Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Manažment rizík

Bezpečnostné riziká, opatrenia a prevencia (Blok II)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

prof. Ing. Tomáš Loveček, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Tomas.Lovecek@uniza.sk

Normatívne požiadavky Vyhlášky NBÚ č.362/2018 Z.z.

- **Všetky aktíva** súvisiace so zariadeniami na spracovanie informácií a informačnými prostriedkami **sú identifikované a inventár týchto aktív je centrálne zaznamenaný a riadený.** *(§6 ods.2))*

- Riadenie aktív pozostáva z identifikácie a evidencie všetkých *(§6 ods.3))*:
  a) aktív, od ktorých závisí poskytovanie základnej služby,
  b) podporných služieb, prostredníctvom ktorých sa zabezpečuje kontinuita základnej služby a jej poskytovanie,
  c) zodpovedných osôb za identifikáciu a evidenciu aktív a
  d) vlastníkov aktív.
- Ukončením pracovného pomeru alebo iného obdobného pracovného vzťahu zamestnancov prevádzkovateľa základnej služby a zamestnancov tretích strán sa zadokumentovaným spôsobom vracajú späť všetky zverené aktíva. *(§6 ods.5))*

Normatívne požiadavky zákona o ITVS

- Správca – orgán riadenia (UNIZA) je na úseku obstarávania a implementácie informačných technológií verejnej správy povinný **zabezpečiť riadenie aktív**. *(§15 ods. 1), písm. u))*
- V rámci zabezpečenia riadenia aktív v informačných technológiách verejnej správy správca *(§15 ods. 8))*:

  a) identifikuje a udržiava zoznam svojich aktív,

  b) vyhodnocuje možnosti využitia existujúcich informačných technológií alebo informačných technológií určených na spoločné využitie viacerými orgánmi riadenia a možnosti zdieľania svojich aktív s iným orgánom riadenia (napr. ministerstvo, obec, vyšší územný celok, právnická osoba v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti, atď.),

  c) identifikuje časti aktív, ktorých nedostupnosť alebo znížená kvalita má zásadný vplyv na poskytovanie služieb verejnej správy, služieb vo verejnom záujme alebo verejných služieb,

  d) plánuje životný cyklus aktív v súlade so strategickými plánmi rozvoja informačných technológií verejnej správy a s aktuálnymi potrebami ich prevádzky.

Aktívum vs informačné aktívum

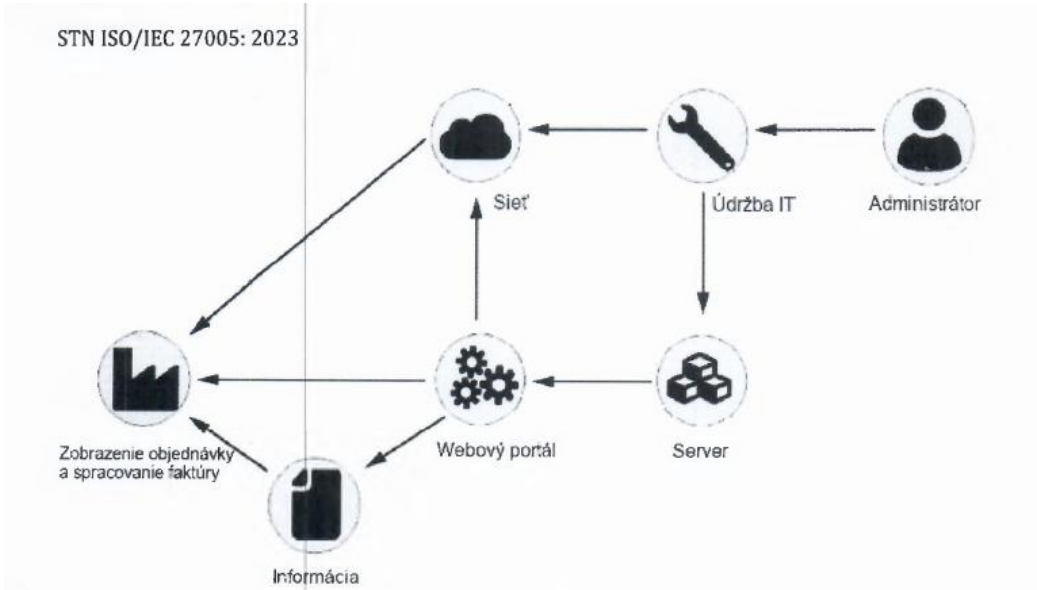
- **Aktívum** - programové vybavenie, technické zariadenie, poskytovaná služba, kvalifikovaná osoba, dobré meno orgánu riadenia a informácia, dokumentácia, zmluva a iná skutočnosť, ktorú považuje orgán riadenia za citlivú. *(Zákon o ITVS §3 písm. u))*
- Klasifikačné stupne opisujú citlivosť **informácií**, **údajov** alebo ďalších s nimi spojených informačných aktív (ďalej len „**informačné aktíva**“). *(Vyhláška NBÚ č.227/2025 Z.z., Príloha č.2)*

Aktíva podľa Vyhlášky č. 179/2020 Z.z.

- Zoznam aktív obsahuje označenie operačného systému alebo firemného softvéru a jeho aktuálne používanej verzie všetkých týchto komponentov informačných technológií verejnej správy (Príloha 1):
  a) pracovná stanica – stolová,
  b) pracovná stanica – prenosná,
  c) aplikačný softvér,
  d) kancelársky softvér,
  e) internetový prehliadač,
  f) antivírusový softvér,
  g) komunikačný softvér,
  h) ďalší využívaný komerčný softvér,
  i) všetky druhy serverov,
  j) virtualizačné prostredie,
  k) databázové prostredie,
  l) komerčný podnikový softvér,
  m) sieťový firewall,
  n) sieťový router,
  o) sieťový prepínač,
  p) komunikačné prostredie,
  q) zálohovacie prostredie,
  r) mobilné zariadenia,
  s) dátové úložiská,
  t) ostatné zariadenia alebo sieťové prvky schopné komunikovať so zvyškom ekosystému informačných technológií verejnej správy,
  u) prenosné zariadenia.

Aktívum

- Aktíva možno rozdeliť do dvoch kategórií (STN ISO/IEC 27005:2023):
  a) **primárne/prevádzkové aktíva** - **informácie** alebo **procesy**, ktoré majú pre organizáciu hodnotu;
  b) **podporné aktíva** - **komponenty informačného systému**, na ktorých je závislé jedno alebo viacero prevádzkových aktív.



Obrázok A.2 – Príklad grafu závislosti aktív

Aktívum

- **Aktívum** (asset) je čokoľvek, čo má pre organizáciu hodnotu. V kontexte informačnej bezpečnosti možno rozlišovať dva druhy aktív (STN ISO/IEC 27002:2023):

  a) **Primárne (prevádzkové) aktíva**:
     i. informácie;
     ii. obchodné procesy a činnosti;

  b) **Podporné aktíva** (na ktoré sa primárne aktíva spoliehajú) všetkých typov, napríklad:
     i. hardvér;
     ii. softvér;
     iii. sieť;
     iv. personál (ako riadiaci orgán, vrcholový manažment, zamestnanci, dočasní zamestnanci, dodávatelia a dobrovoľníci);
     v. lokalita;
     vi. štruktúra organizácie.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Aktívum

- Príklady podľa STN ISO/IEC 27005:2019:
  - a) **Hardvér**: zariadenia na spracovanie dát, mobilné zariadenie, pevné zariadenie, spracovateľské periférie, médiá.
  - b) **Softvér**: operačný systém, SW zabezpečujúci služby, balíkový alebo štandardný SW, podnikateľské aplikácie,
  - c) **Sieť:** napr. verejná komutovaná telefónna sieť (PSTN), ethernet, gigabitový ethernet, asymetrická digitálna účastnícka prípojka (ADSL), špecifikácia bezdrôtového protokolu (napríklad WiFi 802.11), Bluetooth, FireWire, sieťové prvky (router, rozbočovač, prepínač),
  - d) **Personál:** manažment, správa a riadenie ľudských zdrojov, finančný manažment, manažér pre riziká, administrátori systému, administrátori dát, zálohovanie, helpdesk, operátor na využitie aplikácií, bezpečnostní pracovníci, vývojári, ostatní zamestnanci.
  - e) **Lokalita:** Domácnosti zamestnancov, priestory iných organizácií, prostredie mimo lokalitu (mestská oblasť, riziková oblasť), kancelárie, rezervovaná prístupová zóna, bezpečná zóna, inžinierske siete,
  - f) **štruktúra organizácie**: audítori, organizačné zložky, subdodávatelia/dodávatelia, výrobcovia.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Vlastníctvo aktív

- V prípade identifikovaných informácií a iných súvisiacich aktív by sa malo priradiť vlastníctvo aktív jednotlivcovi alebo skupine a mala by sa určiť klasifikácia.
- Mal by sa zaviesť proces na zabezpečenie včasného pridelenia vlastníctva aktív.
- Vlastníctvo by sa malo priradiť pri vytvorení aktív alebo pri prevode aktív do organizácie.
- Vlastníctvo aktív by sa malo podľa potreby prideliť, keď súčasní vlastníci aktív odídu alebo sa zmenia pracovné úlohy.

Povinnosti vlastníka aktív podľa ISO/IEC 27002

- **Vlastník aktíva by mal byť zodpovedný za** správne riadenie aktíva počas celého životného cyklu aktíva, pričom by mal zabezpečiť, aby:
  a) sa informácie a ostatné súvisiace aktíva inventarizovali;
  b) informácie a iné súvisiace aktíva boli vhodne klasifikované a chránené;
  c) sa klasifikácia pravidelne prehodnocovala;
  d) boli uvedené a prepojené komponenty podporujúce technologické aktíva, ako sú databázy, úložiská, softvérové komponenty a subkomponenty;
  e) boli stanovené požiadavky na prijateľné používanie informácií a iných súvisiacich aktív;
  f) obmedzenia prístupu zodpovedali klasifikácii, boli účinné a pravidelne sa prehodnocovali;
  g) sa s informáciami a inými súvisiacimi aktívami pri ich vymazaní alebo likvidácii zaobchádzalo bezpečným spôsobom a boli odstránené z inventárneho zoznamu;
  h) boli zapojené do identifikácie a riadenia rizík spojených s ich aktívami;
  i) podporovali zamestnancov, ktorí majú úlohy a povinnosti súvisiace so správou ich informácií.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Normatívne požiadavky Zákona o KB

- Prevádzkovateľ základnej služby je povinný do 12 mesiacov odo dňa zápisu do registra prevádzkovateľov základnej služby v závislosti od vykonanej **analýzy rizík** prijať, dodržiavať a vykonávať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20. *(§19 ods.1))*

- Prevádzkovateľ základnej služby je povinný pri výkone činnosti, ... prostredníctvom tretej strany, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností ...; pri uzatvorení zmluvy sa vykonáva **analýza rizík**. *(§19 ods.2)*).

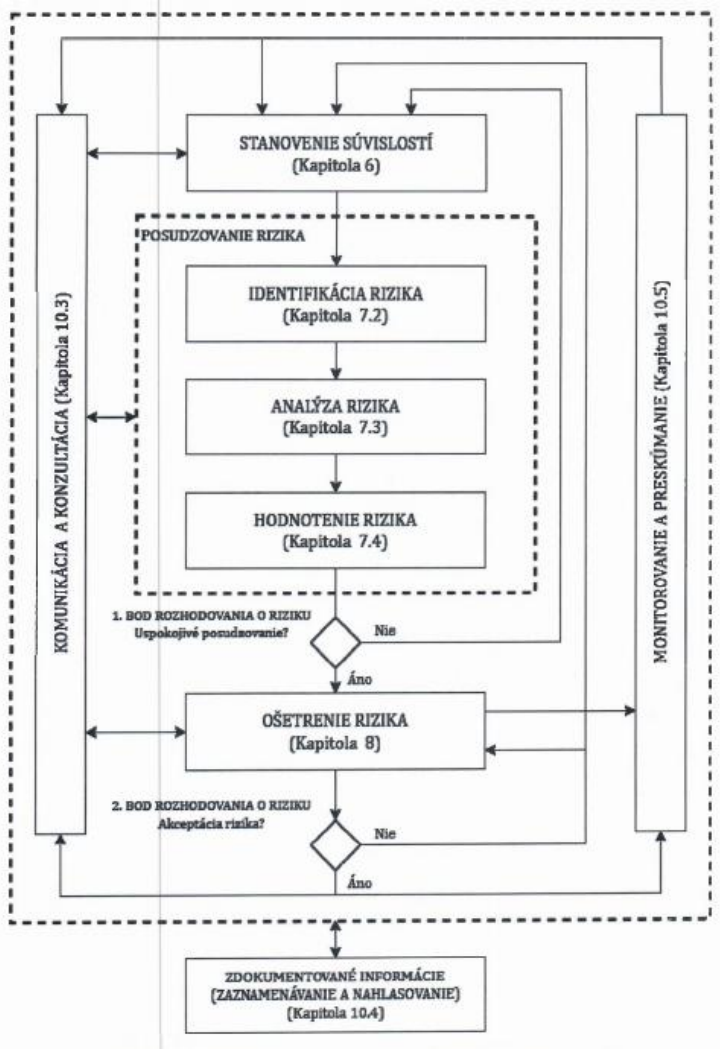
- Bezpečnostné opatrenia sú realizované na základe vykonanej **analýzy rizík** a s prihliadnutím na bezpečnostné metodiky a politiky úradu... *(§20 ods.1)*).

- Bezpečnostné opatrenia sa prijímajú aspoň pre:
  c) správu aktív a **riadenie kybernetických hrozieb a rizík**,... *(§20 ods.2)*).
- Súčasťou analýzy rizík je aj **analýza politického rizika** tretej strany... *(§20 ods.5)*).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Usmernenie k riadeniu rizík informačnej bezpečnosti. (ISO/IEC 27005)

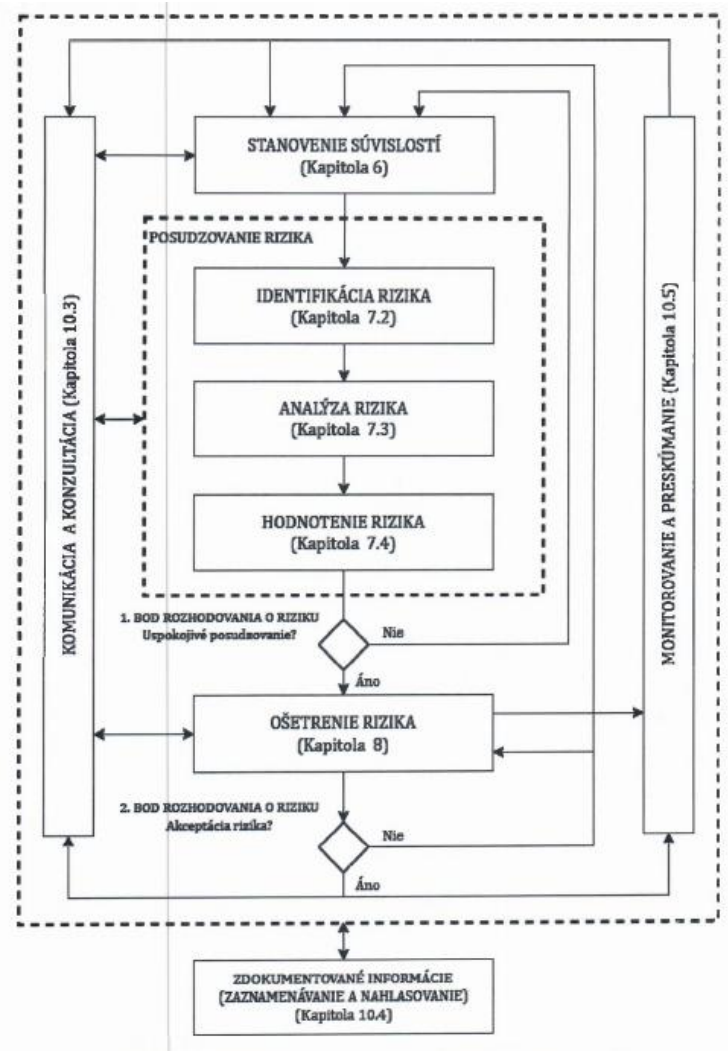
- **Riadenie, resp. manažment, resp. manažérstvo rizika** (risk management) systematické uplatňovanie politík riadenia, procedúr a postupov pri činnostiach komunikácie, konzultácií, stanovenia súvislostí a identifikácie, analýzy, hodnotenia, ošetrenia, monitorovania a preskúmania rizika. (ISO/IEC 31073)
- **Riziká** informačnej bezpečnosti môžu byť spojené s možnosťou, že hrozby zneužijú zraniteľnosti informačného aktíva alebo skupiny informačných aktív a spôsobia tak organizácii škodu. (ISO/IEC 27005).
- **Scenár rizika** (risk scenario) postupnosť alebo kombinácia udalostí vedúca od počiatočnej príčiny k nežiaducemu následku. (ISO/IEC 27005)
- **Úroveň/stupeň rizika** (level of risk) je vyjadrená ako kombinácia následkov a ich pravdepodobnosti. (ISO 31073)



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

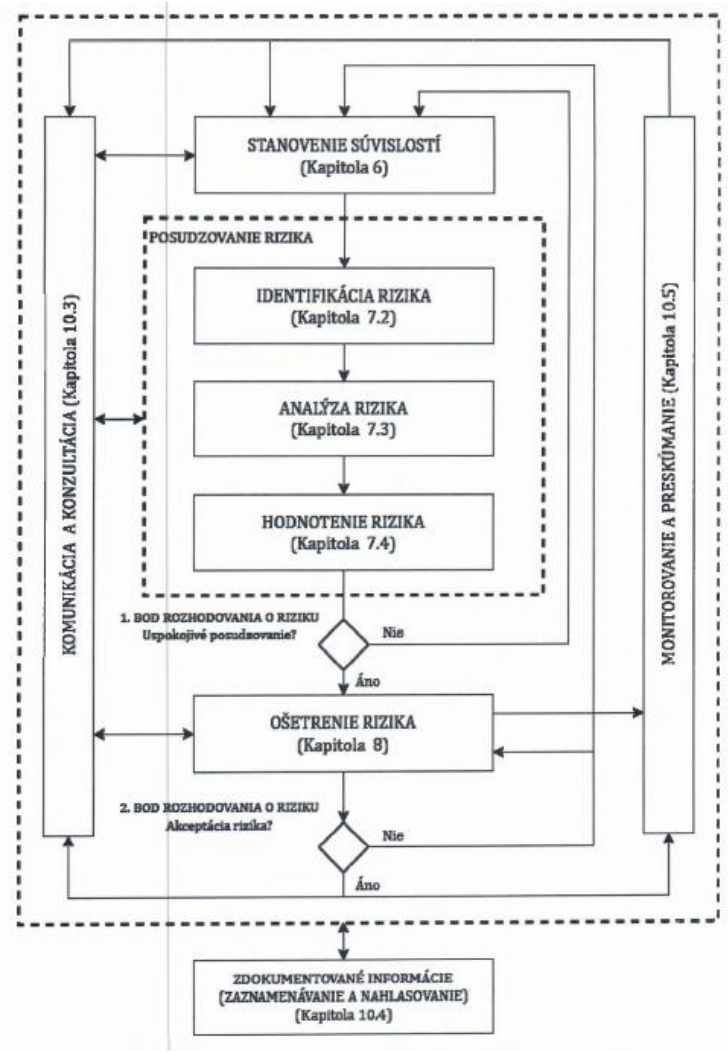
Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Usmernenie k riadeniu rizík informačnej bezpečnosti. (ISO/IEC 27005)

- **Posúdenie rizika** (risk assessment) celkový proces identifikácie rizika, analýzy rizika a hodnotenia rizika. (ISO 31073)
- **Identifikácia rizika** (risk identification) proces vyhľadávania, rozpoznávania a opisu rizík. Identifikácia rizík zahŕňa identifikáciu zdrojov rizík, udalostí, ich príčin a potenciálnych následkov. (ISO 31073)
- **Analýza rizík** (risk analysis) proces na pochopenie povahy rizika a určenie úrovne rizika. Analýza rizika poskytuje základ pre hodnotenie rizík a rozhodnutia o ošetrení rizík .Analýza rizika zahŕňa odhad rizika. (ISO 31073)
- **Hodnotenie rizík** (risk evaluation) proces porovnávania výsledkov analýzy rizík s kritériami rizika s cieľom určiť, či je riziko a/alebo jeho významnosť. Hodnotenie rizika pomáha pri rozhodovaní o ošetrení rizík. (ISO 31073)
- **Ošetrenie rizík** (risk treatment) proces na úpravu rizika. (ISO 31073)



Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Usmernenie k riadeniu rizík informačnej bezpečnosti. (ISO/IEC 27005)

- **Akceptovanie rizika** (risk aceptance) informované rozhodnutie podstúpiť určité riziko. K akceptácii rizika môže dôjsť bez ošetrenia rizika alebo počas procesu ošetrenia rizika. Prijaté riziká podliehajú monitorovaniu a preskúmaniu. (ISO 31073)
- **Zvyškové riziko** (residual risk) je riziko zostávajúce po ošetrení rizika. Zvyškové riziko môže obsahovať neidentifikované riziko. Zvyškové riziká môžu obsahovať aj ponechané riziko. (ISO 31073)
- **Vlastník rizika** (risk owner) osoba alebo subjekt so zodpovednosťou a právomocou riadiť riziko. (ISO/IEC 27000)
- **Ochota podstupovať riziko** (risk appetite) množstvo a typ rizika, ktoré je organizácia ochotná podstúpiť alebo si ponechať. (ISO/IEC 27005)



Proces posúdenia rizík informačnej bezpečnosti
Identifikácia rizík informačnej bezpečnosti

- **Hrozba** (threat) potenciálna príčina nežiaduceho incidentu, ktorý môže mať za následok poškodenie systému, jednotlivca alebo organizácie. (ISO/IEC 27000)
- **Kybernetická hrozba** je každá potenciálna okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť siete a informačné systémy, užívateľov takýchto systémov a iné osoby. (Zákon o KB)
- **Hrozba** – potencionálny zdroj nebezpečia, ujmy alebo iného nežiadúceho výsledku. (ISO 31073)
- **Zdroj hrozby** (threat agent) je jednotlivec alebo skupina jednotlivcov, ktorí majú akúkoľvek úlohu pri vykonávaní alebo podpore útoku. (ISO/IEC 27032)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Proces posúdenia rizík informačnej bezpečnosti
Identifikácia rizík informačnej bezpečnosti

- **Útok** (attack) pokus o zničenie, odhalenie, zmenenie, znefunkčnenie, ukradnutie alebo získanie neoprávneného prístupu k aktívam alebo ich neoprávnene používať. (ISO/IEC 27000)
- **Vektor útoku** (attack vector) cesta alebo prostriedok, ktorým útočník môže získať prístup k počítaču alebo sieťovému serveru na vykonanie škodlivej činnosti. (ISO/IEC 27032)
- **Zmiešaný útok** (blended attack) útok, ktorý sa snaží maximalizovať závažnosť škody a rýchlosť šírenia nákazy kombináciou viacerých útočných metód. (ISO/IEC 27032)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Proces posúdenia rizík informačnej bezpečnosti

Identifikácia rizík informačnej bezpečnosti

Kategória	Číslo	Popis hrozby	Typ zdroja rizika [a]
Fyzické hrozby	TP01	Požiar	A, D, E
	TP02	Voda	A, D, E
	TP03	Znečistenie, škodlivé žiarenie	A, D, E
	TP04	Vážna nehoda	A, D, E
	TP05	Výbuch	A, D, E
	TP06	Prach, korózia, mráz	A, D, E
Prírodné hrozby	TN01	Klimatický jav	E
	TN02	Seizmický jav	E
	TN03	Vulkanický jav	E
	TN04	Meteorologický jav	E
	TN05	Povodne	E
	TN06	Pandémia/epidémia	E
Zlyhania infraštruktúry	TI01	Porucha zásobovacieho systému	A, D
	TI02	Porucha chladiaceho alebo ventilačného systému	A, D
	TI03	Strata napájania	A, D, E
	TI04	Zlyhanie telekomunikačnej siete	A, D, E
	TI05	Porucha telekomunikačného zariadenia	A, D
	TI06	Elektromagnetické žiarenie	A, D, E
	TI07	Tepelné žiarenie	A, D, E
	TI08	Elektromagnetické impulzy	A, D, E

Kategória	Číslo	Popis hrozby	Typ zdroja rizika [a]
Technické poruchy	TT01	Porucha zariadenia alebo systému	A
	TT02	Nasýtenie informačného systému	A, D
	TT03	Porušenie udržiavateľnosti informačného systému	A, D
Ľudské činy	TH01	Teroristický útok, sabotáž	D
	TH02	Sociálne inžinierstvo	D
	TH03	Zachytenie žiarenia zariadenia	D
	TH04	Špehovanie na diaľku	D
	TH05	Odpočúvanie	D
	TH06	Krádež médií alebo dokumentov	D
	TH07	Krádež zariadenia	D
	TH08	Krádež digitálnej identity alebo poverení	D
	TH09	Získavanie recyklovaných alebo vyradených médií	D
	TH10	Zverejňovanie informácií	A, D
	TH11	Zadávanie údajov z nedôveryhodných zdrojov	A, D
	TH12	Manipulácia s hardvérom	D
	TH13	Manipulácia so softvérom	A, D
	TH14	Zneužitie zraniteľnosti webovou komunikáciou	D
	TH15	Útok opakovaním, útok man-in-the-middle	D
	TH16	Neoprávnené spracúvanie osobných údajov	A, D
	TH17	Neoprávnený vstup do zariadení	D
	TH18	Neoprávnené používanie zariadení	D
	TH19	Nesprávne používanie zariadení	A, D
	TH20	Poškodenie zariadení alebo médií	A, D
	TH21	Podvodné kopírovanie softvéru	D
	TH22	Používanie falšovaného alebo kopírovaného softvéru	A, D
	TH23	Poškodenie údajov	D
	TH24	Nezákonné spracovanie údajov	D
	TH25	Odosielanie alebo distribúcia škodlivého softvéru	A, D, E
	TH26	Zisťovanie polohy	D
Kompromitácia funkcií alebo služieb	TC01	Chyba pri používaní	A
	TC02	Zneužitie práv alebo povolení	A, D
	TC03	Falšovanie práv alebo povolení	D
	TC04	Odmietnutie aktivít	D
Organizačné hrozby	TO01	Nedostatok zamestnancov	A, E
	TO02	Nedostatok zdrojov	A, E
	TO03	Zlyhanie poskytovateľov služieb	A, E
	TO04	Porušenie zákonov alebo predpisov	A, D

[a] D = úmyselná; A = náhodná; E = environmentálna.

Príklad typických hrozieb

Proces posúdenia rizík informačnej bezpečnosti
Identifikácia rizík informačnej bezpečnosti

- **Zraniteľnosť** (vulnerability) je slabé miesto aktíva alebo opatrenia, ktoré môže byť zneužité jednou alebo viacerými hrozbami. (ISO/IEC 27000)
- **Zraniteľnosť** (vulnerability) chyba, slabina alebo vlastnosť v návrhu alebo implementácii informačného systému (vrátane jeho bezpečnostných opatrení) alebo jeho prostredia, ktoré by mohli byť úmyselne alebo neúmyselne zneužité a ktoré by mohli nepriaznivo ovplyvniť aktíva alebo prevádzku organizácie. (ISO/IEC TR 19791)
- **Zraniteľnosť** akýkoľvek nežiaduci stav alebo chyba technického prostriedku alebo programového prostriedku, alebo nedostatok procesu vrátane nesprávnej bezpečnostnej konfigurácie, ktorá môže byť zneužitá kybernetickou hrozbou. (Zákon o KB)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Proces posúdenia rizík informačnej bezpečnosti

Identifikácia rizík informačnej bezpečnosti

Kategória	Číslo	Príklady zraniteľností
Hardvér	VH01	Nedostatočná údržba/chybná inštalácia pamäťových médií
	VH02	Nedostatočné plány pravidelnej výmeny zariadení
	VH03	Náchylnosť na vlhkosť, prach, znečistenie
	VH04	Citlivosť na elektromagnetické žiarenie
	VH05	Nedostatočná kontrola zmien konfigurácie
	VH06	Citlivosť na zmeny napätia
	VH07	Citlivosť na zmeny teploty
	VH08	Nechránené ukladanie
	VH09	Nedostatok starostlivosti pri likvidácii
	VH10	Nekontrolované kopírovanie
Softvér	VS01	Žiadne alebo nedostatočné testovanie softvéru
	VS02	Známe chyby v softvéri
	VS03	Žiadne „odhlásenie" pri opustení pracovnej stanice
	VS04	Likvidácia alebo opätovné použitie pamäťových médií bez riadneho vymazania
	VS05	Nedostatočná konfigurácia logov na účely auditného záznamu
	VS06	Nesprávne pridelenie prístupových práv
	VS07	Široko distribuovaný softvér
	VS08	Použitie aplikačných programov na nesprávne údaje z časového hľadiska
	VS09	Komplikované používateľské rozhranie
	VS10	Nedostatočná alebo chýbajúca dokumentácia
	VS11	Nesprávne nastavenie parametrov
	VS12	Nesprávne dátumy
	VS13	Nedostatočné identifikačné a autentifikačné mechanizmy (napr. na overenie používateľa)
	VS14	Nechránené tabuľky hesiel
	VS15	Slabá správa hesiel
	VS16	Povolené nepotrebné služby
	VS17	Nevyspelý alebo nový softvér
	VS18	Nejasné alebo neúplné špecifikácie pre vývojárov
	VS19	Neúčinná kontrola zmien
	VS20	Nekontrolované sťahovanie a používanie softvéru
	VS21	Nedostatok alebo neúplnosť záložných kópií
	VS22	Nevypracovanie správ o riadení
Sieť	VN01	Nedostatočné mechanizmy na preukázanie odoslania alebo prijatia správy
	VN02	Nechránené komunikačné linky
	VN03	Nechránená citlivá prevádzka
	VN04	Zlá spoločná kabeláž
	VN05	Jediný bod zlyhania

Kategória	Číslo	Príklady zraniteľností
Sieť	VN06	Neúčinné alebo chýbajúce mechanizmy na identifikáciu a autentifikáciu odosielateľa a príjemcu
	VN07	Nezabezpečená sieťová architektúra
	VN08	Prenos hesiel v čitateľnej podobe
	VN09	Nedostatočné riadenie siete (odolnosť smerovania)
	VN10	Nechránené verejné sieťové pripojenia
Personál	VP01	Neprítomnosť personálu
	VP02	Nedostatočné postupy pri prijímaní zamestnancov
	VP03	Nedostatočné bezpečnostné školenie
	VP04	Nesprávne používanie softvéru a hardvéru
	VP05	Slabé povedomie o bezpečnosti
	VP06	Nedostatočné alebo chýbajúce mechanizmy monitorovania
	VP07	Práca bez dozoru externých alebo upratovacích pracovníkov
	VP08	Neúčinné alebo chýbajúce zásady správneho používania telekomunikačných médií a zasielania správ
Lokalita	VS01	Nedostatočné alebo nedbalé používanie fyzických opatrení prístupu do budov a miestností
	VS02	Poloha v oblasti náchylnej na záplavy
	VS03	Nestabilná elektrická sieť
	VS04	Nedostatočná fyzická ochrana budovy, dverí a okien
Organizácia	VO01	Formálny postup registrácie a zrušenia registrácie používateľov nie je vypracovaný alebo jeho vykonávanie je neúčinné
	VO02	Formálny proces preskúmania prístupových práv (dohľad) nie je vypracovaný alebo jeho vykonávanie je neúčinné
	VO03	Nedostatočné ustanovenia (týkajúce sa bezpečnosti) v zmluvách so zákazníkmi a/alebo tretími stranami
	VO04	Postup monitorovania zariadení na spracovanie informácií nie je vypracovaný alebo jeho vykonávanie je neúčinné
	VO05	Audity (dohľad) sa nevykonávajú pravidelne
	VO06	Postupy identifikácie a posúdenia rizík nie sú vypracované alebo ich vykonávanie je neúčinné
	VO07	Nedostatočné alebo chýbajúce hlásenia o poruchách zaznamenané v logoch správcu a operátora
	VO08	Neprimeraná reakcia na servisnú údržbu
	VO09	Nedostatočná alebo chýbajúca dohoda o úrovni služieb
	VO10	Postup kontroly zmien nie je vypracovaný alebo jeho vykonávanie je neúčinné
	VO11	Formálny postup kontroly dokumentácie ISMS nie je vypracovaný alebo jeho implementácia je neúčinná
	VO12	Formálny postup pre dohľad nad záznamami ISMS nie je vypracovaný alebo jeho vykonávanie je neúčinné
	VO13	Formálny proces autorizácie verejne dostupných informácií nie je vypracovaný alebo jeho vykonávanie je neúčinné

Príklad typických zraniteľností

Proces posúdenia rizík informačnej bezpečnosti

Identifikácia rizík informačnej bezpečnosti

Kategória	Číslo	Príklady zraniteľností
Organizácia	V014	Nesprávne rozdelenie zodpovednosti za informačnú bezpečnosť
	V015	Plány kontinuity neexistujú, sú neúplné alebo zastarané
	V016	Politika používania elektronickej pošty nie je vypracovaná alebo jej vykonávanie je neúčinné
	V017	Postupy zavádzania softvéru do prevádzkových systémov nie sú vypracované alebo ich implementácia je neúčinná
	V018	Postupy pre manipuláciu s klasifikovanými informáciami nie sú vypracované alebo ich vykonávanie je neúčinné
	V019	Povinnosti v oblasti informačnej bezpečnosti nie sú uvedené v opisoch pracovných miest
	V020	Nedostatočné alebo chýbajúce ustanovenia (týkajúce sa informačnej bezpečnosti) v zmluvách so zamestnancami
	V021	Disciplinárny postup v prípade incidentu v oblasti informačnej bezpečnosti nie je definovaný alebo nefunguje správne
	V022	Formálna politika používania mobilných počítačov nie je vypracovaná alebo jej uplatňovanie je neúčinné
	V023	Nedostatočná kontrola aktív mimo pracoviska
	V034	Nedostatočná alebo chýbajúca politika „čistého stola a čistej obrazovky"
	V025	Autorizácia zariadení na spracovanie informácií nie je zavedená alebo nefunguje správne
	V026	Mechanizmy monitorovania narušení bezpečnosti nie sú riadne zavedené
	V027	Postupy na nahlasovanie bezpečnostných nedostatkov nie sú vypracované alebo ich vykonávanie je neúčinné
	V028	Postupy dodržiavania ustanovení o duševných právach nie sú vypracované alebo ich uplatňovanie je neúčinné

Príklad typických zraniteľností

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Proces ošetrenia rizík informačnej bezpečnosti
Výber vhodných možností ošetrenia rizík informačnej bezpečnosti

- Medzi niekoľko možností ošetrenia rizík patrí:
  a) vyhnutie sa riziku, a to rozhodnutím nezačať alebo nepokračovať v činnosti, ktorá spôsobuje riziko;
  b) úprava rizika zmenou pravdepodobnosti výskytu udalosti alebo následku alebo zmenou závažnosti následku;
  c) zachovanie rizika prostredníctvom informovaného rozhodnutia;
  d) zdieľanie rizika rozdelením zodpovednosti s inými stranami, buď interne, alebo externe (napr. rozdelenie následkov prostredníctvom poistenia).

Proces ošetrenia rizík informačnej bezpečnosti
Určenie všetkých opatrení, ktoré sú potrebné na implementáciu

- Medzinárodná norma ISO/IEC 27002 je určená pre organizácie všetkých typov a veľkostí. Používa sa ako referencia na určenie a implementáciu opatrení na ošetrenie rizík informačnej bezpečnosti v systéme riadenia informačnej bezpečnosti (ISMS) založenom na ISO/IEC 27001.
- Organizačné alebo prostrediu špecifické opatrenia odlišné od opatrení zahrnutých v norme, je možné určiť prostredníctvom posúdenia rizík podľa potreby.
- Norma poskytuje všeobecnú kombináciu organizačných, ľudských, fyzických a technologických opatrení informačnej bezpečnosti odvodených z medzinárodne uznávaných osvedčených postupov.
- Pri špecifikovaní takýchto opatrení by organizácia mala zvážiť zdroje a investície potrebné na implementáciu a prevádzku opatrení s realizovanou obchodnou hodnotou.

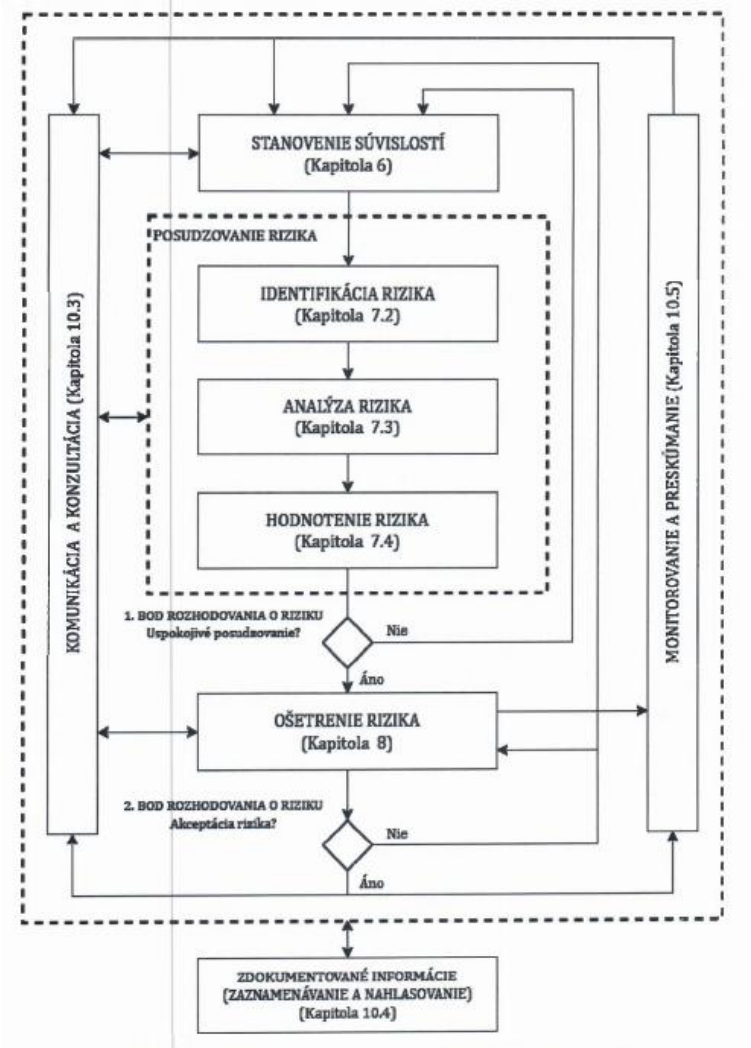
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Proces ošetrenia rizík informačnej bezpečnosti

Určenie všetkých opatrení, ktoré sú potrebné na implementáciu možností ošetrenia rizík informačnej bezpečnosti

- Existujú normy špecifické pre odvetvie, ktoré obsahujú ďalšie opatrenia, ktorých cieľom je riešiť konkrétne oblasti (napr. ISO/IEC 27017 pre cloudové služby, ISO/IEC 27701 pre ochranu osobných údajov, ISO/IEC 27019 pre energetický priemysel, ISO/IEC 27011 pre telekomunikačné služby a ISO 277999 pre oblasť zdravotníctva).
- Norma je štruktúrovaná do nasledujúcich kapitol/tém:
  a) Organizačné opatrenia (kapitola 5).
  b) Personálne opatrenia (kapitola 6).
  c) Fyzické opatrenia (kapitola 7).
  d) Technické opatrenia (kapitola 8).

Zamestnanec v procese ochrany aktív vo svojej organizácii (diskusia)



Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Manažment rizík

Bezpečnostné riziká, opatrenia a prevencia (Blok II)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

prof. Ing. Tomáš Loveček, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Tomas.Lovecek@uniza.sk