MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Plán obnovy činností IS
DRP – Disaster Recovery Plan

I. Plán obnovy činností IS (DRP)

Plány obnovy (Disaster recovery plan - DRP) sú vytvárané s cieľom minimalizovať dopady narušenia informačných systémov (dobu výpadku alebo nedostupnosti príslušného IS), tiež bezpečnostného incidentu, 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 administrátorom / 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:

- 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,
- aktualizácie BCP a DRP.

Najdôležitejšou časťou pri tvorbe DRP je vytvorenie 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).

Pozn. Organizácia musí v analýze dopadov (BIA) 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. (ide o príklad jedného z opatrení ako výsledku analýzy rizík, na ktorých je postavený DRP):

Typ dát	***Zodpovedná osoba***	***Zodpovednosť***	***Spôsob, metóda***	***Perióda***	***Zálohovací HW***	***Typ zálohy***
Systémové registre serverov, elektronická 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

II. Metodika pri tvorbe plánu obnovy činností (DRP)

Pre každú sieť a informačný systém podporujúci kritickú službu organizácie 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

- 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

III. Scenáre v rámci plánu kontinuity činností (BCP)

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 zistime, že nastal negatívny scenár.

➢ Príklady:

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

Fáza reakcie

V rámci reakcie na incident je potrebné definovať kritériá, na základe ktorých sa DRP aktivuje.

➢ 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)

IV. Návrh vzoru plánu obnovy činností (DRP)

PLÁN OBNOVY ČINNOSTÍ / HAVARIJNÝ PLÁN (DRP)	
Popis zdroja / systému	➢ Popis zdroja ➢ Vlastník / gestor zdroja a jeho zástupcovia ➢ Zoznam podporovaných procesov ➢ Požiadavky na obnovu (MTO, RTO, RPO) ➢ Stratégia obnovy
Kategória DRP IS	➢ kritické DRP IS ➢ ostatné DRP IS
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	

Scenár pokrýva najhorší variant, kedy bude potrebné opustiť budovu organizácie, v ktorej je umiestnená serverovňa. *Pozn. v rámci testovania DRP a aj v priebehu ostrého nasadenia DRP musia byť všetky činnosti obnovy dokumentované, aby mohli byť tu uvedené postupy v prípade potreby 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	
Menej závažný vývoj situácie znamená, že krízový štáb alebo bezpečnostný výbor na základe indikácií a vlastnej analýzy predloženej situácie subjektívne zváži, že vývoj situácie nebude smerovať k závažnému kybernetickému bezpečnostnému incidentu alebo k ohrozeniu zdravia a života osôb. 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.	