

Plán obnovy činností IS DRP – Disaster Recovery Plan

Plán obnovy činností IS (DRP)

Plány obnovy (DRP) sú vytvárané s cieľom minimalizovať dobu výpadku alebo nedostupnosti príslušného IS a tiež minimalizovať stratu uchovávaných a spracúvaných dát.

Konkrétne postupy na obnovenie činnosti IS a dát – plány na obnovu IS by mali byť uvedené v samostatných dokumentoch vypracovaných a dodaných autorom príslušného IS ako súčasť prevádzkovej dokumentácie.

Plánovanie obnovy informačných systémov (ďalej len “IS”) vychádza z požiadaviek a potrieb používateľov na prevádzku IS a na dostupnosť všetkých údajov, ktoré sa na nich nachádzajú. DRP pozostáva z nasledujúcich krokov:

- analýza dopadov - v úvodnom kroku sú identifikované požiadavky používateľov na obnovu IS,
- identifikácia krízových scenárov a definovanie stratégií obnovy – na základe rizík, ktoré pôsobia na IS organizácie zodpovední zamestnanci identifikujú krízové scenáre a definujú stratégie obnovy IS tak, aby boli v súlade s požiadavkami používateľov a možnosťami organizácie,
- tvorba a testovanie plánov obnovy – zodpovední zamestnanci na základe definovaných stratégií popíšu plány obnovy pre jednotlivé IS (detailné plány obnovy) ako aj plán obnovy IS organizácie ako celku (komplexný plán obnovy).

Analýza dopadov tvorí základný dokument pre stanovenie pravidiel plánovania obnovy, pričom identifikácia krízových scenárov a definovanie stratégií obnovy je predmetom internej smernice. Na základe danej smernice sú určené taktiež pravidlá na tvorbu a testovanie plánov obnovy. Plánovanie obnovy je cyklický proces. Úvodné analýzy sa opakujú v pravidelnom intervale, napr. každé dva roky, alebo po každej významnej zmene v IS organizácie. Na základe úprav alebo zmien v IS sú vykonávané zmeny v plánoch obnovy.

Organizácia musí stanoviť požiadavky na obnovu IS a zodpovedá za finančné zabezpečenie záložných technológií a procesov obnovy. Požiadavky na obnovu IS môžu byť pridelené napríklad nasledovným spôsobom, ktorý znázorňuje tabuľka č. 1.

Typ dát	Zodpovedná osoba	Zodpovednosť	Spôsob, metóda	Periódna	Zálohovací HW	Typ zálohy
Systémové registre serverov, elektonická pošta, a pod.	Administrátor IS, Správcovia aplikácií, a pod.	Zálohovanie databáz, súborov, a pod.	Fyzický HW – nástrojmi OS, virtuálne servery, a pod.	Denne, pred aplikovaním zmien, a pod.	Pásková knižnica, a pod.	Plná záloha, inkrementálna, a pod.

Tabuľka č. 1

Plán obnovy činností / Havarijný plán (DRP)

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

Popis zdroja (systému)

- Popis zdroja
- Vlastník / gestor zdroja a jeho zástupcovia
- Zoznam podporovaných procesov
- Požiadavky na obnovu (MTO, RTO, RPO)
- Stratégia obnovy

Popis scenáru / scenárov

- Konkrétny scenár podľa internej smernice popisujúcej scenáre kybernetických bezpečnostných rizík
- Ďalšie príklady scenárov:
 - Obnova údajov zo zálohy
 - Obnova konfigurácie aplikácie / databázy / operačného systému
 - Opätovná inštalácia aplikácie / databázy / operačného systému
 - Výmena hardvérového komponentu
 - Opätovná inštalácia celého hardvéru

Obmedzenia / predpoklady

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

Kontaktné údaje všetkých osôb uvedených v DRP

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

Prípravné úlohy

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

- Príklady:
 - Udržiavanie konfiguračnej databázy
 - Predpripravený „image“ systému
 - Zabezpečenie náhradného hardvéru
 - Dohodnutie SLA s dodávateľom hardvéru

- Aktívny monitoring

Identifikácia problému

Akým spôsobom zistíme, že nastal negatívny scenár.

➤ Príklady:

- Aktivácia DRP z nadradeného BCP
- Automatické notifikácie
- Identifikácia zamestnancami IT
- Hlásenie dodávateľa
- Identifikácia používateľmi (zamestnancami)
- Identifikácia klientmi

Fáza reakcie

Reakcia na incident.

➤ Príklady:

- Informovanie relevantných osôb (vlastník, BCM koordinátor, manažér KIB)
- Potvrdenie scenára

Obnovovacie postupy

Kroky na obnovenie plnej prevádzky podľa zvoleného scenára

➤ Príklady scenárov:

- Obnova údajov zo zálohy
- Obnova konfigurácie aplikácie / databázy / operačného systému
- Opätovná inštalácia aplikácie / databázy / operačného systému
- Výmena hardvérového komponentu
- Opätovná inštalácia celého hardvéru

Kontrolné úlohy

Aktivity vykonávané na uistenie pred prechodom do plnej prevádzky

➤ Príklady:

- Kontrola dostupnosti a funkčnosti IKT systémov
- Kontrola obnovy a aktuálnosti údajov
- Informovanie relevantných osôb (vlastník, BCM koordinátor, manažér KIB)

Plán obnovy činností / Havarijný plán (DRP) – jeden z možných príkladov, ako spracovať plán kontinuity činností

PLÁN OBNOVY ČINNOSTÍ / HAVARIJNÝ PLÁN (DRP)	
Popis zdroja / systému	<ul style="list-style-type: none"> ➤ Popis zdroja ➤ Vlastník / gestor zdroja a jeho zástupcovia ➤ Zoznam podporovaných procesov ➤ Požiadavky na obnovu (MTO, RTO, RPO) ➤ Stratégia obnovy
Kategória DRP IS	<ul style="list-style-type: none"> ➤ kritické DRP IS ➤ vitálne DRP IS ➤ ostatné DRP IS
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 DRP	
OPATRENIE PRE KONKRÉTNY SCENÁR	
Prípravné úlohy	Napr. Predpripravený „image“ systému
Identifikácia problému	Napr. Identifikácia zamestnancami IT
Fáza reakcie	Napr. Informovanie relevantných osôb (vlastník, BCM koordinátor, manažér KIB)
Obnovovacie postupy	Napr. Opätovná inštalácia a konfigurácia aplikácie / databázy / operačného systému
Kontrolné úlohy	Napr. Kontrola obnovy a aktuálnosti údajov
PREVENCIA	
1. Napr. Vytvorenie záloh.	
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. <u>Príklad činností a časových intervalov sú uvedené nižšie.</u>	Doba trvania
<p>1. Zvolanie krízového štábu organizácie</p> <ul style="list-style-type: none"> - Zvolanie krízového tímu IT. - Postup podľa povodňového plánu organizácie. - Rozhodnutie o aktivácii záložnej lokality. 	2 hod.
<p>2. Zahájenie prípravy spustenia záložnej lokality</p> <ul style="list-style-type: none"> - 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.
<p>3. Zahájenie ostrej prevádzky v záložnej lokalite</p> <ul style="list-style-type: none"> - Informovanie vedenia organizácie o obnovení dostupnosti aplikácií v záložnej lokalite. 	2 hod.
Koniec (Celková doba trvania)	9 hod.
ODPORUČENIE PRO MENEJ ZÁVAŽNÝ VÝVOJ SITUÁCIE	
Např. 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	
Např. Mimoriadna udalosť bude naďalej monitorovaná. Po opadnutí povodne začnú likvidačné práce a obnovenie činností organizácie v plnom rozsahu.	