Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Riadenie kontinuity činností

Zálohovanie, obnova systémov po havárii a krízové riadenie (Blok II)

Kurz: Manažér kybernetickej bezpečnosti

Doc. Ing. Katarína Kampová, PhD.

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

Katarina.Kampova@uniza.sk

Neviditeľná búrka s reálnymi následkami

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

Vnímanie kontinuity činnosti

Kontinuita podnikania znamená plány kontinuity podnikania.

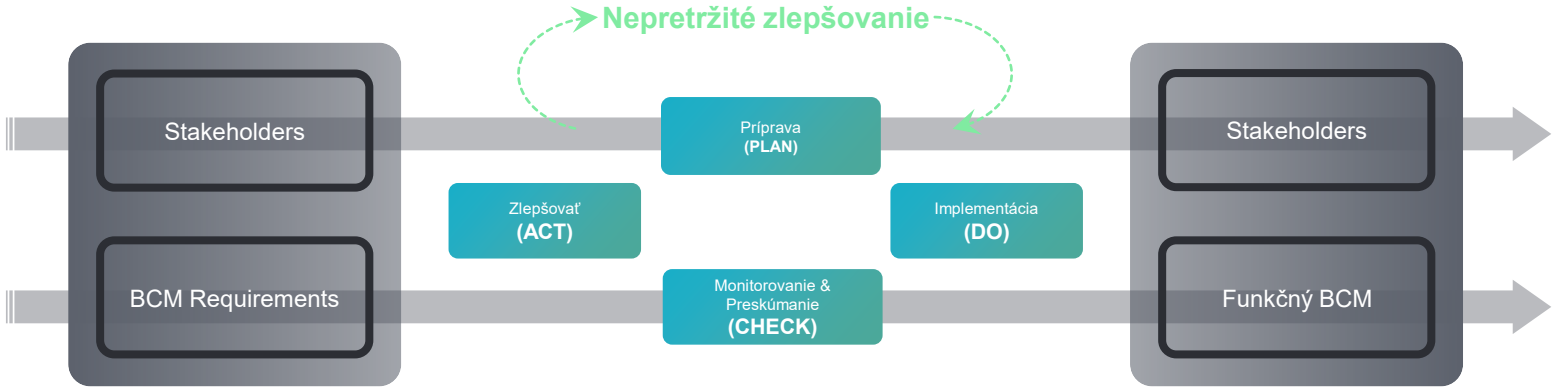
Kontinuita podnikania je práca pre IT odborníkov.

Kontinuita podnikania je jednorazová práca.

Čo je systém kontinuity podnikania

- (Business Continuity Management System - BCMS) je komplexný rámec a systém, ktorý organizácie používajú na plánovanie a riadenie kontinuity svojich kľúčových činností a procesov v prípade neočakávaných udalostí, krízových situácií, havárií alebo iných rušivých udalostí.

- Cieľom BCMS je zabezpečiť, aby organizácie boli schopné udržať svoju prevádzku a minimalizovať dopady týchto udalostí na svojich zamestnancov, zákazníkov, dodávateľov a celkovú činnosť.

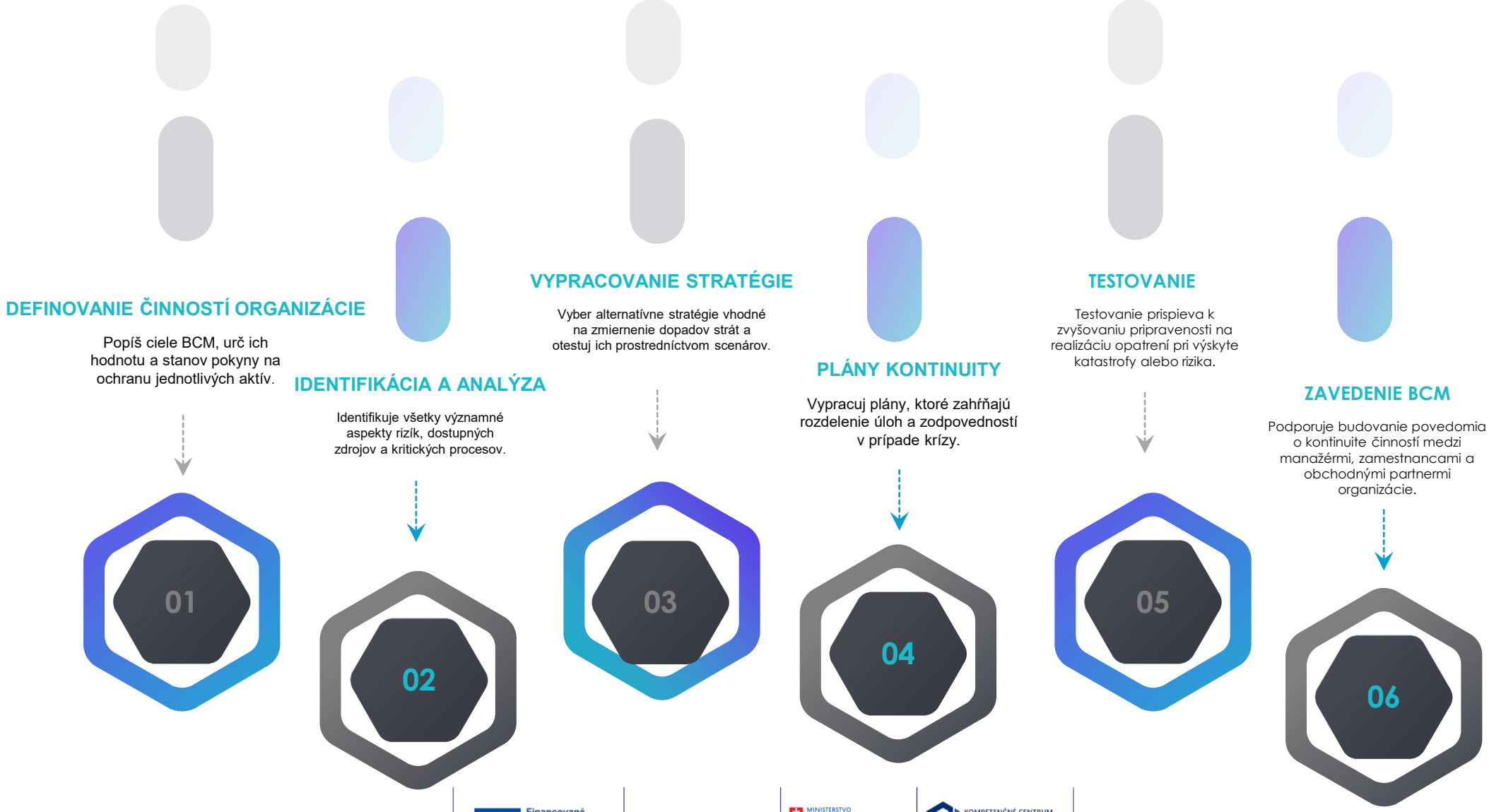


Základné normy a dokumenty na kontinuitu činností?

- **Oblasť riadenia bezpečnosti informácií – rada ISO/IEC 27000**
  - 📘 ISO/IEC 27001:2022 – základná norma pre systém manažérstva informačnej bezpečnosti (ISMS).
    - **Opatrenie A.5.29** – „Riadenie kontinuity informačnej bezpečnosti“.
    - Organizácia musí plánovať a zaviesť opatrenia, ktoré umožnia ochranu a obnovu informácií aj počas incidentov.
  - 📘 **ISO/IEC 27031:2011** – špecifická smernica pre kontinuitu informačných a komunikačných technológií (IKT).
    - Návod, ako pripraviť IT systémy na podporu celkovej kontinuity organizácie.
- **Oblasť celkového riadenia kontinuity organizácie – BCM**
  - 📘 ISO 22301:2019 – norma pre Systém manažérstva kontinuity činností (BCMS).
    - Určuje, ako má organizácia plánovať, zavádzať a udržiavať schopnosť obnovy kľúčových činností po narušení.
    - Tvorba štandardov a usmernení pre informačnú bezpečnosť
- NIST (National Institute of Standards and Technology)
  - 📘 NIST SP 800-34 – Príručka pre kontingenčné plánovanie IT systémov (revízia 1)
    - Pokyny pre obnovu IT služieb po incidente
    - Kontingenčné plánovanie = Dočasné opatrenia na obnovenie IT služieb

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

Kontinuita činnosti v krokoch



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

Základné termíny z BCM

- **Maximálne akceptovateľný výpadok** (**MAO** - Maximum Acceptable Outage) doba, počas ktorej môžu pretrvávať nepriaznivé dopady, ktoré môžu narastať v dôsledku neposkytovania produktu/služby alebo nevykonávania činnosti, než sa stanú neakceptovateľnými
  - POZNÁMKA: Pozri tiež maximálne prijateľnú dobu narušenia.
- **Maximálna prípustná doba narušenia** (**MTPD** - Maximum Tolerable Period of Disruption) doba, počas ktorej môžu pretrvávať nepriaznivé dopady, ktoré môžu narastať v dôsledku neposkytovania produktu/služby alebo nevykonávania činnosti, než sa stanú neakceptovateľnými.
- **Maximálne prípustné prerušenie činnosti** (**MTD** Maximum Tolerable Downtime) - Maximálna doba, počas ktorej môže byť proces prerušený bez nezvratných škôd (NIST).
- **Cieľový bod obnovy** (**RPO** - Recovery Point Objective) bod, k ktorému musia byť informácie používané pri činnosti obnovy obnovené, aby po opätovnom spustení prevádzky mohla byť činnosť vykonaná.
  - POZNÁMKA: Tento termín môže byť tiež formulovaný ako „maximálna strata dát“.
- **Cieľ doby obnovy** (**RTO** - Recovery Time Objective) časový interval po incidente, v rámci ktorého musí byť: produkt alebo služba obnovená, alebo činnosť obnovená, alebo zdroje nahradené.
  - POZNÁMKA: Pri produktoch, službách a činnostiach musí byť cieľ doby obnovy kratší, než doba pôsobenia nepriaznivého dopadu, ktorý znemožňuje poskytovanie produktov/služieb alebo vykonávanie činností, ktoré by sa stali neakceptovateľnými.

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

Rozdiel medzi MAO a MTPD

Kritérium	**MAO (Maximum Acceptable Outage)**	**MTPD/MTD (Maximum Tolerable Period of Disruption / Maximum Tolerable Downtime)**
Povaha pojmu	Strategický pojem	Operatívny technický pojem
Čo vyjadruje	Ako dlho si organizácia ešte môže dovoliť neprerušené fungovanie bez zásadného poškodenia.	Koľko maximálne môže trvať prerušenie činnosti konkrétneho procesu, kým dôjde k vážnym následkom.
Úroveň	Strategická – celková akceptácia prerušenia.	Taktická – konkrétny čas na obnovu daného procesu.
Použitie	Skôr pri hodnotení celkovej kritickosti organizácie.	Pri plánovaní obnovy jednotlivých procesov (napr. výroba, IT podpora).
Pojmové prepojenie	Hovorí o prijateľnosti dôsledkov.	Hovorí o maximálnom povolenom čase prerušenia.

🎯 Poznámka: MAO sa používa skôr na úrovni celkového manažmentu rizík.
MTPD/MTD sa využíva pri praktickom plánovaní obnovy konkrétnych procesov a nastavení cieľov obnovy v BIA (Business Impact Analysis).

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

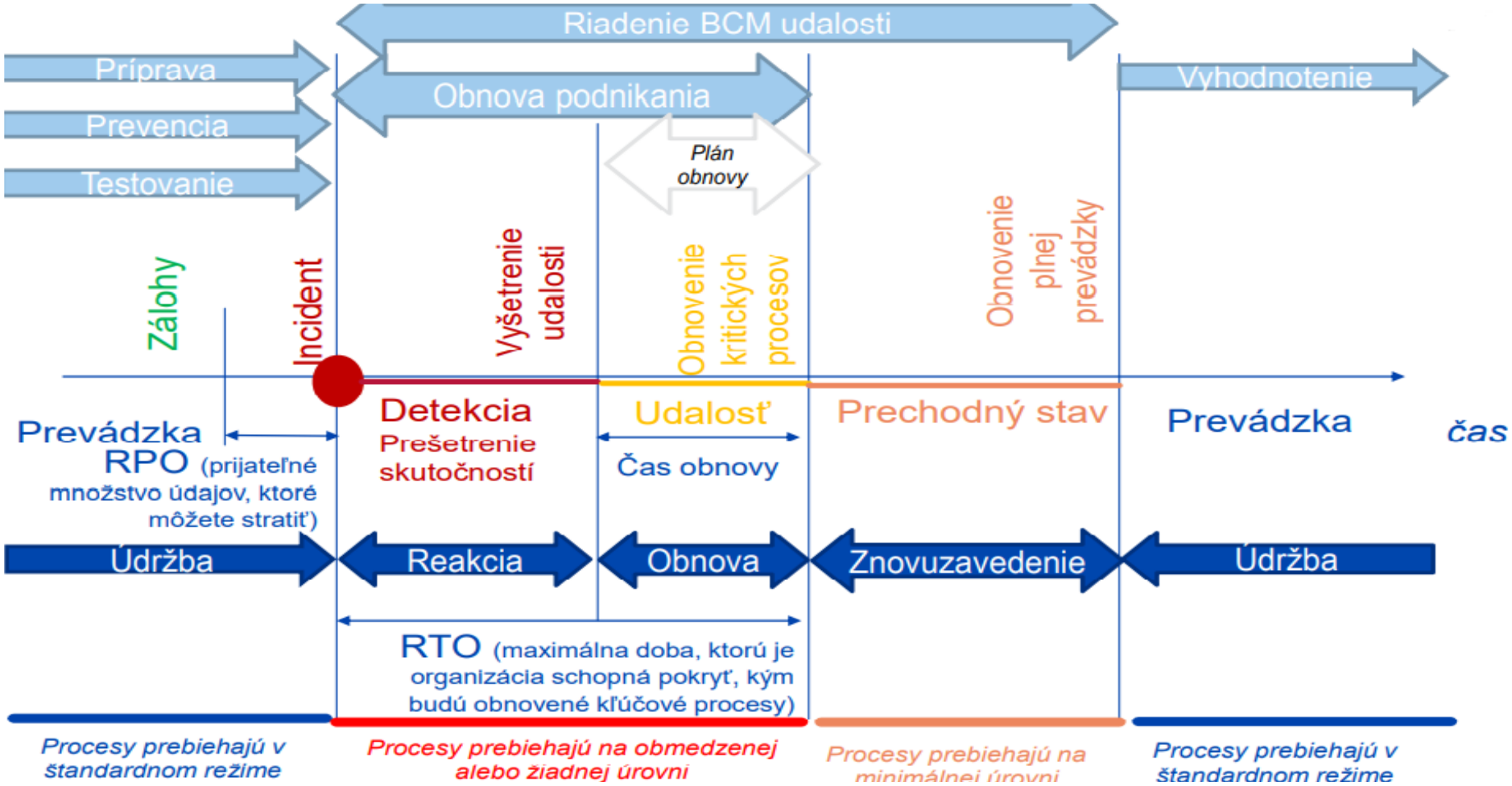
Rozdiely medzi pojmami ako RPO, RTO, MTPD a MAO

Parameter	Hodnota	Vysvetlenie
Parameter	1 hodina	Koľko dát môžeme maximálne stratiť. V tomto prípade sa dáta zálohujú každú hodinu – ak dôjde k incidentu, stratíme maximálne hodinu záznamov.
RPO (Recovery Point Objective)	4 hodiny	Ako rýchlo musíme obnoviť IT systém, aby nemocnica mohla ďalej fungovať. Máme teda 4 hodiny na technickú obnovu systému.
RTO (Recovery Time Objective)	6 hodín	Ako dlho môže byť systém prerušený, kým nastanú vážne dopady (napr. ohrozenie zdravia pacientov, právne následky).
MTPD (Maximum Tolerable Period of Disruption)	6 / 12 hodín	Širší, strategickejší pohľad: nemocnica si môže určiť, že maximálny výpadok pre rôzne služby je napr. 6 alebo až 12 hodín.

Časová os:
◄— RPO (1h) —► INCIDENT —► RTO (4h) —► MTPD/MAO (6h)

◄— RPO (1h) —► INCIDENT —► RTO (4h) —► MTPD (6h) —► MAO (12h)

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


Riadenie BCM udalosti
Príprava
Prevencia
Testovanie
Obnova podnikania
Vyhodnotenie
Plán obnovy
Zálohy
Incident
Vyšetrenie udalosti
Obnovenie kritických procesov
Obnovenie plnej prevádzky
Detekcia
Prešetrenie skutočností
Udalosť
Prechodný stav
Prevádzka
čas
Prevádzka
RPO (prijateľné množstvo údajov, ktoré môžete stratiť)
Čas obnovy
Údržba
Reakcia
Obnova
Znovuzavedenie
Údržba
RTO (maximálna doba, ktorú je organizácia schopná pokryť, kým budú obnovené kľúčové procesy)
Procesy prebiehajú v štandardnom režime
Procesy prebiehajú na obmedzenej alebo žiadnej úrovni
Procesy prebiehajú na minimálnej úrovni
Procesy prebiehajú v štandardnom režime

Business Impact Analysis

- Systematický proces identifikácie kritických procesov a hodnotenia dôsledkov ich prerušenia.
- Základný kameň plánovania kontinuity činností (BCP) a plánovania obnovy po incidente.
- **BIA je proces identifikácie činností a hodnotenia ich dopadov v prípade prerušenia, ktoré by mohlo narušiť schopnosť organizácie fungovať (ISO 22300).**

Cieľ: Minimalizovať dopady na organizáciu pri výpadku IT služieb alebo kybernetickom incidente.

Kľúčové body BIA

- Cieľ BIA
  - Určiť, ktoré činnosti sú kľúčové pre prežitie a kontinuitu organizácie
    - Zhodnotiť, aké následky (finančné, právne, reputačné, prevádzkové,...) by malo ich prerušenie
    - Stanoviť priority obnovy a potrebné zdroje
- Výstupy BIA
  - Zoznam kritických procesov a služieb
  - RTO, RPO, MTPD,...
  - Odporúčanie pre tvorbu plánov kontinuity činností (BCP)
- Proces BIA zahŕňa
  - Identifikáciu kľúčových činností a závislostí.
  - Určenie kritických zdrojov (personál, IT, infraštruktúra, dodávatelia)
  - Odhad časového a finančného dopadu prerušenia.
  - Návrh opatrení na zmiernenie rizík

Príklad CloudServis, s. r. o.

Profil organizácie:

- Spoločnosť **CloudServis, s. r. o.** je poskytovateľom cloudových riešení typu **SaaS (Software as a Service)** a **PaaS (Platform as a Service)**. Zabezpečuje cloudovú platformu pre stovky firemných klientov. Medzi hlavné služby patrí **zákaznícky portál**, prostredníctvom ktorého môžu klienti: spravovať svoje cloudové prostredie, pristupovať k dátam, konfigurovať poskytované služby.

Realizácia Business Impact Analysis (BIA):

- V rámci implementácie systému manažérstva kontinuity činností podľa ISO 22301 vykonala spoločnosť CloudServis podrobnú analýzu dopadov na podnikanie (BIA). Cieľom bolo identifikovať kritické procesy, stanoviť maximálne tolerované prestoje a navrhnúť vhodné stratégie.

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

Identifikácia a určenie kľúčových procesov

Proces	Popis činnosti	Dôsledky prerušenia	Priorita	Dôvod priority	Závislosti
Prevádzka zákazníckeho portálu	Klienti cez portál spravujú služby a dáta	Okamžité výpadky služieb klientov	🟥 Vysoká	Portál je hlavné rozhranie pre všetky služby	Cloud infraštruktúra, IAM, databázy, vývojový tím
Dostupnosť cloudovej infraštruktúry	Hosting aplikácií, služieb a databáz	Nefunkčné aplikácie klientov	🟥 Vysoká	Kľúčová vrstva – bez nej nič nefunguje	Napájanie, sieťové pripojenie, hardvér, virtualizačné platformy
Správa prístupov (IAM)	Zabezpečuje, kto a ako sa môže prihlásiť	Riziko zneužitia alebo nedostupnosti účtov	🟧 Stredná	Kritické pre bezpečnosť, ale má záložné mechanizmy	Adresárové služby (LDAP), autentifikačné servery, sieťová bezpečnosť
Monitoring a incident management	Detekcia výpadkov, útokov, riešenie incidentov	Nezistené chyby a oneskorené reakcie	🟧 Stredná	Zásadné pre rýchle riešenie, ale chvíľu môže byť nefunkčné	Monitorovacie nástroje, logovanie, tím IT bezpečnosti
Zálohovanie a obnova dát	Ochrana proti strate dát	Neobnoviteľné dáta, porušenie zmlúv	🟨 Stredná až nízka	Dôležité pri dlhších výpadkoch – nevyžaduje okamžité obnovenie	Zálohovací softvér, záložné servery, cloud storage
Technická podpora	Komunikácia s klientmi pri problémoch	Nespokojnosť, sťažnosti	🟨 Stredná až nízka	Klient môže chvíľu čakať – nie je to technické jadro systému	Helpdesk nástroje, komunikačné platformy, školený personál

Identifikované procesy v spoločnosti CloudServis, s. r. o.

Identifikácia kritických činností:

- **Prevádzka zákazníckeho portálu** - označený ako **kritická služba**, pretože:
  - Slúži na správu objednávok, konfiguráciu služieb a komunikáciu s klientmi.
  - Je priamym rozhraním medzi spoločnosťou a jej zákazníkmi.

Analýza dopadov prerušenia služby:

- Simuláciou rôznych scenárov sa zistilo, že:
  - Výpadok portálu dlhší ako 2 hodiny vedie k vážnym následkom:
  - Zvýšenému počtu sťažností a odchodov klientov ku konkurencii.
  - Okamžitému negatívnemu vplyvu na reputáciu spoločnosti (napr. negatívne recenzie, medializácia problému).
  - Riziku nesplnenia SLA (Service Level Agreements) s kľúčovými zákazníkmi, čo by mohlo viesť k zmluvným pokutám.

Príklad: BOMBOVÝ ÚTOK

- 1. **Scenár nie je „útok“ – ale jeho následky**
  - BCM a BIA nehodnotia „útok ako taký“, ale **dopad útoku na kritické procesy**.
- 🔍 **Čo skúmame v simulácii scenára?**
  - Bombový útok – evakuácia budovy – zamestnanci nemôžu pracovať – prístup do systémov je prerušený.
- 🔽 Simuluješ napríklad:

Trvanie vplyvu	Dopady na proces	Možnosti riešenia
2 hodiny	Meškanie služieb, chaos v podpore	Presmerovanie ticketov, prístup z domu
1 deň	Výpadok zákazníckeho portálu (nikto ho nespravuje)	Aktivácia krízového tímu, záložné miesto
3 dni	Masívne sťažnosti, strata klientov	Externá podpora, presun na záložnú lokalitu
1 týždeň	Dlhodobá reputačná a finančná škoda	Plán obnovy činnosti, náhradné kapacity

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

Stanovenie obnovovacích cieľov (RTO, RPO, MTPD)

- Na základe simulácie nastavujeme limity obnovy:
  - RTO (Recovery Time Objective) = do kedy musíme obnoviť činnosť, inak budú vážne škody, napr. „**portál musí byť obnovený do 2 hodín**“
  - RPO (Recovery Point Objective) = koľko dát si môžeme dovoliť stratiť, napr. „maximálna dátová strata je 15 minút **– zálohovanie každú štvrťhodinu**“
  - MTPD (Maximum Tolerable Period of Disruption) = najdlhší prípustný výpadok, napr. „1 deň je najdlhšia prípustná strata bez definitívnej škody“

- Na základe BIA teraz vieme*:*
  - čo je kritické,
  - čo ho ohrozuje,
  - ako rýchlo to musíme obnoviť.

Parameter	Vysvetlenie	Čas
RTO (Recovery Time Objective)	Do tohto času to ešte vieme „ustáť“ – musíme stihnúť obnoviť	✅ **2 hodiny**
MTPD (Maximálne prípustný výpadok)	Za touto hranicou sú dôsledky už neakceptovateľné	napr. na slide 16 uvažujem 1 deň – musí to byť odôvodnené)

Návrh a implementácia opatrení na základe BIA

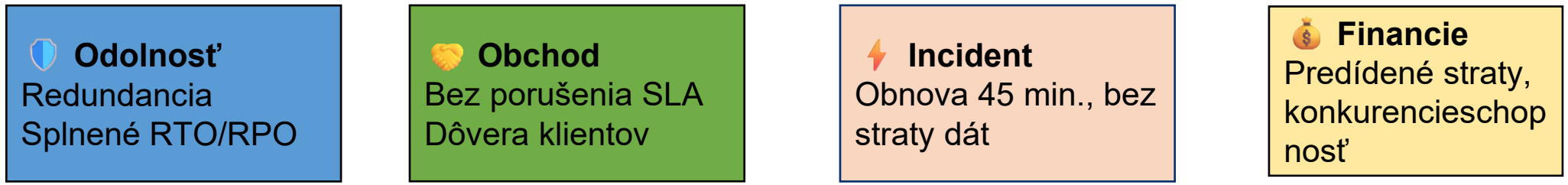
- Na základe výsledkov analýzy dopadov spoločnosť prijala nasledovné **opatrenia kontinuity a preventívne opatrenia**:

1. **Redundantná infraštruktúra:**
    1. Zavedenie **geograficky oddeleného sekundárneho dátového centra** s možnosťou automatického prepnutia (failover) v prípade zlyhania primárneho servera.
    2. Implementácia riešenia **High Availability (HA)** pre databázový server.
2. **Zálohovacie politiky:**
    1. Nastavenie pravidelného **inkrementálneho zálohovania každých 10 minút**.
    2. Zálohy sú replikované do bezpečného offsite úložiska v reálnom čase.
3. **Testovanie a overovanie:**
    1. Zavedenie pravidelných **testov obnovy** (Disaster Recovery Testing) na overenie splnenia RTO a RPO.
    2. Školenie IT personálu na postupy rýchlej obnovy služieb.
4. **Úprava SLA a komunikácie:**
    1. Aktualizácia SLA s klientmi vrátane garantovaných časov obnovy.
    2. Príprava **krízového komunikačného plánu** pre prípad dlhšieho výpadku

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

Opatrenia v spoločnosti CloudServis, s.r.o.

- Príklad ako by to vyzeralo pri incidente po implementáciu opatrení po BIA
  - **Zvýšenie odolnosti voči výpadkom**
    Redundancia a automatizovaná obnova minimalizovali dopad incidentov. Splnené RTO (1 hod.) a RPO (15 min.).
  - **Úspešné zvládnutie incidentu**
    Pri zlyhaní hardvéru prebehlo automatické prepnutie (failover) a obnova databázy do 15 minút bez straty dát.
  - **Ochrana obchodných záujmov**
    Bez porušenia SLA, zachovaná dôvera klientov, žiadne reputačné škody.
  - **Finančné a strategické prínosy**
    Predídené straty a sankcie, posilnenie konkurencieschopnosti vďaka vysokej úrovni odolnosti.



Rozdiel medzi BIA a Risk Assessment (posúdením rizík)

1️⃣ Risk Assessment (v zákone Analýza rizík)

- **Cieľ:** Identifikovať riziká = kombináciu:
  - **Hrozba (threat)**
  - **Zraniteľnosť (vulnerability)**
  - **Dopad (impact)**
- **Dopad v RA:**
  Hodnotíš, **čo sa stane, ak sa hrozba zrealizuje**.
  Tento dopad je súčasťou výpočtu rizika (**Riziko = Pravdepodobnosť × Dopad**).
- **Príklad:**
  Hrozba: Ransomvér.
  Zraniteľnosť: Slabé zálohovanie.
  Dopad: Strata prístupu k dátam, finančná strata 50 000 €.
  ➡️ Výsledok: Vysoké riziko, treba zaviesť opatrenia.

✅ **Posúdenie rizík sa teda zameriava na to, aby sme vedeli, kde je riziko príliš vysoké a musíme ho znížiť vo vzťahu k súčastiam procesu (závislostiam).**

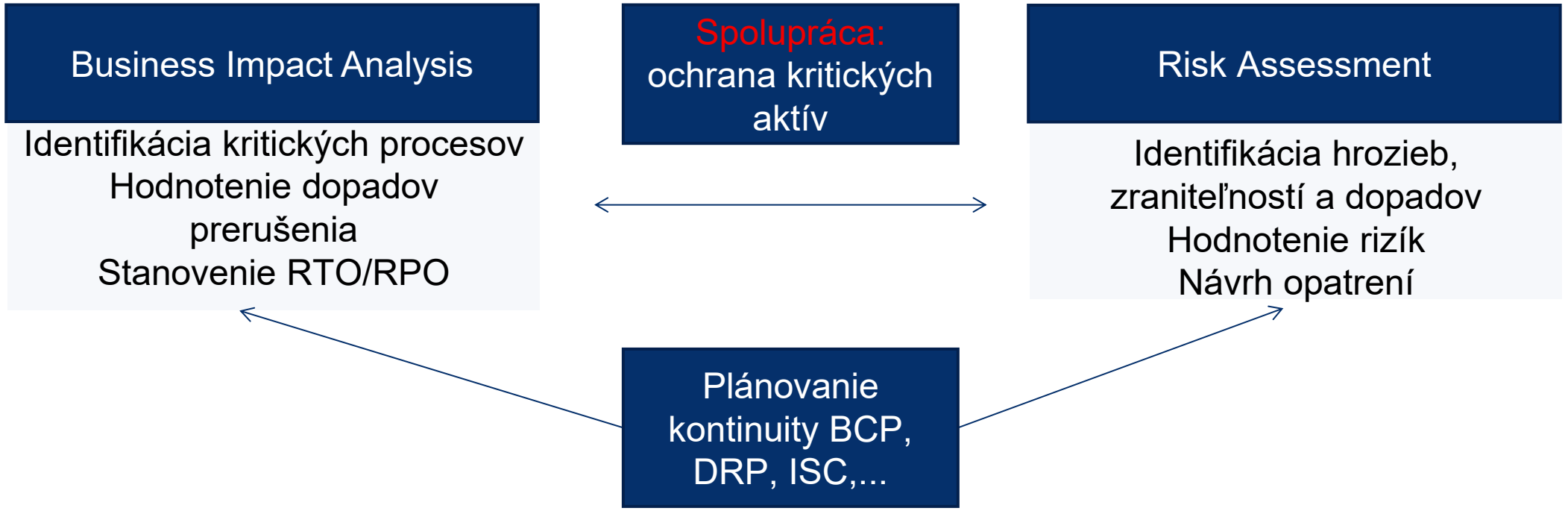
2️⃣ Business Impact Analysis (BIA)

- **Cieľ:** Hodnotiť **dopady PRERUŠENIA** kritických procesov, **nezávisle od príčiny**.
- V BIA sa nepýtaš, aká hrozba spôsobí výpadok – ty **už počítaš s tým, že výpadok nastane**.
- **Dopad v BIA:**
  - Aké budú následky na biznis, ak určitý proces alebo služba prestane fungovať (bez ohľadu na to, či to bol ransomware, DDoS, zlyhanie systému alebo požiar)?
  - Stanovíš časové limity (MTPD, RTO, RPO) a priority obnovy.
- **Príklad:**
  Proces: E-shop.
  Čo ak vypadne?
  - Po 3 hodinách prichádzame o 20 % tržieb denne, po 1 dni hrozí odchod klientov.
  - Bez ohľadu na to, či výpadok spôsobila kybernetická hrozba alebo technická porucha.

✅ **BIA sa teda zameriava na plánovanie obnovy a kontinuitu – aké následky budú mať prestoje/prerušenia, nech už sú dôvody akékoľvek.**

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

Prepojenie Business Impact Analysis a Risk Assesment



🚒 Príklad – Požiar serverovne

Risk Assessment	BIA
Hrozba: Požiar	Proces: IT infraštruktúra (serverovňa)
Zraniteľnosť: Nedostatočná protipožiarna ochrana	Otázka: „Čo sa stane, keď serverovňa vypadne?“
Dopad: Zničenie hardvéru, výpadok služieb, strata dát	Odpoveď: Po 2 hodinách výpadku prichádzame o klientov
➡️ Riešenie: Zlepšiť ochranu, zaviesť detekciu požiaru	➡️ Riešenie: Pripraviť záložné riešenie a plán obnovy

Risk Assessment	BIA
Vieš, čo je ohrozené	Vieš, čo je kritické
Vieš, aké sú pravdepodobné hrozby	Vieš, aký bude dopad výpadku
Pomáha určiť priority ochrany	Pomáha určiť priority obnovy
➡️ „Čo spôsobí, že to vypadne?“	➡️ „Čo nemôže vypadnúť?“

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

Ako nastaviť hodnotenie dopadov tak, aby to ladilo

Úroveň dopadu	Popis v BIA	Popis v analýze rizík
Nízka	Nepodstatný výpadok, klienti si nevšimnú	Dopad do 1 000 € alebo interná nepríjemnosť
Stredná	Obmedzenie služieb, drobné sťažnosti	Finančný dopad do 10 000 €, mierne poškodenie dôvery
Vysoká	Výpadok hlavnej služby, reputačné škody	Zmluvné pokuty, strata klientov, > 50 000 €
Kritická	Ohrozenie celej firmy	Porušenie zákona, dlhodobá nefunkčnosť

🧩 **Prečo sa to má zladiť?**
Aby sa nestalo, že v BIA povieš, že výpadok portálu je „vysoký dopad“, ale v analýze rizík sa ten istý výpadok zhodnotí ako „nízky dopad“. **To by narušilo konzistenciu plánovania.**

Štandardný postup BIA pozostáva z týchto krokov

KROK 1: Príprava a plánovanie BIA

- ✅ **Čo sa robí:**
  - Definuje sa **účel a rozsah BIA**.
  - Určí sa tím alebo zodpovedné osoby (typicky bezpečnostný manažér, IT, prevádzka).
  - Pripravia sa nástroje – dotazníky, interview formuláre, šablóny.
- ✅ **Cieľ:**
  - Vedieť PREČO BIA robíme a KTORÝCH PROCESOV sa týka (napr. celá firma, alebo len IT služby).

- 🎓 **Príklad:** Firma rozhodne, že BIA bude pokrývať len kľúčové procesy v oblasti zákazníckej podpory a logistiky.

Štandardný postup BIA pozostáva z týchto krokov

KROK 2: Identifikácia kľúčových činností a procesov

✅ Čo sa robí:

- Zozbierajú sa všetky hlavné procesy organizácie.
- Určia sa tie, ktoré sú **kritické pre fungovanie** (bez ktorých by organizácia utrpela vážne škody).

✅ Ako sa to robí:

- Rozhovory s vedúcimi oddelení.
- Dotazníky pre zmapovanie procesov.
- Analýza závislostí (napr. IT systémy, dodávatelia, personál).

🎓 **Príklad:** V e-shope sú identifikované procesy:

- **Spracovanie objednávok** (kritické).
- **Marketingové kampane** (nekritické v krátkodobom horizonte).

Štandardný postup BIA pozostáva z týchto krokov

KROK 3: Hodnotenie dopadov prerušenia činností

✅ Čo sa robí:

- **Pre každý kritický** proces sa posudzuje:
  - **Aké budú dopady, ak sa preruší?**
  - Po akej dobe začne byť výpadok kritický?

✅ Metóda:

- Použitie škály (napr. zanedbateľný – nízky – stredný – závažný - katastrofický).
- Vyčíslenie finančných strát, ak je to možné.
- Časové hodnotenie dopadov

- ✅ **Typy dopadov: Finančný, prevádzkový, dopad na súlad, reputačný, dopad na bezpečnosť a zdravie (v špecifických odvetviach),...**

Opis dopadu	Finančný dopad	Prevádzkový dopad	Dopad na súlad	Reputačný dopad
Zanedbateľný	Žiadny	Interne jeden útvar	Zlyhanie interného procesu	Určité prekážky v komunikácii v rámci organizácie
Nízky	<5 000 €	Interne viacero útvarov	Zlyhanie kritických procesov	Prekážky v komunikácii v rámci organizácie
Stredný	5 000 – 10 000 €	Organizácia, malá časť zamestnancov a študentov	Začatie správneho konania smerujúce k opatreniu na nápravu	Závažné prekážky v externej komunikácii
Závažný	10 000 – 100 000 €	Organizácia, značná časť zamestnancov a študentov	Začatie správneho konania smerujúce k uloženiu pokuty	Nepriaznivá publicita, prípadne na národnej úrovni
Katastrofický	>100 000 €	Organizácia, všetci zamestnanci a študenti	Pozastavenie časti služieb/ukončenie činnosti	Intenzívna nepriaznivá publicita na národnej alebo medzinárodnej úrovni

Štandardný postup BIA pozostáva z týchto krokov

KROK 3: Hodnotenie dopadov prerušenia činností

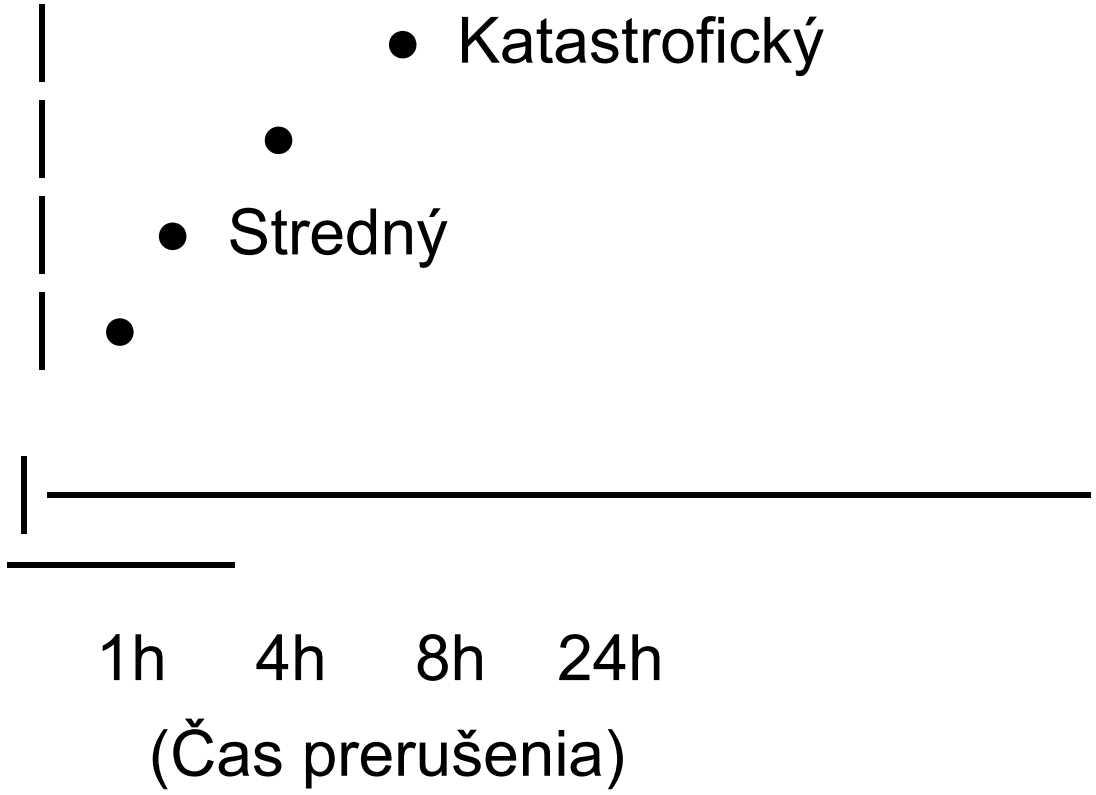
Proces	Dopad po 1h	Vysvetlenie	Dopad po 4h	Vysvetlenie	Dopad po 24h	Vysvetlenie
Spracovanie objednávok	Nízky	Krátkodobý výpadok, klienti si nevšimnú	Stredný	Prvé sťažnosti, meškanie objednávok	Katastrofický	Strata klientov, veľké finančné straty
Interná administratíva	Žiadny	Výpadok bez vplyvu na prevádzku	Nízky	Menšie vnútorné obmedzenia	Stredný	Zníženie efektivity, oneskorenie interných úloh
IT Helpdesk	Žiadny	Bežné požiadavky počkajú	Nízky	Zvýšená nespokojnosť zamestnancov	Stredný	Závažné sťažnosti, narušenie vnútornej podpory
Fakturácia	Žiadny	Bez vplyvu, fakturácia nie je urgentná	Žiadny	Stále bez výrazného dopadu	Nízky	Mierne oneskorenie platieb
Zákaznícka podpora	Nízky	Klienti čakajú dlhšie na odpovede	Stredný	Sťažnosti, riziko eskalácie	Závažný	Strata dôvery zákazníkov

Štandardný postup BIA pozostáva z týchto krokov

KROK 3: Hodnotenie dopadov prerušenia činností

1. Pre každý proces sa vytvorí časový profil dopadov.

2. Na základe toho sa určí MTD a RTO.
   - Ak napr. po 8 hodinách dopad presiahne "Závažný", nastaví sa **MTD = 8 hodín**.
   - RTO je stanovené o niečo nižšie, aby bol čas na obnovu.



Štandardný postup BIA pozostáva z týchto krokov

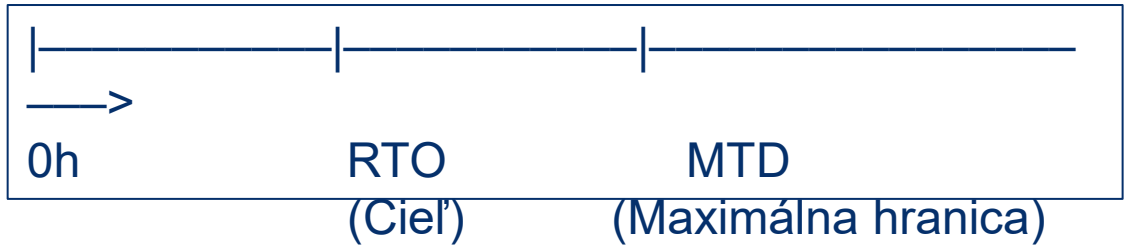
KROK 4: Stanovenie MTD, RTO a RPO

✅ **Pojmy:**

- **MTD (Maximum Tolerable Downtime):**
  - Maximálna doba, počas ktorej môže byť proces prerušený **bez nezvratných škôd**.
- **RTO (Recovery Time Objective):**
  - Cieľová doba, za ktorú musíme obnoviť činnosť.
- **RPO (Recovery Point Objective):**
  - Maximálna prijateľná strata dát (koľko starých dát môžeme pri obnove „stratiť“).

✅ **Príklad:**

- Proces: **Spracovanie objednávok**
  - MTD = 24 hodín
  - RTO = 8 hodín
  - RPO = 30 minút



➡️ Znamená to, že proces musí byť obnovený do 8 hodín, pričom nesmieme stratiť viac ako 30 minút dát.

Štandardný postup BIA pozostáva z týchto krokov

KROK 5: Identifikácia závislostí a potrebných zdrojov

✅ **Čo sa robí:**

- Pre každý kritický proces sa určí:
  - Na akých **systémoch**, **dodávateľoch**, **ľuďoch** a **infraštruktúre** závisí.
  - Aké sú potrebné **minimálne zdroje** na fungovanie v núdzovom režime.

🎓 **Príklad:** Proces spracovania objednávok závisí od:

- ERP systému.
- Pripojenia na internet.
- Externého logistického partnera.

✅ **Proces:** Spracovanie objednávok (e-shop)

- Nestačí vedieť, **čo je kritický proces**, ale aj **od čoho všetkého závisí**.
- Zároveň si musíme uvedomiť, že v prípade incidentu sa neobnovuje plná prevádzka, ale **len kľúčové zdroje**, ktoré zabezpečia základnú funkčnosť.

Štandardný postup BIA pozostáva z týchto krokov

KROK 5: Identifikácia závislostí a potrebných zdrojov

Oblasť	Závislosti	Minimálne zdroje pre núdzový režim
Systémy	ERP systém, databáza, e-shop portál	Záložný server alebo cloud prístup
Dodávatelia	Logistický partner, poskytovateľ IT infraštruktúry	Dohoda o prioritnom režime, hotline podpora
Ľudia	2 pracovníci zákazníckej podpory, 1 IT technik	Minimálne 1 pracovník + IT technik on-call
Infraštruktúra	Internet, elektrina, kancelárske priestory	Záložné pripojenie (LTE), UPS, home office

Štandardný postup BIA pozostáva z týchto krokov

KROK 6: Určenie priorít obnovy

- V prípade výpadku nemôžeme všetko obnoviť naraz. Musíme sa rozhodnúť:
  - „Ktoré procesy a systémy sú také dôležité, že musia fungovať ako prvé?“Je to ako pri riešení havárie – najprv riešiš najkritickejšie oblasti, ktoré priamo ohrozujú chod organizácie.

✅ Čo teda sa robí:

- Na základe všetkých údajov sa zostaví **poradie priorít**, ktoré procesy a systémy obnovovať ako prvé.

🎓 Príklad:

1. Obnoviť ERP systém.
2. Zabezpečiť prístup k databáze klientov.
3. Až potom obnoviť internú e-mailovú komunikáciu.

Štandardný postup BIA pozostáva z týchto krokov

KROK 7: Dokumentácia a odporúčania

✅ Čo sa robí:

- Výsledky BIA sa zapíšu do prehľadného dokumentu.
- Odporúčania pre:
  - Plány kontinuity (BCP, DRP).
  - Investície do odolnosti.
  - Návrhy na testovanie a zlepšovanie.

🎓 Príklad:

- Záznam: „Proces X musí byť obnovený do 4 hodín, odporúčame zaviesť záložný server a zmluvne ošetriť SLA s dodávateľom.“

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

Štandardný postup BIA pozostáva z týchto krokov

Ako určiť MTD (Maximum Tolerable Downtime)?

- **MTD = Maximálna doba, počas ktorej môže byť proces prerušený bez nezvratných škôd.**
- **Postup:**
  - **Analyzuj dopady výpadku v čase** (presne ako v tvojej tabuľke – po 1h, 4h, 24h, atď.).
  - Zisti, **kedy dopad dosiahne úroveň "neakceptovateľný"**:
    1. Kedy by vznikli právne následky (pokuty, porušenie zmlúv)?
    2. Kedy by firma začala strácať zákazníkov?
    3. Kedy by reputácia utrpela zásadný zásah?
- MTD je ten bod, kedy by výpadok **spôsobil zásadnú stratu alebo ohrozenie existencie**.

Štandardný postup BIA pozostáva z týchto krokov

Ukážkový príklad (firma eShopServis, s.r.o.)

Proces	Činnosť	Kritickosť	MTD	RTO	RPO	Dopad výpadku	Závislosti
Spracovanie objednávok	Prijatie objednávky	Vysoká	4 hodiny	1 hodina	15 min	Strata tržieb, nespokojnosť klientov	Webový portál, databáza
Spracovanie objednávok	Overenie platby	Stredná	8 hodín	4 hodiny	30 min	Meškanie spracovania objednávok	Bankové API
Spracovanie objednávok	Generovanie faktúr	Nízka	48 hodín	24 hodín	1 hodina	Administratívne oneskorenie	ERP systém
Zákaznícka podpora	Prijímanie reklamácií	Vysoká	6 hodín	2 hodiny	30 min	Riziko právnych problémov	Helpdesk systém
Marketing	Odosielanie newsletterov	Nízka	5 dní	2 dni	1 deň	Minimálny dopad	E-mailová platforma

Štandardný postup BIA pozostáva z týchto krokov

BIA – analýza dopadov

Proces / Systém	Kritickosť	Dopad po 1h	Dopad po 4h	Dopad po 24h	MTD	RTO	RPO	Závislosti	Minimálne zdroje	Priorita obnovy	Dôvod priority
ERP systém	Vysoká	Nízky	Stredný	Katastrofický	24 hodín	8 hodín	30 min	Databáza, internet	Záložný server, pripojenie	1	Kľúčový pre objednávky a fakturáciu
Databáza klientov	Vysoká	Nízky	Stredný	Závažný	36 hodín	12 hodín	1 hodina	ERP, cloud	Záloha databázy, cloud prístup	2	Bez nej nemožno obslúžiť zákazníkov
Zákaznícka podpora	Stredná	Žiadny	Nízky	Stredný	48 hodín	24 hodín	2 hodiny	Helpdesk systém	1 pracovník, telefón	3	Potrebná na riešenie problémov klientov
E-mailová komunikácia	Nízka	Žiadny	Žiadny	Nízky	72 hodín	48 hodín	4 hodiny	Internet	Telefón, osobná komunikácia	4	Podporný systém, dá sa nahradiť alternatívami
Marketingový systém	Nízka	Žiadny	Žiadny	Žiadny	5 dní	3 dni	1 deň	Interné dáta	Nie je potrebný v núdzovom režime	5	Neohrozuje prevádzku, môže byť obnovený neskôr

Štandardný postup BIA pozostáva z týchto krokov

Checklist: Postup podľa ISO 22301

Krok podľa ISO 22301	Hotovo?	Poznámka / Čo skontrolovať
1️⃣ **Stanovenie kontextu organizácie**	✅ / ❌	Máš definované ciele BCM, interné a externé faktory, požiadavky zainteresovaných strán?
2️⃣ **Identifikácia kritických činností (BIA)**	✅ / ❌	Máš spracovanú BIA – analýzu dopadov na podnikanie
3️⃣ **Posúdenie rizík (Risk Assessment)**	✅ / ❌	Identifikácia hrozieb, zraniteľností a hodnotenie rizík pre kritické procesy
4️⃣ **Návrh stratégie kontinuity**	✅ / ❌	Stanovenie, ako zabezpečíš fungovanie počas prerušenia
5️⃣ **Vypracovanie plánov (BCP, DRP, ISCP)**	✅ / ❌	Vytvorenie konkrétnych plánov reakcie a obnovy
6️⃣ **Definovanie rolí a zodpovedností**	✅ / ❌	Určené tímy, zodpovednosti, kontakty
7️⃣ **Komunikačný plán**	✅ / ❌	Interná a externá komunikácia počas incidentov
8️⃣ **Testovanie a cvičenia**	✅ / ❌	Plánovanie a realizácia testov a simulácií
9️⃣ **Revízia, audit, zlepšovanie**	✅ / ❌	Pravidelná kontrola, aktualizácia a neustále zlepšovanie
🔟 **Dokumentácia a evidencia**	✅ / ❌	Všetky dokumenty riadne uložené, spravované a schválené vedením

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

Čo je stratégia kontinuity?

- Stratégia kontinuity definuje **AKO** bude organizácia zabezpečovať fungovanie svojich kritických činností počas a po narušení (výpadku, incidente, katastrofe).

- **Cieľ:** Minimalizovať dopady prerušenia a zabezpečiť, že kritické procesy budú obnovené v rámci stanovených MTD, RTO a RPO.

Príklad hlavných stratégií kontinuity

1️⃣ Záložné riešenia (Alternate Solutions)

➡️ **Popis:** Zabezpečenie alternatívnych technických a prevádzkových kapacít, ktoré umožnia pokračovať v kritických činnostiach pri výpadku hlavných systémov alebo pracovísk.

✅ **Typy riešení:**

IT oblasti:

- **Hot site** – plne pripravené záložné dátové centrum (okamžité prepnutie).
- **Warm site** – čiastočne pripravené, vyžaduje čas na aktiváciu.
- **Cold site** – prázdna lokalita, kde je potrebné všetko nainštalovať.
- **Cloud DR (Disaster Recovery)** – obnova v cloude.
- **Virtualizácia systémov** – flexibilné presuny prostredí.

Prevádzka:

- **Alternatívne pracoviská – zmluvne dohodnuté kancelárie.**
- **Home office – pripravená politika a technológie pre prácu na diaľku.**
- **Mobilné pracoviská – kontajnery, dočasné stanovištia.**

Príklad hlavných stratégií kontinuity

2️⃣ **Zálohovanie a obnova dát** (Backup & Recovery)

➡️ **Popis:** Zaistenie dostupnosti dát podľa požiadaviek RPO a RTO.

✅ **Kľúčové prvky:**

- Pravidelné zálohovanie (on-site aj off-site).
- Automatizovaná replikácia dát do cloudu.
- Testovanie obnovy – overenie, že zálohy sú použiteľné.
- Verzionovanie – ochrana proti ransomvéru.

3️⃣ **Dohody s dodávateľmi (Supplier Agreements)**

➡️ **Popis:** Zabezpečenie dostupnosti kľúčových služieb a tovarov aj v krízových situáciách.

✅ **Obsah stratégie:**

- SLA s garantovanou dobou dodania.
- Zmluvy o prednostnom plnení počas incidentov.
- Identifikácia náhradných dodávateľov (dual sourcing).
- Dohody o spoločnej BCM politike s partnermi.

Príklad hlavných stratégií kontinuity

4️⃣ Ľudské zdroje (People Continuity)

➡️ **Popis:** Zabezpečenie, že kľúčové činnosti budú mať dostupný personál aj v prípade nepriaznivých udalostí.

✅ **Opatrenia:**

- Definovanie kritických rolí (tím kontinuity).
- Zastupiteľnosť – školenia a rotácie pracovníkov.
- Plány pre prípad pandémie, štrajku, neprístupnosti lokality.
- Psychologická odolnosť tímov (stress management).

5️⃣ Komunikácia v kríze (Crisis Communication)

➡️ **Popis:** Efektívna výmena informácií počas incidentu, aby nedošlo k chaosu.

✅ **Nástroje a opatrenia:**

- Záložné komunikačné kanály (SMS gateway, satelitné telefóny).
- Krízové komunikačné tímy.
- Pripravené scenáre a šablóny oznámení.
- Monitoring médií a sociálnych sietí.

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

Hlavných stratégií kontinuity

6️⃣ Núdzové procesy (Manual Workarounds)

➡️ Popis:

Dočasné, manuálne alebo alternatívne postupy na zabezpečenie základného fungovania bez plnej infraštruktúry.

✅ Príklady:

- Ručné vystavovanie objednávok/faktúr.
- Telefonická komunikácia namiesto e-mailov.
- Použitie jednoduchých nástrojov (Excel namiesto ERP).
- Papierové formuláre pre evidenciu.

Prehľad plánov v BCM lady plánov

Typ plánu	Zameranie	Príklad
BCP	Pokračovanie kľúčových činností	Ako firma funguje počas výpadku
DRP	Obnova IT systémov	Obnova servera po kyberútoku
ISCP	Núdzový režim konkrétneho systému	Dočasné riešenie pri výpadku e-mailu
Crisis Communication Plan	Komunikácia počas incidentu	Informovanie klientov o výpadku
Emergency Response Plan	Okamžitá reakcia na fyzické hrozby	Evakuácia pri požiari
Pandemic Plan	Prevádzka počas zdravotnej krízy	Nastavenie home office a ochranných opatrení

Príklad zoznam krízových plánov

BCM plány pre situáciu	Vlastník krízového plánu	Pravdepodobnosť vzniku situácie	Následok situácie
Výpadok kľúčových služieb ERP systém	Oddelenie IT prevádzky	Nízka	Vysoký
Strata/poškodenie metadát/konfiguračných údajov	Vedúci technologického tímu	Stredná	Vysoký
Dlhodobý výpadok/strata kľúčových pracovníkov	Projektový Manažér	Stredná	Stredný
Strata väčšieho počtu pracovníkov	Projektový Manažér	Nízka	Vysoký
Dlhodobý/trvalý výpadok služieb ERP	Oddelenie IT prevádzky	Nízka	Vysoký
Dlhodobý/trvalý výpadok dodávateľa 1	Vedúci technologického tímu	Nízka	Vysoký
Dlhodobý/trvalý výpadok dodávateľa 2	Vedúci technologického tímu	Nízka	Vysoký
Výpadok biznis dostupnosti komponentov	Vedúci technologického tímu	Stredná	Vysoký

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

01

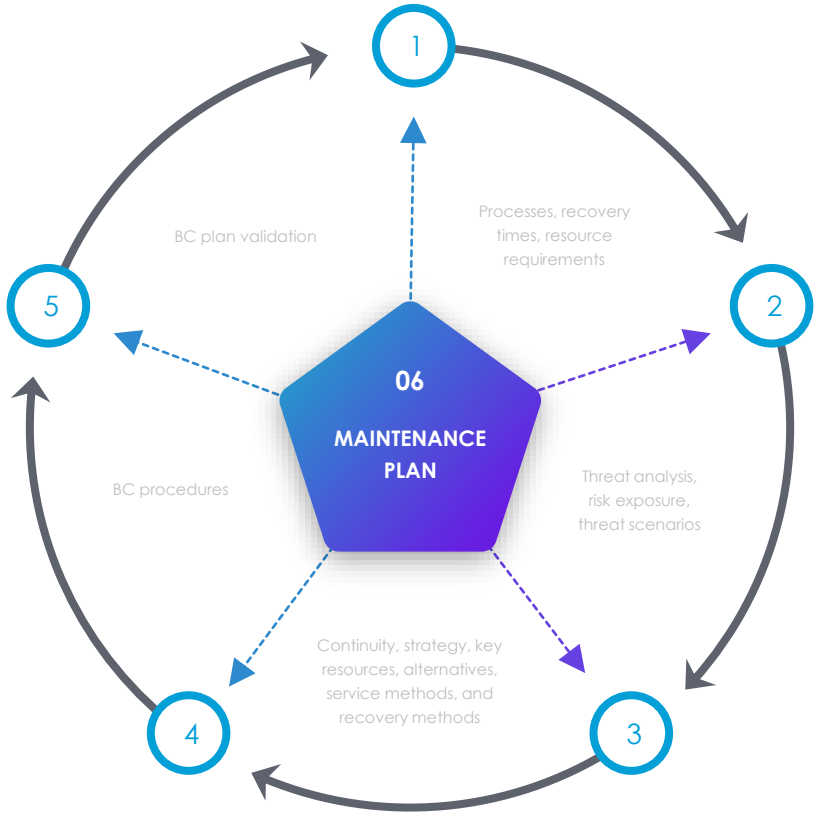
The BIA, which is conducted during the first stage, analyze the financial & operational impact of disruptive events on the business areas & processes.

02

This is composed of risk analysis and risk evaluation, is performed on the critical processes identified during the BIA stage.

03

The main purpose of this stage is to develop a business continuity strategy. That satisfies the business recovery requirements.



04

The predetermined procedures & guidelines prevent organizations from making on the spot critical decisions in the middle of a crisis.

05

Its main purpose is to validate the business continuity strategy, activities, assumptions regarding times in business continuity plans.

06

This phase maintain the BCP in a constant ready-state. The maintenance process of a BCMS is constant and dynamic.

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

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 !

Zálohovanie, obnova systémov po havárii a krízové riadenie (Blok II)
Kurz: Manažér kybernetickej bezpečnosti

Doc. Ing. Katarína Kampová, PhD.

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

Katarina.Kampova@uniza.sk