

Havarijní plány

OBSAH

| | | |
|------------------|---|----------|
| ČÁST I. | Úvodní ustanovení | 3 |
| Kapitola 1 | Definice pojmů | 3 |
| Kapitola 2 | Rozsah působnosti | 3 |
| ČÁST II. | Role, odpovědnosti a pravomoci | 3 |
| ČÁST III. | Životní cyklus havarijního plánu | 4 |
| Kapitola 1 | Vytvoření havarijního plánu..... | 4 |
| Kapitola 2 | Údržba havarijního plánu | 5 |
| 2.1 | Testování havarijního plánu..... | 5 |
| 2.2 | Aktualizace havarijního plánu | 6 |
| ČÁST II. | Aktivace havarijního plánu | 6 |
| ČÁST III. | Přechodná ustanovení | 6 |

ČÁST I. ÚVODNÍ USTANOVENÍ

Kapitola 1 DEFINICE POJMŮ

Havárie: závažné zhoršení, případně úplný výpadek, funkčnosti nebo dostupnosti konkrétního informačního systému.

Havarijní plán: dokument, který popisuje posloupnost činností a odpovědností za ně, které je potřeba provést při vzniku havárie, aby došlo k minimalizaci jejích následků (pokud je to účelné, může se sestávat z několika havarijních scénářů pro konkrétní havarijní situace).

Havarijní scénář: konkrétní postup pro řešení dané havárie, resp. konkrétní havarijní situace.

Havarijní tým: účelově vytvořený tým, jehož úkolem je v požadovaném čase obnovit funkčnost a dostupnost daného IS v případě aktivace havarijního plánu.

Incident: jakákoli odchylka od popsaného stavu, resp. výpadek služby.

Bezpečnostní incident: událost v IS, která způsobila narušení důvěrnosti, integrity, dostupnosti nebo neodmítnutelnosti informace v důsledku selhání bezpečnostních opatření nebo porušení bezpečnostní politiky.

Informační aktivum: jakákoli informace nebo prostředek pro práci s ní, který má pro MD nějakou hodnotu.

Informační systém (IS): informační infrastruktura, soustava aplikací, organizačních opatření, procedur a souvisejících služeb pro tvorbu, získávání, zpracování, ukládání a prezentaci informací.

Správce IS: vedoucí zaměstnanec, který určuje účel zpracování informací a podmínky provozování IS.

Kapitola 2 ROZSAH PŮSOBNOSTI

Tato příloha Bezpečnostní politiky informací MD (dále jen BPI MD) popisuje základní pravidla, zásady a principy tvorby a údržby havarijních plánů informačního systému MD. Řídí se jí všichni zaměstnanci MD. Externí subjekty jsou zavázány k plnění této přílohy smluvně.

Havarijní plány jsou vytvářeny pro všechny důležité IS MD, prioritně pak pro:

- informační systémy Kritické informační infrastruktury,
- Významné informační systémy.

ČÁST II. ROLE, ODPOVĚDNOSTI A PRAVOMOCI

Manažer KB:

- koordinuje a metodicky řídí vytvoření havarijních plánů v rámci IS MD jako celku,
- z metodického hlediska posuzuje a připomínkuje vypracované havarijní plány,
- řídí přípravu harmonogramu a průběh testování havarijních plánů jednotlivých IS,
- má právo se účastnit testování havarijních plánů,
- s ohledem na výsledky testů dává doporučení na změny a doplnění plánů.

Manažer KB má právo požadovat odpovídající součinnost věcně příslušných útvarů a Odboru ICT.

Správce IS rámci své působnosti odpovídá za vytvoření havarijních plánů a jmenuje vedoucí havarijních týmů (pokud vedoucího havarijního týmu nejmenuje, je jím implicitně samotný správce IS).

Havarijní tým

Každý havarijní plán má svůj havarijní tým, jehož členové musí disponovat:

- věcnou znalostí oblasti, kterou daný systém podporuje (tyto členy havarijního týmu určuje správce IS),
- technickou znalostí daného IS resp. systémů, se kterými daný IS komunikuje (tyto členy havarijního týmu určuje ředitel Odboru ICT).

Vedoucí havarijního týmu:

- odpovídá za vypracování havarijního plánu daného IS,
- zajišťuje, aby zaměstnanci, kteří mají v rámci havarijního plánu přiřazenu nějakou roli, byli odpovídajícím způsobem proškoleni,
- vyhlašuje aktivaci plánu obnovy daného IS na základě vlastního zhodnocení situace,
- vyžaduje v případě potřeby nezbytnou součinnost útvarů MD,
- podává informace vedení MD o průběhu a řešení nastalé havárie,
- není řešitelem,
- řídí a koordinuje všechny činnosti zvládnutí havárie,
- zajišťuje prostředky a podmínky pro práci členů týmu po celou dobu aktivace havarijního plánu,
- má přehled o všech činnostech, které je potřebné v rámci obnovení dostupnosti systému vykonat, zejména z hlediska jejich kapacitních požadavků a časové náročnosti,
- sestavuje harmonogram pravidelného testování havarijního plánu,
- provádí pravidelnou údržbu (revizi, aktualizaci a testování) havarijního plánu,
- distribuuje aktuální verzi havarijního plánu podle distribučního seznamu (ten je součástí každého havarijního plánu),
- předkládá výsledky testů havarijního plánu správci IS, řediteli Odboru ICT a Manažerovi KB.

ČÁST III. ŽIVOTNÍ CYKLUS HAVARIJNÍHO PLÁNU

Životní cyklus havarijního plánu je:

- vypracování havarijního plánu a jeho schválení,
- údržba havarijního plánu (pravidelné testování a aktualizace) havarijního plánu,
- aktualizace navazující na výsledky testů a na změny dané agendy nebo s ní souvisejícího havarijního plánu.

Kapitola 1 VYTVOŘENÍ HAVARIJNÍHO PLÁNU

Každý havarijní plán obsahuje:

- název IS, pro který je havarijní plán zpracován (případně průřezové oblasti, kterou je např. infrastruktura IS MD),
- identifikaci pracoviště a lokality, které se bude havarijní plán týkat,
- přehled revizí (uvedeno musí být i to, že ke změně v rámci aktualizace nedošlo),
- distribuční seznam (jeho součástí jsou povinně vlastníci primárních informačních aktiv, se kterými daný IS pracuje),
- osoby, které hrají v havarijním plánu nějakou roli a kontakty na ně,
- rozsah havarijního plánu, zahrnující výčet havarijních situací, např.:
 - úplné nebo částečné zničení celého datového centra,
 - úplné nebo částečné zničení technického vybavení,
 - nedostupnost datového centra,

- úplná nebo částečná nedostupnost pracovního prostředí uživatelů IS MD (zatopení budovy MD a podobně),
- určení, jaký havarijní scénář bude v rámci jednotlivých havarijních situací uplatněn,
- popis jednotlivých havarijních scénářů, které obsahují:
 - seznam pracovníků, které je zapotřebí neprodleně informovat včetně jejich zástupců,
 - eskalační postupy (např. v případě, že je někdo z výše uvedeného seznamu i přes uvedenou zastupitelnost nedostupný),
 - odkaz na aktuální dokumentaci systému v papírové i elektronické formě včetně jejího umístění (aktuální popis konfigurace, postup pro obnovu ze zálohy a podobně),
 - odkaz na znalostní „databázi“ (knowledgebase), relevantně vzhledem ke scénáři,
 - seznam náhradních zdrojů (prostory, technologie, lidé, relevantně vzhledem ke scénáři),
 - umístění záloh instalačních médií a podobně (relevantně vzhledem ke scénáři),
 - popis postupu pro jednotlivé role v rámci scénáře,
- popis obecného scénáře, pokud by vzniklá havárie neodpovídala žádnému konkrétnímu scénáři.

Kapitola 2 ÚDRŽBA HAVARIJNÍHO PLÁNU

2.1 Testování havarijního plánu

Havarijní plán musí být pravidelně testován za účelem:

- prověření a procvičení znalostí a schopností jednotlivých členů havarijního týmu a tohoto týmu jako celku,
- identifikace slabých míst havarijního plánu a jejich odstranění.

Harmonogram testování havarijního plánu je v kompetenci vedoucího havarijního týmu. Plán všech testů havarijních plánů v rámci MD koordinuje po dohodě se správcem IS (ti dodají podklady vždy k 1. 12.) Manažer KB. Celkový plán havarijních testů pro daný rok schvaluje ředitel Odboru ICT.

Každý test musí:

- ověřit připravenost záložní lokality,
- specifikovat požadavky na lidské a technické zdroje,
- obsahovat přesný harmonogram testu,
- probíhat tak, aby testovací procedury nenarušily rutinní provoz daného IS,

Test může být spuštěn pouze na základě souhlasu správce daného IS.

O průběhu testu musí být pořízena zpráva, která obsahuje:

- informaci o cílech a průběhu testu,
- manažerské shrnutí pro správce IS,
- zhodnocení průběhu a výsledků testu (doporučeno je provést toto zhodnocení přímo s účastníky testu, aby mohli aktivně přispět svým názorem),
- vyjádření Manažera KB,
- doporučení na úpravy a zlepšení plánu.

2.2 Aktualizace havarijního plánu

Havarijní plány odpovídají aktuální situaci. Reagují na výsledky testů (návrhy na úpravy a zlepšení) a na změny v rámci MD, které mohou ovlivnit havarijní postupy - zejména pak na změny:

- daného procesu nebo agendy,
- podpůrného IS,
- organizační struktury,
- personální,
- požadavků na výkon IS, jeho dostupnost a případně na bezpečnostní klasifikaci informací, které daný IS zpracovává.

Vedoucí havarijního týmu zajistí:

- aktualizaci havarijního týmu bez zbytečného odkladu,
- aktualizaci kontaktních údajů nejméně jednou za čtvrt roku,
- řízenou distribuci aktualizovaného havarijního plánu podle distribučního seznamu.

ČÁST II. AKTIVACE HAVARIJNÍHO PLÁNU

Vstupy pro rozhodnutí o aktivaci havarijního plánu jsou zejména informace z Incident Managementu a Problem Managementu. Vedoucí havarijního týmu incidentem nebo problémem zasaženého IS po zhodnocení závažnosti rozhodne, zda se jedná o méně závažný bezpečnostní incident, který bude řešen běžnými provozními postupy, nebo zda se jedná o havárii.

V případě, že je situace vedoucím havarijního týmu vyhodnocena jako havárie, aktivuje havarijní plán podle scénáře, který odpovídá dané havarijní situaci.

ČÁST III. PŘECHODNÁ USTANOVENÍ

Do doby zajištění technických prostředků a podmínek pro vytvoření, testování a správu havarijních plánů je nutné postupovat v co největší možné míře souladu s touto přílohou BPI MD.