MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Plán Kontinuity činností
BCP – Business Continuity Plan

Plán kontinuity činností (BCP)

Plán kontinuity činností (BCP) v organizácií upravuje procesy zálohovania, havarijného plánovania a obnovy prevádzky informačných systémov (ďalej ako „IS“) po výskyte krízovej udalosti v organizácii. Definuje povinnosti organizácie a jej zamestnancov tak, aby bolo možné prevádzku IS obnoviť v požadovanom rozsahu a čase.
Účelom dokumentu BCP je zároveň definovať základné prvky, ktoré sa majú implementovať v rámci sietí a informačných systémov organizácie s cieľom pripraviť sa na rýchle zvládnutie akejkoľvek krízovej situácie a zabezpečiť kontinuitu činností. **Krízová udalosť** je udalosť, ktorá spôsobí prerušenie prevádzky IS a má vážny negatívny vplyv na činnosť organizácie. Výskyt, typ a rozsah krízovej udalosti sa nedá vopred naplánovať a nie je možné ani presne predpovedať jej dopad. Negatívne účinky jej výskytu je však možné eliminovať adekvátnou prípravou. BCP poskytujú návod a postupy pre rýchle a efektívne obnovenie činností kľúčových technológií, infraštruktúry, aplikácií a dát po výskyte krízovej udalosti.
Počas prerušenia bežnej prevádzky, havárie alebo krízovej situácie sú základné predbežné prípravy a rýchlosť reakcie nevyhnutné na obmedzenie súvisiacich dopadov.

Riadenie kontinuity činností sa vzťahuje na všetky identifikované siete a informačné systémy organizácie a zameriava sa na riešenie kríz súvisiacich prevažne s:

- bezpečnosťou zamestnancov (alebo osôb v priestoroch organizácie),
- krízovou situáciou súvisiacou so službami alebo dodávkami, ktoré majú dopad na činnosti organizácie bez ohľadu na dôvody (technické, sociálne, právne, bezpečnostné, environmentálne, a pod.),
- akoukoľvek situáciou, ktorá ohrozuje dobré meno a povesť organizácie.

Organizácia by mala uznať potenciálne riziká, ktoré môžu mať vplyv na jej činnosť, a je potrebné organizovať ich tak, aby čelili a zvládali všetky krízové situácie, ktoré môžu mať vplyv na jej podnikanie. Organizácia by mala nastaviť základné procesy riadenia kontinuity činností s cieľom zmierniť dopady akejkoľvek mimoriadnej, resp. krízovej situácie. V neposlednom rade musí vymenovať kľúčové kontakty na úrovni krízového výboru s cieľom zabezpečiť správnu reakciu na mimoriadnu, resp. krízovú situáciu. Zodpovednosti krízového tímu v prípade mimoriadnej situácie sú nasledovné:

- potvrdí vzniknutú situáciu ako mimoriadnu, resp. krízovú,
- zostaví vhodný tím na riešenie mimoriadnej, resp. krízovej situácie a zabezpečí jeho dostupnosť. To znamená, že podľa vzniknutej situácie určí jedného operačného manažéra a zástupcu operačného manažéra, určí jedného manažéra komunikácie pre externú a internú komunikáciu, podľa potreby pridelí ďalšie kľúčové úlohy (právne, poisťovacie, IT, ...) a zabezpečí, aby boli ich misie správne definované s operačným manažérom
- zabezpečí, aby boli k dispozícii základné podklady a dokumentácia v oblasti riadenia kontinuity činností,
- zabezpečuje, pomáha a monitoruje efektívne nastavenie tímu na riešenie mimoriadnej, resp. krízovej situácie,
- vedie a robí rozhodnutia
- ukončuje mimoriadnu, resp. krízovú situáciu.

Organizácia musí rozvíjať, udržiavať a neustále zlepšovať plán kontinuity činností a plány obnovy prevádzky a tiež pravidelne realizovať testovanie plánov kontinuity činností, resp. plánov obnovy prevádzky.

Vzor plánu kontinuity činností

Pre každú sieť a informačný systém v rámci aktív organizácie spracuje jeho správca BCP v nasledovnej štruktúre:

Popis procesu

- Popis procesu z analýzy dopadov
- Vlastník procesu a jeho zástupcovia
- Parametre procesu – MTO, RTO, RPO
- Zdroje využívané procesom
- Aplikácie
- Infraštruktúra
- Údaje (vo fyzickej aj logickej podobe)
- Ľudské zdroje
- Lokality
- Dodávatelia

Popis scenáru / scenárov

- Konkrétny scenár podľa internej smernice organizácie popisujúcej scenáre kybernetických bezpečnostných rizík
- Ďalšie príklady scenárov:
    - Nedostupnosť aplikácie
    - Obmedzenie funkčnosti aplikácie
    - Nedostupnosť budovy
    - Výpadok podporných služieb (elektrina, voda, kúrenie)
    - Výpadok služieb dodávateľa
    - Nedostupnosť ľudských zdrojov

Obmedzenia / predpoklady

- Kvalifikácia personálu
- Vhodné priestory – riadne alebo náhradné
- Dostupná sieťová infraštruktúra - pripojenie do lokálnej siete / na internet

Kontaktné údaje všetkých osôb uvedených v BCP

Pre **každý scenár** je spracovaný postup podľa nasledovnej štruktúry:

Prípravné úlohy

Všetky aktivity, ktoré majú byť vykonané pred tým, ako je BCP použitý pri realizácii negatívneho scenára.

- Príklady:
  - Zabezpečenie náhradných priestorov
  - Zabezpečenie náhradnej techniky
  - Príprava internej a externej komunikácie
  - Dohodnutie SLA s dodávateľom
  - Aktívny monitoring

Identifikácia problému

Akým spôsobom zistime, že nastal negatívny scenár.

- Príklady:
  - Automatické notifikácie
  - Identifikácia zamestnancami IT
  - Hlásenie dodávateľa
  - Identifikácia používateľmi (zamestnancami)
  - Identifikácia klientmi
  - Kontaktná osoba

Fáza reakcie

Reakcia na incident.

- Príklady:
  - Informovanie relevantných osôb (vlastník, BCM koordinátor, manažér KIB)
  - Potvrdenie scenára
  - Aktivácia krízového riadenia
  - Aktivácia DRP
  - Rozhodnutie o alternatívnom procese
  - Informovanie ďalších osôb (interní používatelia)

Alternatívny proces

Alternatívne spôsoby výkonu procesu (ak existujú)

- Príklady:

- Realizácia procesu v alternatívnych priestoroch
- Home Office
- Realizácia procesu náhradným personálom
- Použitie kancelárskeho softvéru namiesto aplikácie
- Manuálne spracovanie namiesto automatizovaného
- Informovanie na web stránke, sociálnych sieťach
- „Čakanie“

Obnovovacie postupy

Kroky na obnovenie plnej prevádzky

➢ Príklady:

- Realizácia DRP
- Obnova údajov zo zálohy
- Reštart IKT systémov
- Realizácia krokov, ktoré nie sú v DRP, alebo ak pre dané aktívum neexistuje DRP
- Obnova v spolupráci s dodávateľom

Kontrolné úlohy

Aktivity vykonávané na uistenie pred prechodom do plnej prevádzky

➢ Príklady:

- Kontrola dostupnosti a funkčnosti IKT systémov
- Kontrola obnovy a aktuálnosti údajov
- Kontrola dostupnosti priestorov
- Potvrdenie dostupnosti personálu
- Odstránenie informácie z web stránky
- Informovanie relevantných osôb (vlastník, BCM koordinátor, manažér KIB)
- Informovanie ďalších osôb (interní používatelia)

Plán kontinuity činností (BCP) – jeden z možných príkladov, ako spracovať plán kontinuity činností

PLÁN KONTINUITY ČINNOSTÍ (BCP)	
Popis procesu	➢ Vlastník procesu a jeho zástupcovia ➢ Parametre procesu – MTO, RTO, RPO ➢ Zdroje využívané procesom ➢ Aplikácie ➢ Infraštruktúra ➢ Údaje (vo fyzickej aj logickej podobe) ➢ Ľudské zdroje ➢ Lokality ➢ Dodávatelia
Analýza dopadov	Plánovanie obnovy IS vychádza z požiadaviek a potrieb používateľov na prevádzku IS a na dostupnosť údajov v nich. Na to spracúva ANALÝZA DOPADOV (identifikácia požiadaviek používateľov na obnovu IS: ➢ Typ dát ➢ Zodpovednú osobu ➢ Mieru zodpovednosti ➢ Spôsob / metódu ➢ Periódu ➢ Zálohovací hardvér ➢ Typ zálohy ➢ Určenie zálohovaných serverov na úrovni FS ➢ Určenie zálohovaných serverov na úrovni DB ➢ Určenie zálohovaných DB
Hrozba	Podľa príslušnej smernice popisujúcej kybernetické bezpečnostné hrozby
Popis scenáru	Podľa príslušnej smernice popisujúcej scenáre kybernetických bezpečnostných rizík
Pravdepodobnosť vzniku	Nízka / Stredná / Vysoká
Obmedzenia / predpoklady	Napr. Dostupná sieťová infraštruktúra - pripojenie do lokálnej siete / na internet
Kontaktné údaje všetkých osôb	

Komunikačný plán pre BCP	
OPATRENIE PRE KONKRÉTNY SCENÁR	
Prípravné úlohy	Napr. Dohodnutie SLA s dodávateľom
Identifikácia problému	Napr. Identifikácia používateľmi (zamestnancami)
Fáza reakcie	Napr. Aktivácia DRP
Alternatívny proces	Napr. Manuálne spracovanie namiesto automatizovaného
Obnovovacie postupy	Napr. Obnova v spolupráci s dodávateľom
Kontrolné úlohy	Napr. Kontrola dostupnosti priestorov

PREVENCIA

1. Napr. Umiestnenie serverovne do vyšších poschodí budovy.
2. Napr. Vytvorenie záloh.
3. Napr. Zmluvné dohodnutie záložnej lokality. V prípade vzniku mimoriadnej udalosti presunutie prevádzky informačného alebo komunikačného systému do alternatívnej (záložnej) lokality.

ČINNOSTI V PRÍPADE AKTIVÁCIE ZDROJA HROZBY	
Scenár pokrýva najhorší variant, kedy bude potrebné opustiť budovu organizácie, v ktorej je umiestnená serverovňa. V rámci testovania a aj v priebehu ostrého nasadenia plánu protiopatrenia musia byť všetky činnosti obnovy dokumentované, aby mohli byť tu uvedené postupy obnovy prípadne aktualizované alebo spresnené - vykonáva určený člen tímu. *Príklad činností a časových intervalov sú uvedené nižšie.*	**Doba trvania**
1. Zvolanie krízového štábu organizácie - Zvolanie krízového tímu IT. - Postup podľa povodňového plánu organizácie. - Rozhodnutie o aktivácii záložnej lokality.	2 hod.

2. Zahájení prípravy spustenia záložnej lokality - Zbalenie vytvorených záloh na základe DRP. - Presun zodpovedných osôb do záložnej lokality – pracovníci odboru IT, a ďalší členovia tímu potrební pre zachovanie chodu nevyhnutných činností organizácie. - Aplikovanie opatrení pre minimalizáciu škôd. - Evakuácia zvyšku osôb a nariadenie útlmovej činnosti. - Inštalácia a konfigurácia serverov, aplikácií, sieťových prvkov na základe DRP.	5 hod.
3. Zahájenie ostrej prevádzky v záložnej lokalite - Informovanie vedenia organizácie o obnovení dostupnosti aplikácií v záložnej lokalite.	2 hod.
Koniec (Celková doba trvania)	**9 hod.**
ODPORUČENIE PRO MENEJ ZÁVAŽNÝ VÝVOJ SITUÁCIE	
Napr. V prípade, že sa krízový štáb rozhodne neaktivovať záložnú lokalitu, bude utlmená činnosť organizácie, budú podniknuté opatrenia pre minimalizáciu škôd (protipovodňové opatrenia), a všetky osoby budú evakuované.	
ĎALŠÍ POSTUP	
Napr. Mimoriadna udalosť bude naďalej monitorovaná. Po opadnutí povodne začnú likvidačné práce a obnovenie činností organizácie v plnom rozsahu.	