorba a prijatie bezpečnostnej koncepcie a politiky**
3. **Vytvorenie a riadenie bezpečnostného systému**



1. Proces zdokumentovania aktív, identifikácie hrozieb, hodnotenia rizík a návrh opatrení
2. Spôsob akým sa riadia riziká, popisy procesov, kompetencii, zodpovedností, ale aj trend a ciele v oblasti bezpečnosti
3. Systém, ktorý pozostáva z viacerých úrovní riadenia rizík – organizačná, personálna a technická úroveň

MATEMATICKÉ VYJADRENIE RIZIKA

$$R=P \times D$$

Kde:

- **R** = Riziko (Risk)
- **P** = Pravdepodobnosť (Probability) vzniku udalosti
- **D** = Dopad (Damage), resp. následky udalosti

Tento vzťah pomáha určiť závažnosť rizík a stanoviť priority.



Je to hodnota vyjadrujúca vzťah medzi pravdepodobnosťou, a dopadom

Existujú rozšírené výpočty rizika ktoré zahŕňajú:

1. hodnotu aktíva, zraniteľnosť a hrozbu
2. pravdepodobnosť hrozby, expozícia zraniteľnosti a hodnota aktíva

TZV. „CIA TRIÁDA“ – CIELE BEZPEČNOSTI

Atribúty/vlastnosti aktív, ktoré sa snažíme chrániť

Dôvernosť (confidentiality)

aktívum je prístupné len autorizovaným osobám.

Integrita (integrity)

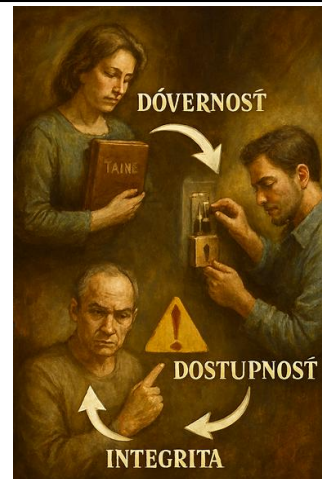
aktívum nebolo neautorizovane zmenené.

Dostupnosť (availability)

aktívum je dostupné vtedy, keď je potrebné,

Vzťahy:

- Dôvernosť bez dostupnosti je neúčinná
- Integrita bez dôvernosti je zraniteľná
- Dostupnosť bez integrity môže byť nebezpečná



PRÁVNY A NORMATÍVNY RÁMEC

Manažment rizík sa opera najmä o nasledovné predpisy a normy:

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti
- Vyhláška č 227/2025 Z. z. (obsah bezpečnostných opatrení)
- Zákon č. 95/2019 Z. z. o IT vo verejnej správe
- Vyhláška č. 179/2020 Z. z. (kategorizácia a bezpečnostné opatrenia ITVS)

Iné normy a bezpečnostné rámce

- **ISO/IEC 27001:2022** (Systémy manažérstva informačnej bezpečnosti)
- **ISO/IEC 27005:2022** (Riadenie rizík informačnej bezpečnosti)
- **ISO 31000:2018** (Manažerstvo rizika – Návod)
- **ENISA** (Interoperabilný rámec riadenia rizík EÚ)
- **EBA** (DORA a RTS pre manažment rizík)
- **NIST SP 800-30 a 800-39** (Managing Information Security Risk)



Modelová situácia 2

	Aktívum	Hrozba	Zraniteľnosť	Opatrenie	Riziko
Krádež údajom					
Údaje					
Hacker					
Školenie					
Neznalosť					



PROCES RIADENIA RIZÍK

Požiadavky na proces

- Systematickosť
- Kontinuita
- Aktuálnosť údajov

Proces sa skladá z dvoch hlavných častí:

1. **Analýza rizík:** Vytvára podklady na vyhodnotenie rizík.
2. **Riadenie (ošetrovanie) rizík:** Minimalizuje potenciálne dopady identifikovaných rizík



1. analýza identifikuje, analyzuje a hodnotí potenciálne riziká súvisiace s hrozbami, aktívami a ich zraniteľnosťami pri posúdení pravdepodobností Môže byť **vysokoúrovňová** na IT procesy, služby ale aj **technická** zameraná na technológie, IS, aplikácie. Úroveň pohľadu na to čo ideme analyzovať je závislá na konkrétnych požiadavkách organizácie.

2 Riadenie rizík znamená **návrh a schválenie** ďalších **činností** čo je potrebné **vykonať** s identifikovanými rizikami aby bola organizácia chránená pred aktuálnymi hrozbami. Taktiež tam patrí **monitorovanie efektivity** a **prehodnocovanie** rizík

PROCES RIADENIA RIZÍK PODĽA ISO 31000

Proces zahŕňa:

1. **Vytvorenie súvislostí**
2. **Posudzovanie rizika**
3. **Zaobchádzanie s rizikom**
4. **Komunikáciu a konzultácie:**
Prebiehajú počas celého procesu
5. **Monitorovanie a preskúvanie:**
Zabezpečuje kontrolu a efektívnosť opatrení

Tento proces je cyklický a neustále sa opakuje.



Proces sa skladá z viacerých na seba nadväzujúcich činností, ktoré v čase sú cyklické.

1. Zahŕňa určenie kontextu, rozsahu, kritéria a spôsob posúdenia rizík.
2. Identifikácia rizík na základe aktív a existencie hrozieb ktoré na ne pôsobia.
Určenie pravdepodobnosti.
3. Stanovuje čo s identifikovaným rizikom urobíme.
4. Pochopenie rizika zainteresovanými stranami, reportovanie vlastníkom aktív, stanovenie vlastníkov rizík ale aj konzultácie pri analýze a návrhu opatrení.
5. Zabezpečuje posúdenie aktuálnosti rizika, stav hrozieb, zraniteľností a efektivity implementovaných opatrení.

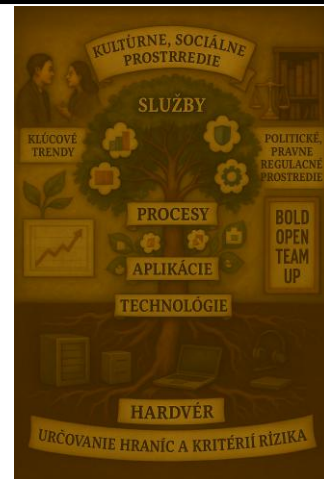
Modelová situácia 2

	Aktívum	Hrozba	Zraniteľnosť	Opatrenie	Riziko
Krádež údajom					x
Údaje	x				
Hacker		x			
Školenie				x	
Neznalosť			x		



VYTVÁRANIE SÚVISLOSTÍ (URČOVANIE KONTEXTU)

- **Externé súvislosti:** Faktory mimo organizácie:
 - Sociálne, politické, právne a regulačné prostredie
 - Kľúčové trendy ovplyvňujúce ciele organizácie
 - Vzťahy a vnímanie externých zainteresovaných strán
- **Interné súvislosti:** Faktory vo vnútri organizácie
 - Riadenie, stratégia, politiky
 - Kultúra organizácie, hodnoty,
- **Hranice analýzy**
 - Aktíva, hranice dôvery, vzťahy medzi aktívami, vlastníci aktív
- **Kritériá rizika**
 - Úroveň rizík, risk apetít, stratégia riadenia rizík



Imidž, meno firmy, veľkosť firmy, oblasť/**sektor** pôsobenia – ma vplyv na to aké zákony a regulácie budú zohľadňované

Posúdenie poskytovaných služieb na trhu a **konkurencia**, trendy využívania **centralizovaných** technológií na trhu cloudové služby a novinky

Plnenie **zmluvných** dojednaní s dodávateľmi a zákazníkmi, závislosť na dodávateľoch, komplexnosť služieb

Organizačná štruktúra, kompetencie jednotlivých oddelení a rolí

Vzťahy medzi zamestnancami, zodpovednosti a povinnosti, priority a dôraz v organizácii (či je to korporát, rodinná firma, medzinárodná firma, startup a pod.)

Kritické aktíva, podporné aktíva, dekompozícia IS, technológií a určenie pohľadu na aktíva **Rasmussenovou** hierarchiou komponentov >> detail vnímania aktív

POSUDZOVANIE RIZÍK (RISK ASSESSMENT)

Posudzovanie rizika je celkový proces, ktorý zahŕňa:

1. **Identifikáciu rizík:** Čo sa môže stať a prečo?
2. **Analýzu rizík:** Aké sú dopady a aká je pravdepodobnosť?
3. **Hodnotenie rizík:** Je úroveň rizika prijateľná, alebo si vyžaduje ošetrovanie?



Identifikácia rizík definuje na hrozby, zraniteľnosti, scenáre rizík súvisiace s konkrétnymi aktívami (IS, procesy, služby, organizácia a pod.)

Analýza rizík určuje – priraduje riziku cez **scenár konkrétny dopad** podľa stanovených úrovni a definovanú pravdepodobnosť výskytu hrozby.

Hodnotenie rizík - **úroveň** identifikovaných rizík na základe definovaných **výpočtov** a stanovených pravidiel,

KROK 1 - IDENTIFIKÁCIA RIZÍK

Cieľ: Vytvoriť zoznam potenciálnych rizík, ktoré môžu ovplyvniť ciele organizácie.

Základná zásada:

Riziká, ktoré nie sú identifikované, nemôžu byť riadené.

Proces zahŕňa:

- Identifikáciu hrozieb a zraniteľností.
- Identifikáciu existujúcich bezpečnostných opatrení.
- Identifikáciu možných následkov (dopadov).
- Vytvorenie **zoznamu rizík** (katalóg, register).



ČO NÁM HROZÍ

Na identifikáciu je potrebné mať **zoznam aktív** a určiť **agentov hrozieb** a **hrozby** ktoré môžu pôsobiť na aktíva

Z predchádzajúcej činnosti Určovanie kontextu máme Hlavné aktíva Podporné aktíva

Agent hrozby – (motivácia, znalosti, peniaze, zdroje) insider, hacker, konkurenčná firma, štát, vandal, zlodej, špión, dodávateľ, nahnevaný, neznalý zamestnanec

Zoznamy agentov hrozieb – Intel , zoznam hrozieb – napr. NBU

Zoznam zraniteľností – ktoré poznáme, skenujeme IS,

Posúdenie dopadov – biznis analytici, bezpečnostní analytici, prevádzka, biznis vlastníci, finančné oddelenie, právne oddelenie, obstarávanie

Modelová situácia 3

Aktívum/Agent hrozby	Hacker	Insider	Dodávateľ	Konkurenčná firma	Zlodej
Sieťový router					
Notebook					
Zdrojový kód					
WEB aplikácia					
Know-how					

Agent hrozby > Aktívum



KROK 2 - ANALÝZA RIZIKA

Cieľ: Určiť **pravdepodobnosť** a **dopady** pre identifikované riziká, a tým stanoviť ich úroveň.

Prečo je dôležitá? Bez analýzy by organizácia:

- Nevedela, čo má chrániť ako prvé.
- Nevybrala správnu úroveň bezpečnosti.
- Nemohla overiť, či sú opatrenia dostatočné.

Je to manažérsky nástroj, ktorý šetrí peniaze a zvyšuje dôveru.



KROK 3 - HODNOTENIE RIZIKA

Ciel: Pomôcť pri rozhodovaní o tom, ktoré riziká vyžadujú ošetrovanie a akú majú prioritu.

Proces zahŕňa:

- **Porovnanie** úrovne rizika (zistenej počas analýzy) s vopred definovanými **kritériami rizika**.
- **Rozhodnutie**, či je riziko prijateľné (akceptovateľné) alebo neprijateľné (neakceptovateľné) a vyžaduje ošetrovanie.
- **Určenie priorít** pre ošetrovanie rizík.

DOPAD	Zaned
Pravdepodobnosť VYSKYTU (frekvencia)	
Zriedkavá	1
Občasná	2
Priemerná	3
Častá	4
Veľmi častá	5



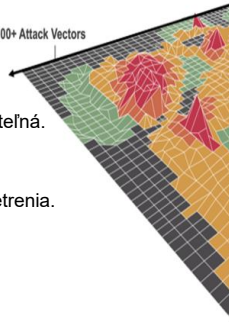
KROK 4 - OŠETRENIE RIZÍK

Ciel: Proces modifikácie rizika.

Ide o opakujúci sa proces:

1. Posúdenie možností ošetrovania.
2. Rozhodnutie, či je zvyšková úroveň rizika prijateľná.
3. Ak nie je, návrh nového ošetrovania.
4. Posúdenie efektívnosti implementovaného ošetrovania.

100+ Attack Vectors



Modelová situácia 3

Aktívum/Agent hrozby	Hacker	Insider	Dodávateľ	Konkurenčná firma	Zlodej
Sieťový router		x			
Notebook					x
Zdrojový kód			x		
WEB aplikácia	x				
Know-how				x	



Agent hrozby > Aktívum

STRATÉGIA A MOŽNOSTI OŠETRENIA RIZIKA

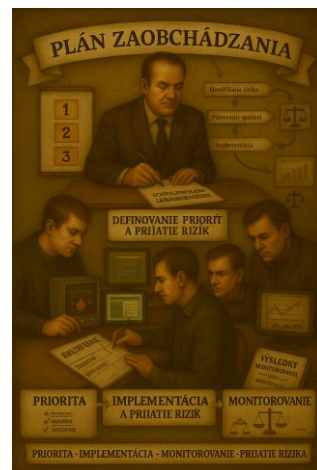
Existujú štyri základné stratégie zaobchádzania s rizikom:

- 1. Vyvarovanie sa riziku (Avoid):** Rozhodnutie nezačať alebo nepokračovať v činnosti, ktorá riziko vytvára.
- 2. Zníženie rizika (Reduce/Mitigate):** Zavedenie opatrení na zníženie pravdepodobnosti alebo dopadu. Toto je najčastejšia stratégia.
- 3. Prenos rizika (Transfer/Share):** Zdieľanie rizika s inou stranou (napr. cez poistenie, outsourcing).
- 4. Zachovanie rizika (Retain/Accept):** Vedomé akceptovanie rizika bez zavedenia opatrení (zvyčajne pri nízkych rizikách).



PLÁN ZAOBCHÁDZANIA S RIZIKOM

- Kritickou fázou je výber optimálneho spôsobu ošetrovania.
- **Plán zaobchádzania s rizikom** špecifikuje, ako budú zvolené možnosti implementované.
- Musí jasne definovať **priority**, v akom poradí sa budú opatrenia zavádzať.
- Je potrebné monitorovať, či zavedené opatrenia nevyvolali nové riziká.



Modelová situácia 4

	Aktívum	Hrozba	Zraniteľnosť	Opatrenie	Riziko
Zamestnanec					
Nepozornosť					
Kontrola príjemcu pred odoslaním					
Osobné údaje					
Únik osobných údajov					



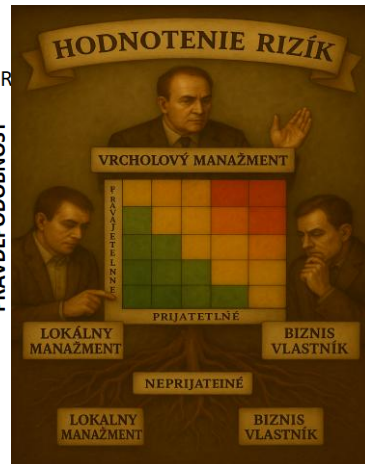
AKCEPTÁCIA ZVYŠKOVÉHO RIZIKA

- **Zvyškové (reziduálne) riziko:** Riziko, ktoré zostáva aj po aplikovaní všetkých opatrení.
- Ak je hodnota tohto rizika dostatočne nízka, organizácia ho môže považovať za prijateľné.
- **Akceptácia rizika** je formálny proces, v ktorom manažment (štatutárny orgán) odsúhlasí eskalované zvyškové riziko.
- Toto rozhodnutie musí byť formálne zaznamenané.

- Pozornosť vrcholového manažmentu
- Pozornosť lokálneho manažmetu
- Bez akcie

TEOR

PRAVDEPODOBNOŠŤ



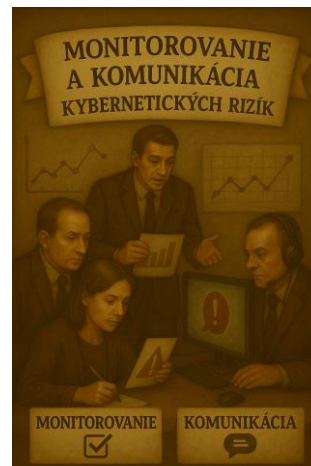
KOMUNIKÁCIA A MONITOROVANIE

Komunikácia rizika:

- Výmena informácií o rizikách medzi kompetetnými a zainteresovanými stranami.
- Informácie zahŕňajú povahu, pravdepodobnosť, závažnosť a spôsob ošetrenia rizík.
- Cieľom je podporiť zodpovednosť a vlastníctvo rizika.

Monitorovanie a preskúvanie:

- Kontinuálny proces, ktorý preveruje efektivitu prijatých opatrení.
- Sleduje, či sa akceptovateľné riziká nestali neakceptovateľnými.



Modelová situácia 4

	Aktívum	Hrozba	Zraniteľnosť	Opatrenie	Riziko
Zamestnanec		x			
Nepozornosť			x		
Kontrola príjemcu pred odoslaním				x	
Osobné údaje	x				
Únik osobných údajov					x



DOKUMENTOVANIE A VYKAZOVANIE

Zaznamenávanie a hlásenie

- Poskytovať informácie pre rozhodovanie.
- Zlepšovať aktivity riadenia rizík.
- Pomáhať pri interakcii so zainteresovanými stranami vrátane tých, ktorí majú zodpovednosť za aktivity riadenia rizík.
- Komunikovať aktivity a výsledky riadenia rizík v celej organizácii



PRAKTICKÉ ASPEKTY A ÚLOHA ZAMESTNANCA

Kto sa zapája do analýzy rizík?

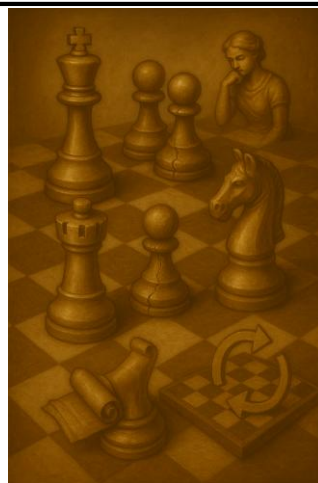
- **CISO alebo MKB:** Definuje metodiku
- **Bezpečnostní a IT špecialisti:** Vykonávajú analýzu rizík.
- **Vedúci oddelení a vlastníci aktív:** Poznajú hodnotu informácií a procesov.
- **Bežní zamestnanci:** Vedia, kde vznikajú reálne riziká v praxi.

Bez spolupráce všetkých nie je analýza rizík úplná.



ÚLOHA

Činnosť	Popis	Poradie
Vyhodnotenie rizík	Vypočítať mieru rizika (Pravdepodobnosť × Dopad)	
Pravidelná aktualizácia	Analýza rizík nie je jednorazová činnosť	
Identifikácia hrozieb a zraniteľností	Čo môže aktívum ohroziť a kde sú jeho slabiny?	
Identifikácia aktív	Zistiť, čo chceme chrániť	
Návrh opatrení	Rozhodnúť, ako budeme s rizikom zaobchádzať	
Určenie hodnoty aktív	Aký by bol dopad ich straty, zneužitia či nedostupnosti?	
Dokumentácia	Zaznamenať celý proces, výsledky a plánované opatrenia.	

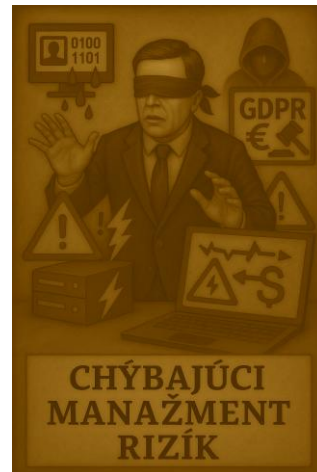


Návrh poradie jednotlivých činností v rámci manažmentu rizík.

- 1. Identifikácia aktív:** Zistiť, čo chceme chrániť.
- 2. Určenie hodnoty aktív:** Aký by bol dopad ich straty, zneužitia či nedostupnosti?
- 3. Identifikácia hrozieb a zraniteľností:** Čo môže aktívum ohroziť a kde sú jeho slabiny?
- 4. Vyhodnotenie rizík:** Vypočítať mieru rizika (Pravdepodobnosť × Dopad).
- 5. Návrh opatrení:** Rozhodnúť, ako budeme s rizikom zaobchádzať.
- 6. Dokumentácia:** Zaznamenať celý proces, výsledky a plánované opatrenia.
- 7. Pravidelná aktualizácia:** Analýza rizík nie je jednorazová činnosť.

DÔSLEDKY CHÝBAJÚCEHO MANAŽMENTU RIZÍK

1. **Nevie, čo je ohrozené a ako vážne:** Chráni nesprávne veci alebo nedostatočne. Investície do bezpečnosti sú neefektívne.
2. **Bezpečnostné rozhodnutia nie sú podložené:** Opatrenia sú len formálne alebo založené na pocitoch.
3. **Nie je pripravená na incidenty:** V prípade útoku alebo výpadku je reakcia chaotická a pomalá.
4. **Hrozí porušenie legislatívnych povinností:** Mnohé predpisy (Zákon o kybernetickej bezpečnosti, GDPR, ISO 27001) analýzu rizík priamo vyžadujú. Hrozia vysoké pokuty.
5. **Vysoká pravdepodobnosť incidentov s veľkým dopadom:** Úniky dát, finančné straty, poškodenie reputácie.



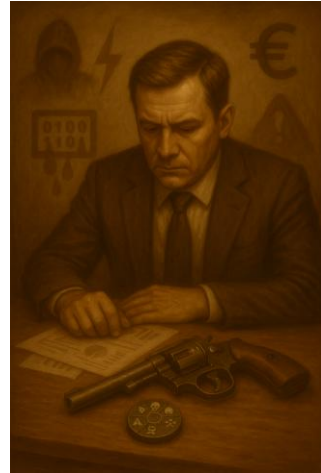
KLÚČOVÉ POSOLSTVO

Riadenie bezpečnostných rizík je **klúčovým nástrojom** pre systematické riadenie bezpečnosti.

Nie je to len povinnosť podľa zákona, ale **zdravý manažérsky nástroj**, ktorý:

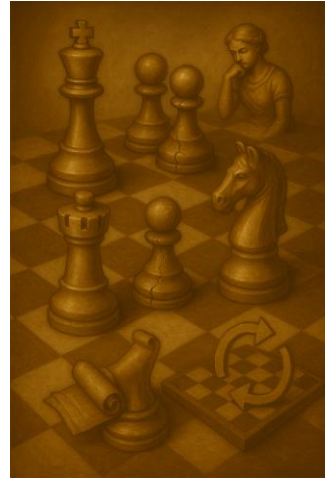
- Znižuje pravdepodobnosť problémov.
- Šetrí finančné prostriedky.
- Zvyšuje dôveru u občanov, zákazníkov, partnerov aj zamestnancov.

Je to **kontinuálny proces**, ktorý chráni organizáciu pred predvídateľnými aj nepredvídateľnými hrozbami.



ĎAKUJEM ZA POZORNOSŤ

Otázky a odpovede



- | | |
|--------------------------------------|---------------------------|
| 1 Kráľ | aktívum (to, čo chránime) |
| 2 Kráľ na podstavci / zvýraznený | hodnota aktíva |
| 3 Pešiak s prasklinou v podstave | zraniteľnosti & hrozby |
| 4 Dáma premýšľajúca nad šachovnicou | výpočet rizika |
| 5 Jazdec v pohybe | návrh opatrení |
| 6 Veža s pergamenom | dokumentácia |
| 7 Šachová doska otáčajúca sa v cykle | pravidelná aktualizácia |