Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Riadenie aktív, identifikácia hrozieb a riadenie rizík

Anton Horváth, Pavol Dovičovič

24. apríl 2025

RIADENIE AKTÍV A RIADENIE RIZÍK

Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti musí zabezpečiť ochranu aktív podľa ich hodnoty.

§ 6 ods. 1 vyhlášky NBÚ č. 362/2018 Z. z.

Riadenie aktív

RIADENIE IT AKTÍV

IT Aktívum – akýkoľvek finančne hodnotný komponent, ktorý sa podieľa na dodávke produktov, alebo služieb

- Aktíva (angl. Assets) - hmotné alebo nehmotné ekonomické prostriedky, ktoré pre organizáciu priamo alebo nepriamo predstavujú súčasnú, alebo potenciálnu hodnotu. (aktívami sú napr.: procesy, dáta, informácie, software, služby, objekty a priestory organizácie)
- Účelom praktiky **Riadenie IT aktív** (IT Asset management) je plánovať a riadiť celý životný cyklus IT aktív tak, aby pomáhala organizácii
  - Maximalizovať hodnotu
  - Riadiť náklady
  - Riadiť riziká
  - Podporovať rozhodovanie ohľadne nákupu, opakovaného využitia, vyradenia a likvidácie IT aktív
  - Dodržiavať regulatórne a zmluvné požiadavky
- Účelom praktiky **riadenia konfigurácií** služby je zaistiť, že sú k dispozícii aktuálne informácie o konfigurácii IT služieb vrátane konfiguračných položiek, z ktorých je služba vyskladaná.

Podľa ITIL®4 best practice – Copyright AXELOS Limited 2019

ROZDELENIE AKTÍV

PRIMÁRNE AKTÍVA

PROCESY / SLUŽBY

INFORMÁCIE / DÁTA

PODPORNÉ AKTÍVA

Technológie
(HW, SW, siete)

Ľudia
(interní, externí)

Lokality

Tretie strany
(dodávateľ/odberateľ)

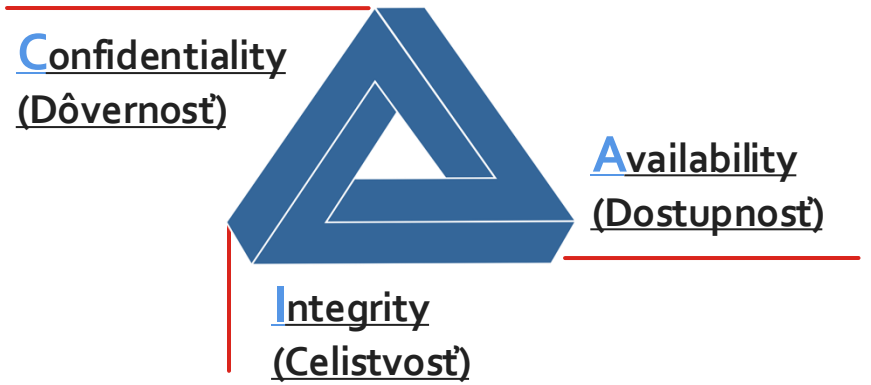
POŽIADAVKY NA RIADENIE AKTÍV

- identifikácia a evidencia
- centralizované riadenie a aktualizácia
- vlastníctvo a zodpovednosti
- klasifikácia informácií
- postupy práce s aktívami
- **ochrana aktív**



KLASIFIKÁCIA INFORMAČNÝCH AKTÍV

- **Aká je úloha klasifikácie pri ochrane informačných aktív?**
  - Koncový používateľ informácie typicky nemá predstavu o hodnote a citlivosti informácie s ktorou pracuje
  - Používateľ nepozná pravidlá ako s informáciou nakladať:
    - čo musí vykonať, aby informáciu ochránil
    - čo s informáciou nesmie robiť, aby ju neohrozil
- **Informačné aktíva sú klasifikované podľa atribútov:**
  - Dôvernosť (Confidentiality)
  - Celistvosť (Integrity)
  - Dostupnosť (Availability)
- Cieľom klasifikácie je vhodne uplatniť odlišné bezpečnostné mechanizmy pre informácie s odlišnou hodnotou pre jednotlivé atribúty

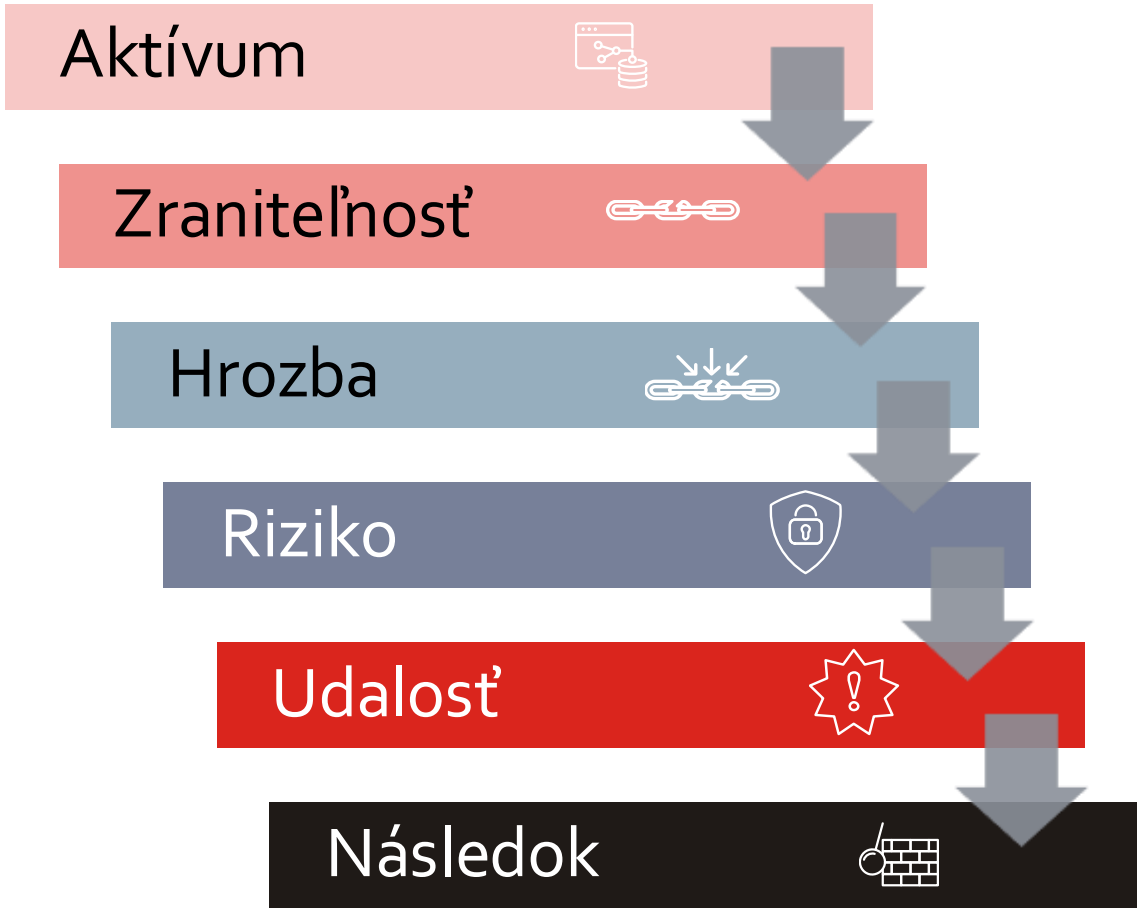


Riadenie rizík

METODICKÝ RÁMEC

- **STN ISO/IEC 27005:2023** Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Usmernenie k riadeniu rizík informačnej bezpečnosti
- **NIST Special Publication 800-30 Rev. 1** Guide for Conducting Risk Assessments
- **NIST Special Publication 800-39** Managing Information Security Risk
- **STN ISO 31000** Manažérstvo Rizika – návod
- Metodika analýzy rizík kybernetickej bezpečnosti (NBÚ)
- Metodika analýzy bezpečnosti pre bezpečnostné projekty ISVS (MIRRI)

RIADENIE RIZÍK – POJMY



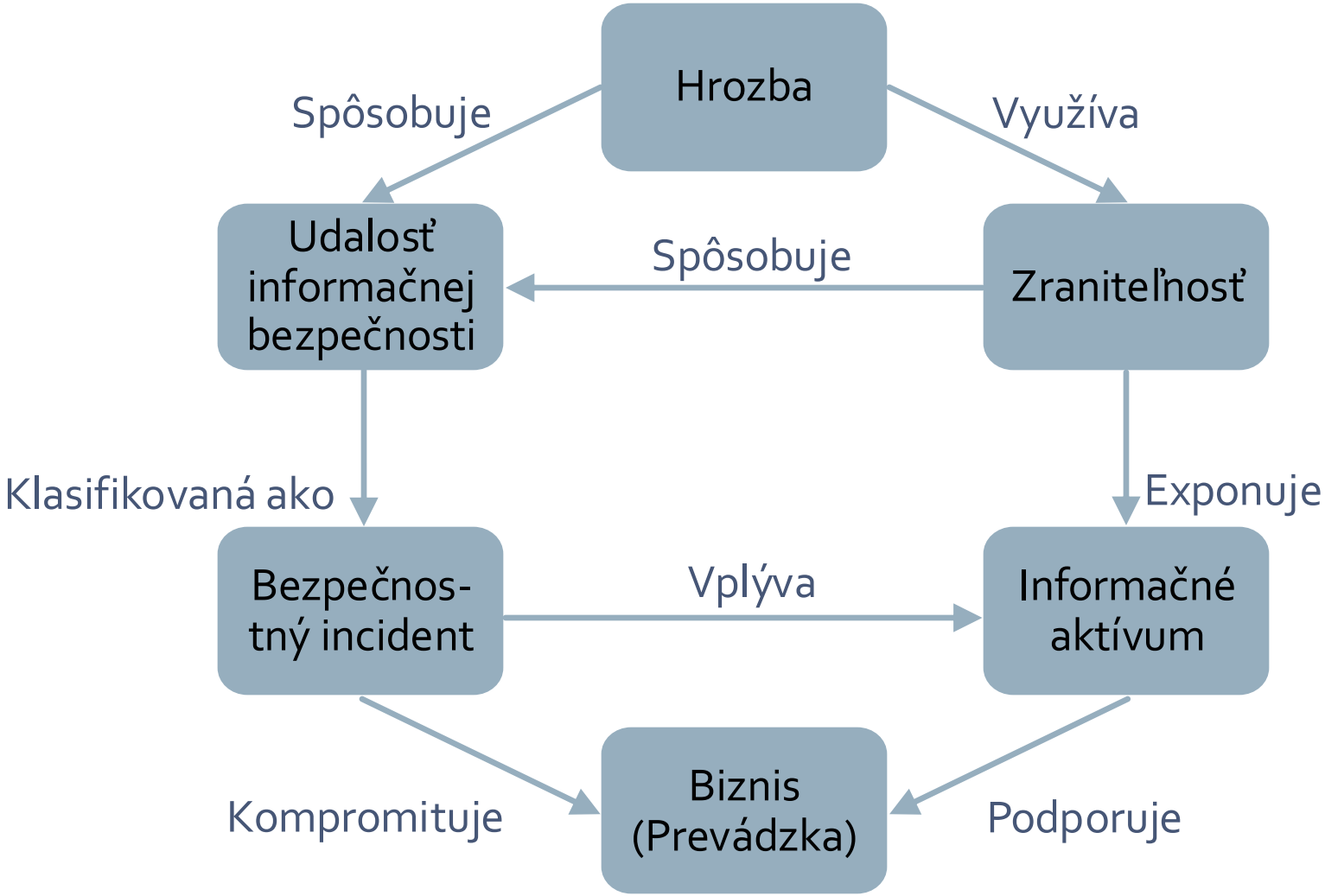
Zraniteľnosť - slabé miesto informačného aktíva, slabina v informačnom systéme, v bezpečnostných procedúrach systému, opatreniach alebo ich implementácii, ktoré môže aktivovať alebo využiť nositeľ hrozieb.

Hrozba - potenciál, že akákoľvek okolnosť či udalosť využije zraniteľnosť informačného aktíva a spôsobí negatívny následok (dopad).

Riziko - funkcia pravdepodobnosti, že hrozba zneužije konkrétnu zraniteľnosť a spôsobí škodlivú udalosť s následnou možnosťou ujmy, negatívneho dopadu alebo škody.

Následok - hodnota závažnosti ujmy, resp. rozsah škody, ktorá môže byť spôsobená zneužitím konkrétnej zraniteľnosti konkrétnou hrozbou.

LOGICKÉ VZŤAHY V RIADENÍ RIZÍK



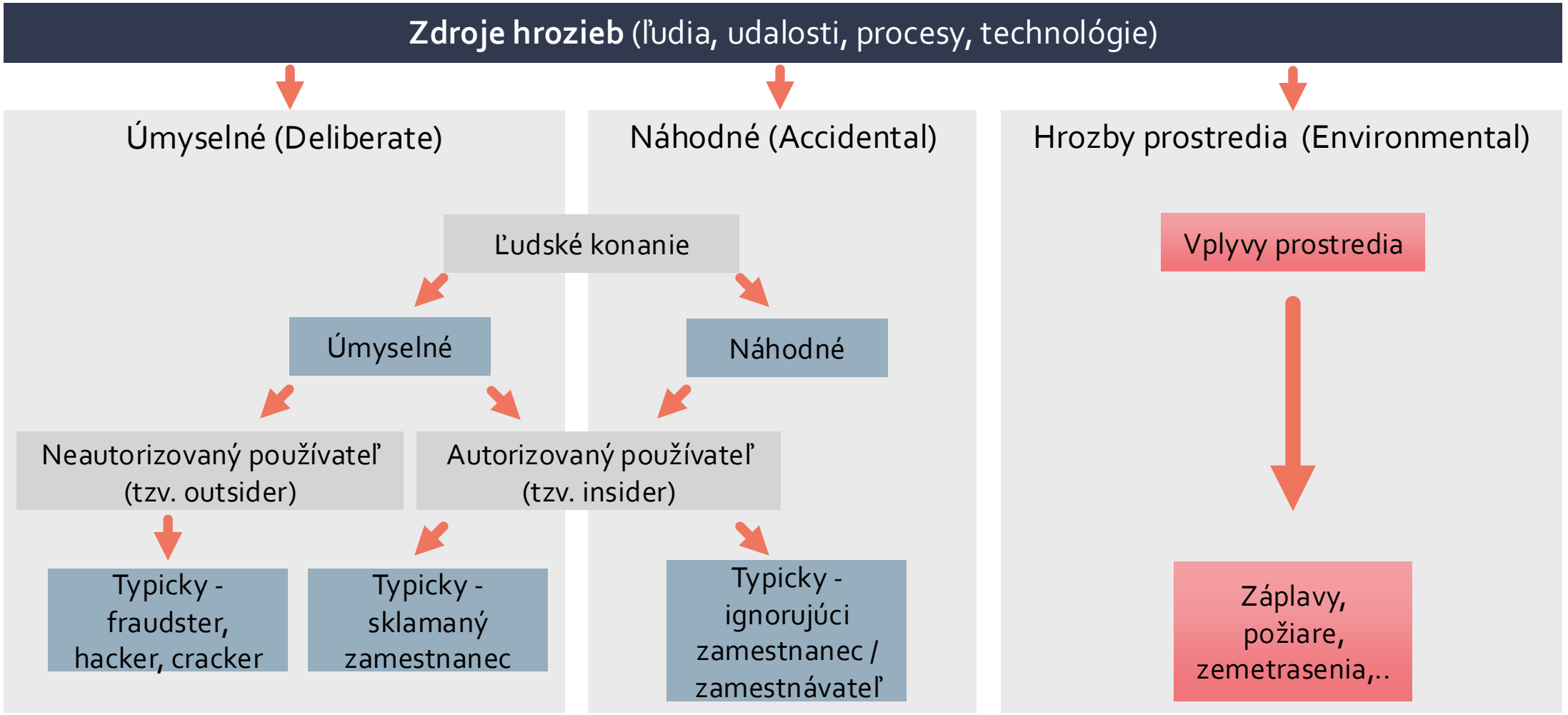
ISO/IEC 27035-1:2016 Informačné technológie - Bezpečnostné metódy - Manažment incidentov v informačnej bezpečnosti - Časť 1: Princípy manažmentu incidentov

ANALÝZA RIZÍK

Postup analýzy rizík:

- stanovenie kontextu
  - identifikácia aktív a ich vlastníkov
  - identifikácia potenciálnych hrozieb
  - identifikácia zraniteľností
  - identifikácia existujúcich opatrení
- identifikácia scenárov rizík
- vyhodnotenie výsledného rizika pre identifikované scenáre rizík
  - určenie pravdepodobnosti naplnenia scenárov rizík
  - ohodnotenie následkov
  - určenie úrovne závažnosti výsledných rizík

HROZBY


Zdroje hrozieb (ľudia, udalosti, procesy, technológie)
Úmyselné (Deliberate)
Náhodné (Accidental)
Hrozby prostredia (Environmental)
Ľudské konanie
Úmyselné
Náhodné
Neautorizovaný používateľ (tzv. outsider)
Autorizovaný používateľ (tzv. insider)
Typicky - fraudster, hacker, cracker
Typicky - sklamaný zamestnanec
Typicky - ignorujúci zamestnanec / zamestnávateľ
Vplyvy prostredia
Záplavy, požiare, zemetrasenia,..

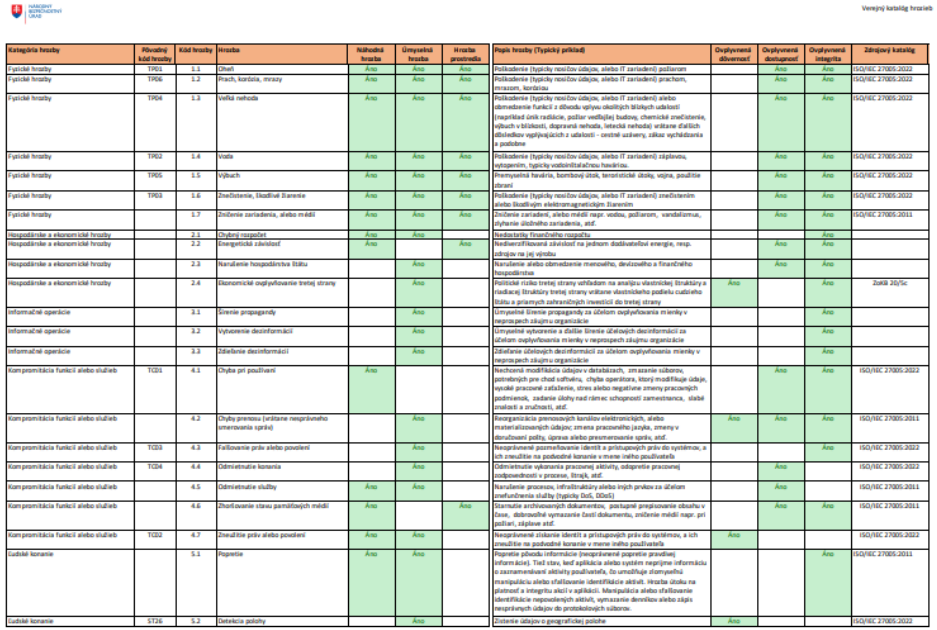
KATALÓGY HROZIEB A ZRANITEĽNOSTÍ

Verejné katalógy hrozieb

- **Katalóg hrozieb NBÚ** - verejný referenčný katalóg hrozieb je poskytnutý PZS ako iniciálny katalóg, ktorý je vhodné doplniť o ďalšie relevantné hrozby *https://www.nbu.gov.sk/verejny-katalog-hrozieb/*
- Katalóg **National Institute of Standards & Technology (NIST) SP 800-30** - poskytuje návrh približne 100 typických škodlivých udalostí
- Katalóg **ENISA Threat Taxonomy** - poskytuje klasifikáciu hrozieb a približne 170 typov hrozieb na rôznej úrovni detailu
- **ISO/IEC 27005** - poskytuje 57 hrozieb v 7 kategóriách
- **Bundesamt fur Sicherheit in der Informatiionstechnik (BSI) IT- Grundschut-Katalog** - poskytuje komplexný zoznam 370 hrozieb spolu s príkladmi pre každú z nich

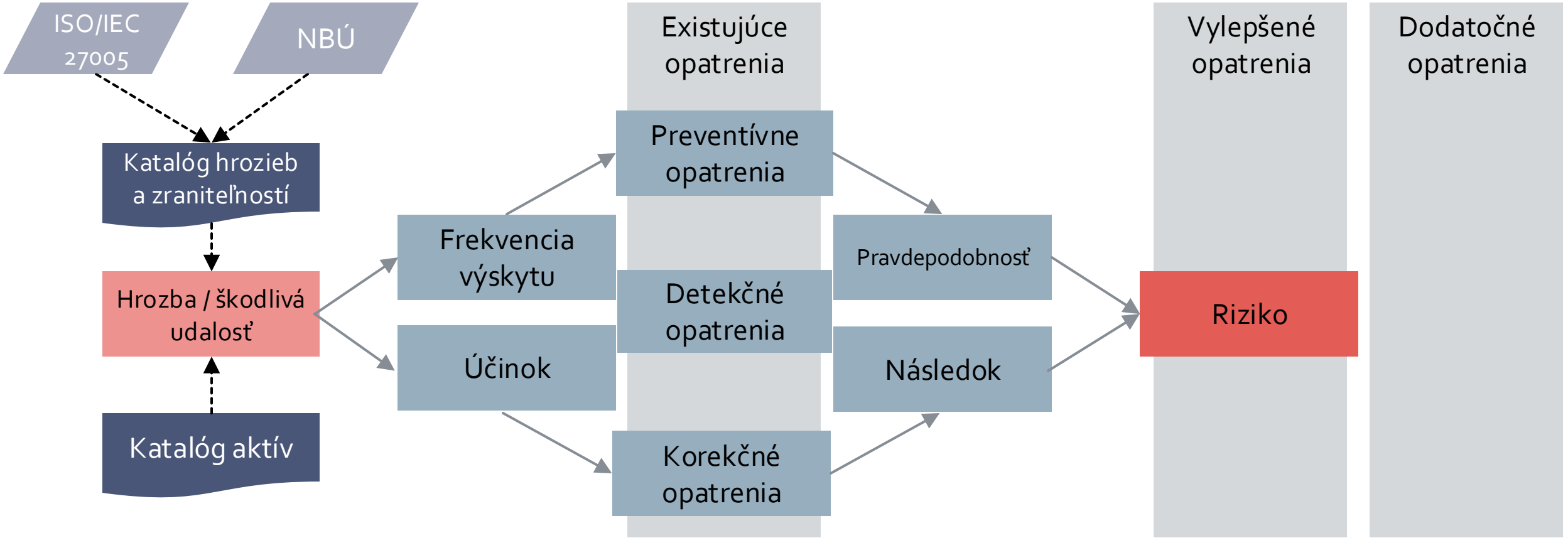
Verejné katalógy zraniteľností

- CVE MITRE - *https://www.cve.org/*
- CVE Details - *https://www.cvedetails.com/*
- CISA - *https://www.cisa.gov/known-exploited-vulnerabilities-catalog*
- OWASP TOP 10



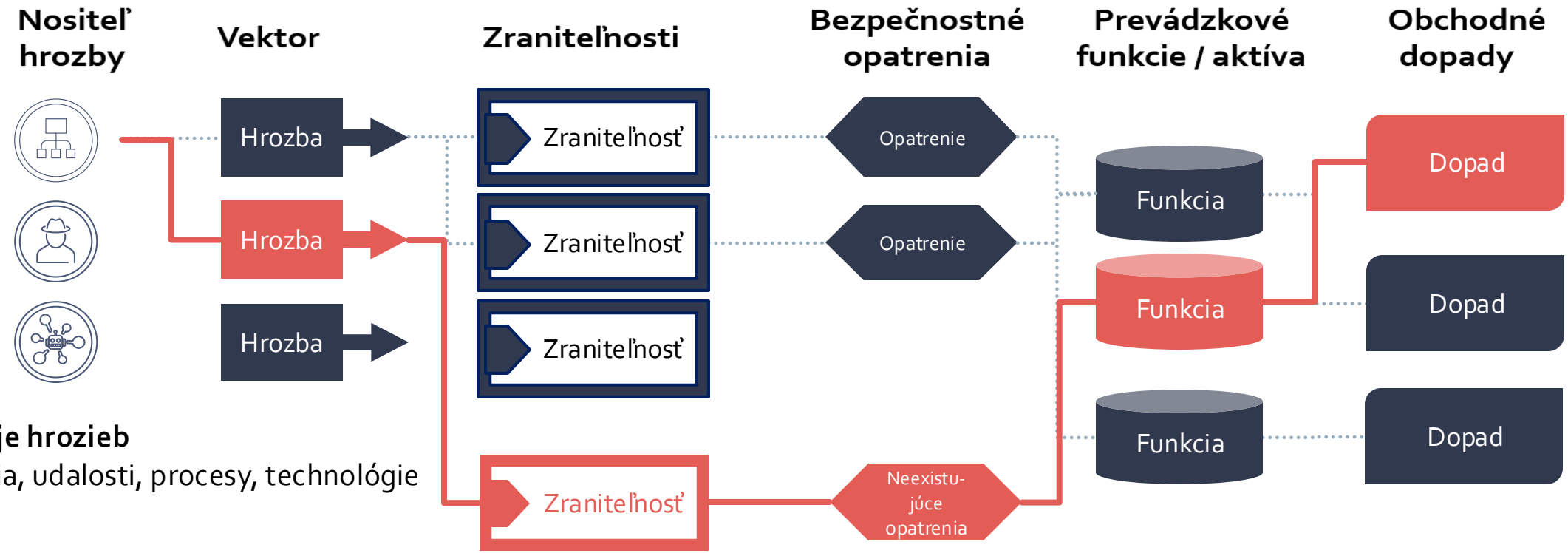
Kategória hrozby	Hlavičný kód hrozby	Kód hrozby	Hrozba	Náhodná hrozba	Úmyselná hrozba	Hrozba prostredia	Popis hrozby (Typický príklad)	Ovplyvnená dôvernosť	Ovplyvnená dostupnosť	Ovplyvnená integrita	Zdrojový katalóg
Fyzické hrozby	TP01	1.1	Oheň	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) požiarom		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP06	1.2	Prach, korózia, mrazy	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) prachom, mrazom, koróziou.		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP04	1.3	Veľká nehoda	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) alebo obmedzenie funkcií z dôvodu výpadu okolitých štítnych udalostí (napríklad únik radiácie, požiar vedľajšej budovy, chemické znečistenie, výbuch v blízkosti, dopravná nehoda, letecká nehoda) vrátane ďalších dôsledkov vyplývajúcich z udalostí - cestné uzávery, zákaz vychádzania a podobne		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP02	1.4	Voda	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) záplavou, vytopením, typicky vodoinštalačnou haváriou.		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP05	1.5	Výbuch	Áno	Áno	Áno	Priemyselná havária, bombový útok, teroristické útoky, vojna, použitie zbraní		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP03	1.6	Znečistenie, škodlivé žiarenie	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) znečistením alebo škodlivým elektromagnetickým žiarením		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby		1.7	Zničenie zariadenia, alebo médií	Áno	Áno	Áno	Zničenie zariadení, alebo médií napr. vodou, požiarom, vandalizmus, zlyhanie úložného zariadenia, atď.		Áno	Áno	ISO/IEC 27005:2011
Hospodárske a ekonomické hrozby		2.1	Chybný rozpočet	Áno	Áno		Nedostatky finančného rozpočtu			Áno	
Hospodárske a ekonomické hrozby		2.2	Energetická závislosť	Áno		Áno	Neefektívnosť závislosť na jednom dodávateľovi energie, resp. zdrojov na jej výrobu		Áno	Áno	
Hospodárske a ekonomické hrozby		2.3	Narušenie hospodárstva štátu		Áno		Narušenie alebo obmedzenie menového, devízového a finančného hospodárstva		Áno	Áno	
Hospodárske a ekonomické hrozby		2.4	Ekonomické ovplyvňovanie tretej strany		Áno		Politické riziko tretej strany vzhľadom na analýzu vlastníkov štruktúry a riadiacej štruktúry tretej strany vrátane vlastníckeho podielu cudzieho štátu a priamych zahraničných investícií do tretej strany.	Áno		Áno	ZoKB 20/Sc
Informačné operácie		3.1	Šírenie propagandy		Áno		Umyselné šírenie propagandy za účelom ovplyvňovania mienky v neprospech záujmu organizácie			Áno	
Informačné operácie		3.2	Vytvorenie dezinformácií		Áno		Umyselné vytvorenie a ďalšie šírenie účelových dezinformácií za účelom ovplyvňovania mienky v neprospech záujmu organizácie			Áno	
Informačné operácie		3.3	Zdieľanie dezinformácií		Áno		Zdieľanie účelových dezinformácií za účelom ovplyvňovania mienky v neprospech záujmu organizácie			Áno	
Kompromitácia funkcií alebo služieb	TC01	4.1	Chyba pri používaní	Áno			Nechtiaca modifikácia údajov v databázach, zmazanie súborov, potrebných pre chod softvéru, chyba operátora, ktorý modifikuje údaje, vysoké pracovné zaťaženie, stres alebo negatívne zmeny pracovných podmienok, zadanie úlohy nad rámec schopností zamestnanca, slabé znalosti a zručnosti, atď.		Áno	Áno	ISO/IEC 27005:2022
Kompromitácia funkcií alebo služieb		4.2	Chyby prenosu (vrátane nesprávneho smerovania správ)		Áno		Reorganizácia prenosových kanálov elektronických, alebo materializovaných údajov; zmena pracovného jazyka, zmeny v doručovaní pošty, úprava alebo presmerovanie správ, atď.	Áno	Áno	Áno	ISO/IEC 27005:2011
Kompromitácia funkcií alebo služieb	TC03	4.3	Falšovanie práv alebo povolení		Áno		Neoprávnené pozmeňovanie identít a prístupových práv do systémov, a ich zneužitie na podvodné konanie v mene iného používateľa			Áno	ISO/IEC 27005:2022
Kompromitácia funkcií alebo služieb	TC04	4.4	Odmietnutie konania		Áno		Odmietnutie vykonania pracovnej aktivity, odoprenie pracovnej zodpovednosti v procese, štrajk, atď.		Áno		ISO/IEC 27005:2022
Kompromitácia funkcií alebo služieb		4.5	Odmietnutie služby	Áno	Áno		Narušenie procesov, infraštruktúry alebo iných práv za účelom znefunkčnenie služby (typicky DoS, DDoS)		Áno		ISO/IEC 27005:2011
Kompromitácia funkcií alebo služieb		4.6	Zhoršovanie stavu pamäťových médií	Áno		Áno	Starnutie archivovaných dokumentov, postupné prepisovanie obsahu v čase, dobrovoľné vymazanie častí dokumentu, zničenie médií napr. pri požiari, záplave atď.		Áno	Áno	ISO/IEC 27005:2011
Kompromitácia funkcií alebo služieb	TC02	4.7	Zneužitie práv alebo povolení	Áno	Áno		Neoprávnené získanie identít a prístupových práv do systémov, a ich zneužitie na podvodné konanie v mene iného používateľa	Áno			ISO/IEC 27005:2022
Ľudské konanie		5.1	Popretie	Áno	Áno		Popretie príčiny informácie (neoprávnené popretie pravdivej informácie). Tiež stav, keď aplikácia alebo systém neprijíme informáciu o zaznamenávaní aktivity používateľa, čo umožňuje zlomyseľnú manipuláciu alebo sfalšovanie identifikácie aktivít. Hrozba útoku na platnosť a integritu akcií v aplikácii. Manipulácia alebo sfalšovanie identifikácie nepoužených aktivít, vymazanie denníkov alebo zápis neoprávnených údajov do protokolových súborov.			Áno	ISO/IEC 27005:2011
Ľudské konanie	ST26	5.2	Detekcia polohy		Áno		Zistenie údajov o geografickej polohe	Áno			ISO/IEC 27005:2022

POSTUP PRI ANALÝZE RIZÍK



SCENÁRE RIZIKA

Scenáre rizika predstavujú špecifické situácie realizácie rizík v kontexte vybraných aktív, pričom môžu byť kombináciou viacerých aktív, kybernetických hrozieb, zraniteľností a ich následkov ako sled alebo kombinácia udalostí vedúcich od počiatočnej príčiny k nežiaducemu následku kybernetického bezpečnostného incidentu.



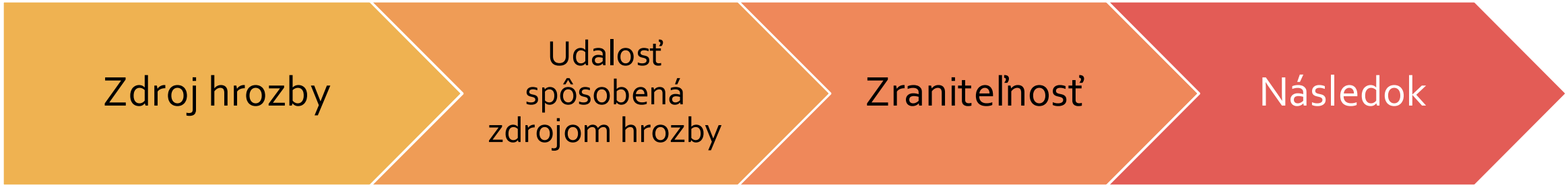
Zdroje hrozieb
- ľudia, udalosti, procesy, technológie

Zdroj: The Open Web Application Security Project (OWASP)

PRÍSTUPY K ANALÝZE RIZIKA

Prístup orientovaný na hrozby (Threat-oriented)

(Zdroj: NIST 800-39, NIST SP 800 30)



Prístup orientovaný na aktíva a následky (Asset-Impact oriented)

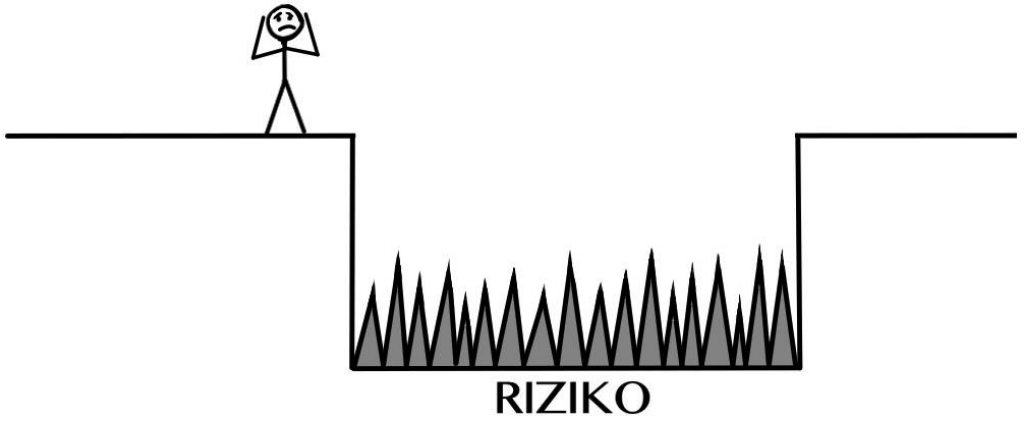


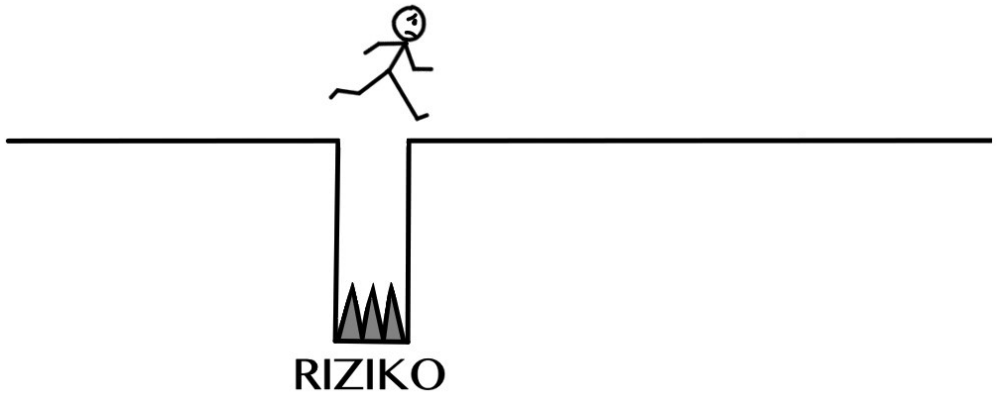
Prístup orientovaný na zraniteľnosti (Vulnerability-oriented)

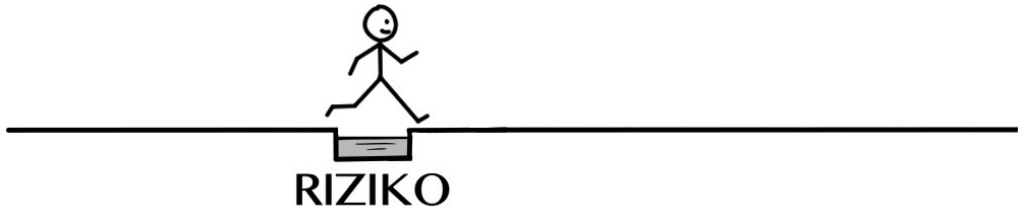


HODNOTENIE RIZIKA









Autor: Hana Gulášová

METÓDY HODNOTENIA RIZIKA

Kvalitatívne metódy

- Použitie **slovných (nečíselných) hodnôt** na vyjadrenie faktorov a úrovní rizika
- Subjektívne hodnotenie (kvalifikovaný odhad)
- Hodnota pravdepodobnosti a dopadu je určená na základe individuálnych odborných znalostí

Kvantitatívne metódy

- Použitie **numerických hodnôt** na vyjadrenie faktorov a úrovní rizika
- Objektívne hodnotenie
- Hodnota pravdepodobnosti a dopadu je určená na základe histórie udalostí

Semikvantitatívne (zmiešané) metódy

- Použitie **numerického rozsahu hodnôt** s jedinečným významom a kontextom
- Kontextové hodnotenie (kvalifikovaný detailný odhad)
- Hodnota pravdepodobnosti a dopadu sú odvodené z rozsahu číselných hodnôt (stupnice) s priradením príslušného stupňa jedinečného významu

PRÍKLAD MATICE PRE STANOVENIE ÚROVNE ZÁVAŽNOSTI RIZIKA KVALITATÍVNOU METÓDOU

Pravdepodobnosť	Dopad			
	Zanedbateľný	Minimálny	Závažný	Katastrofický
Vysoká	C	B	A	A
Stredná	C	B	B	A
Nízka	D	C	B	B
Veľmi nízka	D	D	C	C

Spolufinancovaný Európskou úniou

PRÍKLAD MATICE PRE STANOVENIE ÚROVNE ZÁVAŽNOSTI RIZIKA SEMIKVANTITATÍVNOU METÓDOU

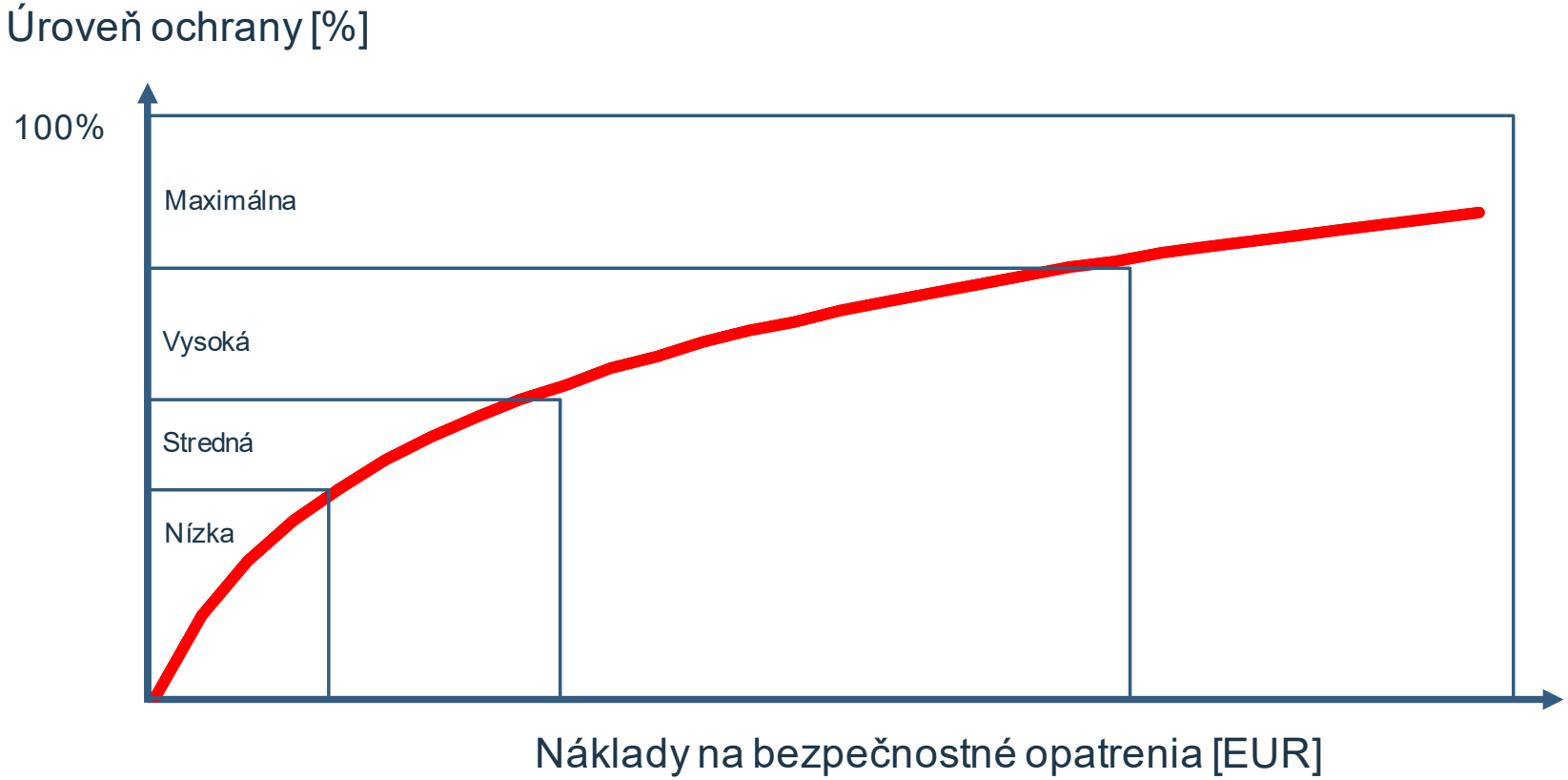
Pravdepodobnosť hrozby	Dopad hrozby				
	Zanedbateľný (5)	Minimálny (20)	Stredný (50)	Závažný (70)	Katastrofický (100)
Vysoká (1)	5*1,0 = 5	20*1,0 = 20	50*1,0 = 50	70*1,0 = 70	100*1,0 = 100
Stredná (0,8)	5*0,8 = 4	20*0,8 = 16	50*0,8 = 40	70*0,8 = 56	100*0,8 = 80
Nízka (0,5)	5*0,5 = 2,5	20*0,5 = 10	50*0,5 = 25	70*0,5 = 35	100*0,5 = 50
Veľmi nízka (0,1)	5*0,1 = 0,5	20*0,1 = 2	50*0,1 = 5	70*0,1 = 7	100*0,1 = 10

KLASIFIKÁCIA ÚROVNÍ ZÁVAŽNOSTI RIZIKA

Závažnosť rizika	Úroveň rizika číselne	Úroveň rizika slovne	Slovný opis závažnosti
A	od 80 do 100	Mimoriadne vysoké	riziko bezprostredne ohrozuje poskytovanie základnej služby, bezpečnosť organizácie, resp. kritického procesu, alebo systému
B	od 50 do 79	Vysoké	riziko potenciálne ohrozuje poskytovanie základnej služby, bezpečnosť organizácie resp. kritického procesu, alebo systému
C	od 10 do 49	Nízke	riziko neohrozuje poskytovanie základnej služby, ohrozuje výkon niektorých podporných procesov, kritické procesy, alebo systémy však nie sú rizikom ohrozené
D	od 1 do 9	Zanedbateľné	riziko neohrozuje poskytovanie základnej služby, výkon procesov a prevádzka systémov nie sú rizikom ohrozené

Ošetrovanie rizík

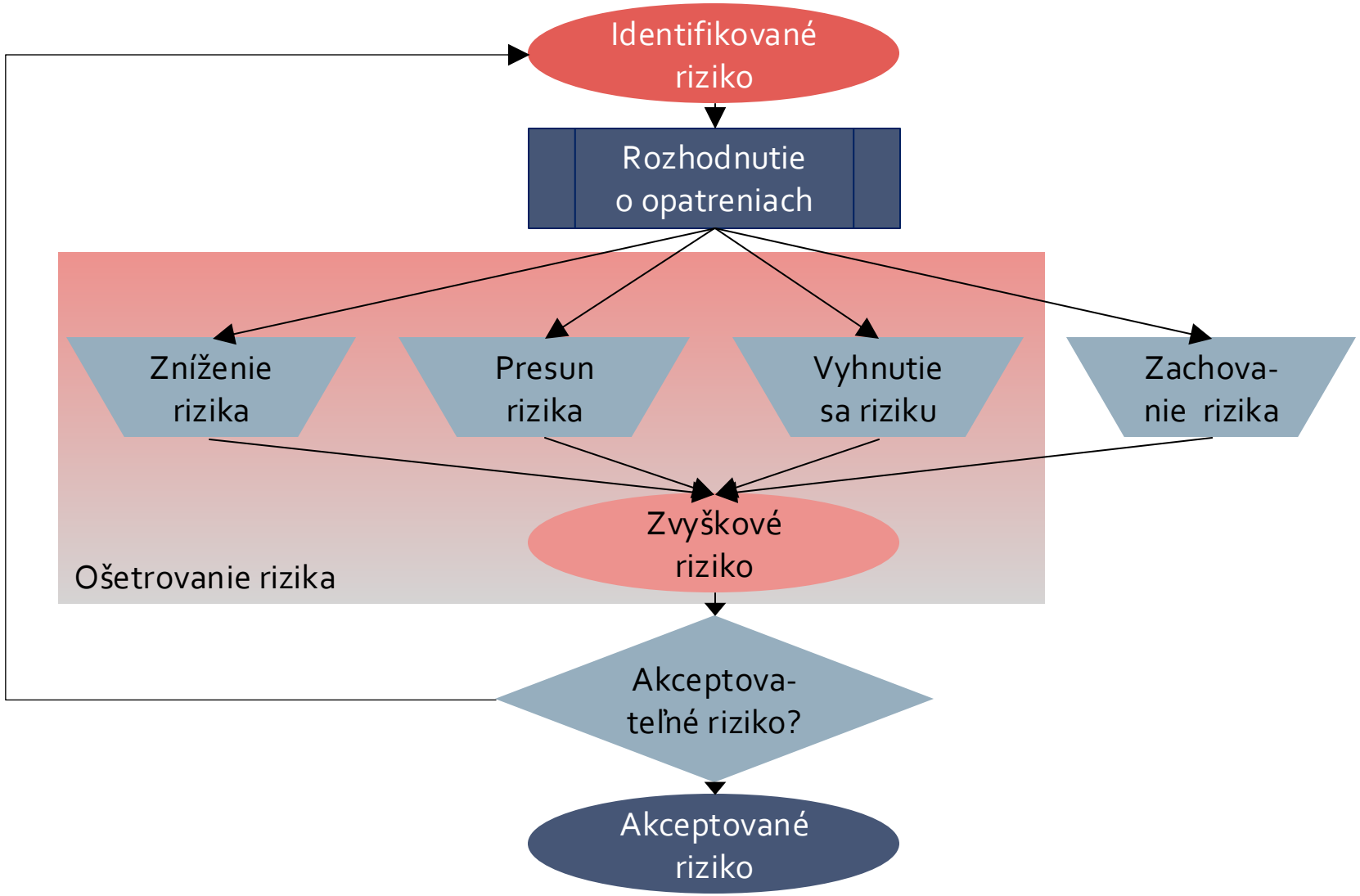
NÁKLADY VS. PRIMERANOSŤ OPATRENÍ



- **Absolútna úroveň bezpečnosti nie je dosiahnuteľná** ani pri neobmedzených nákladoch na bezpečnostné opatrenia
- Rozhodnutie o primeranosti opatrení je úlohou vlastníkov rizík

Zdroj: BSI Standard 100-2 IT-Grundschutz Methodology, v.1.0. Bundesamt für Sicherheit in der Informationstechnik

PROCES OŠETROVANIA RIZÍK



KATALÓGY BEZPEČNOSTNÝCH OPATRENÍ

Verejné katalógy bezpečnostných opatrení

- **Zákon č. 69/2018 o kybernetickej bezpečnosti + Vyhláška 362/2018 Z. z.**
- **Zákon č. 95/2019 o informačných technológiách verejnej správy + Vyhláška 179/2020 Z. z.**
- **ISO/IEC 27002** - Code of Practice for Information Security Controls
- **National Institute of Standards & Technology (NIST) SP 800-53** - Security and Privacy Controls for Information Systems and Organizations
- **NIST Cybersecurity Framework**
- **Bundesamt fur Sicherheit in der Informatiionstechnik (BSI) IT- Grundschut-Katalog**

KOMUNIKÁCIA RIZÍK

- **Komunikácia rizika** – kontinuálny a iteratívny proces, ktorý organizácia vykonáva s cieľom poskytovať, zdieľať alebo získavať informácie a nadviazať dialóg so zainteresovanými stranami o riadení rizika [ISO 31000]
- Organizácia by mala vytvoriť mechanizmy internej komunikácie a reportingu s cieľom podporovať a zodpovednosť za riadenie rizika. Tieto mechanizmy by mali zabezpečiť, aby:
  - kľúčové súčasti rámca riadenia rizík a všetky následné úpravy boli primerane komunikované
  - existuje vhodný interný reporting o rámci, jeho účinnosti a výsledkoch
  - relevantné informácie odvodené z riadenia rizík sú včas k dispozícii na príslušných úrovniach riadenia
  - existujú procesy konzultácie rizika so zainteresovanými stranami
- Tieto mechanizmy by podľa potreby mali zahŕňať postupy na konsolidáciu informácií o rizikách z rôznych zdrojov

ZÁVER

- Ďakujeme za Váš čas
- Nasledujúci webinár na tému „Monitorovanie, hlásenie a riadenie udalostí a kybernetických bezpečnostných incidentov.“ - 20.5.2025



NCC-SK

SLOVAKIA CYBERSECURITY COORDINATION CENTRE



Financované Európskou úniou

Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.

Ochrana vlastníckych práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akékoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastníckych a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.