

HAVARIJNÉ PLÁNY A PLÁNY OBNOVY ENVIRONMENTÁLNEHO INFORMAČNÉHO SYSTÉMU

PAVOL VOJTEK

EMERGENCY SCHEMES AND SCHEMES OF RENOVATION ENVIRONMENTAL INFORMATION SYSTEM

ABSTRAKT

Predmetom tohto príspevku je poukázať na vhodnosť vypracovania metodiky havarijných plánov a plánov obnovy EIS pre environmentálne organizácie, ktoré spravujú, uchovávajú a poskytujú dôležité environmentálne údaje o životnom prostredí pre podporu rozhodovania pre environmentálny manažment. Návrh, implementácia a údržba havarijných plánov je komplexná činnosť, ktorá si vyžaduje metodiku.

Keľúčové slová: *prevencia, reakcia na narušenie, obnova, konsolidácia*

ABSTRACT

The object of this contribution is to point out the suitability of working-out the methodology of emergency schemes and schemes of renovation EIS for environmental organizations, which manage, keep and provide important data about the environment for decision support in environmental management. Proposal, implementation and maintenance of emergency schemes is complex activity and it needs methodology.

Key words: *prevention, response, resumption, recovery, restoration*

Ľudia pracujúci s počítačmi vedia o možných hrozbách „Odcudzenia, modifikovania, alebo zničenia dát“ inou osobou. Je to narastajúci problém hlavne od doby rozšírenia internetu, ktorý pospájal väčšinu informatického sveta do jedného celku a tým umožnil takzvaným šikovným ľuďom, aby prejavili svoje nadanie a ukázali ho aj ostatným napríklad takým spôsobom, že im odcudzili alebo pozmenili ich dáta. Vznikla teda veľká potreba tieto údaje chrániť pred cudzím zrakom, ale aj pred ich neoprávneným získaním.

Okrem tejto hrozby môžu nastať aj situácie, kedy je funkčnosť informačného systému ohrozená nielen „šikovnými ľuďmi“ ale niekedy dochádza z rôznych príčin aj k zlyhaniu rozsiahlych častí informačného systému. Dôvody môžu byť rôzne. Častou príčinou môže byť výpadok sieťových zariadení z dôvodu ich zlyhania, alebo výpadok niektorých serverov, poskytujúcich služby pre environmentálny manažment na rôznych úrovniach. No môže ísť aj o úmysel ľudí vedome znefunkčnúť informačný systém s úmyslom poškodiť. Prostriedky na vniknutie do interných sietí sú stále dokonalejšie. Počet útokov na interné dáta sa rok od roka zdvojnásobuje. Objavujú sa nové možnosti ohrozenia a správcovia sietí majú po detekovaní útoku na internú sieť stále menej a menej času na záchranu dát. Riziká však neprichádzajú iba z externého prostredia.

RUSKO, M. – BALOG, K. [Eds.] 2007:
Manažérstvo životného prostredia 2007 ▼▲▼ Management of Environment '2007
zo VII. konferencie so zahraničnou účasťou konanej 5. - 6. 1. 2007 v Jaslovských Bohuniach
Proceedings of the International Conference, Jaslovské Bohunice, 5-6 January 2007
Žilina: Strix et VeV. Prvé vydanie. ISBN 978-80-89281-18-3.

Preto je potrebné chrániť pred takýmito hrozbami dôležité informačné systémy, ktoré poskytujú, alebo môžu poskytovať strategické environmentálne informácie týkajúce sa životného prostredia pre organizácie, podniky alebo aj firmy pred takýmito hrozbami, vypracovaním plánov, ktorých cieľom bude minimalizovať narušenie funkčnosti IS na čo najkratšiu dobu.

Predmetom tohto príspevku je poukázať na vhodnosť vypracovania havarijných plánov a plánov obnovy EIS pre environmentálne organizácie, ktoré poskytujú, alebo spravujú dôležité environmentálne údaje o životnom prostredí.

Havarijný plán teda má obsahovať súhrn činností, ktoré sa majú vykonať pred, počas a po narušení funkcií prevádzkovateľa EIS s jediným cieľom - zachovať ich funkčnosť, teda zabezpečiť ich obnovu v prípade havárie. Pre každú činnosť je potrebné uviesť aktíva potrebné pre ich realizáciu (ľudské zdroje, záložné priestory, technické vybavenie a podobne)

Hlavným cieľom havarijného plánu je ochrániť prevádzkovateľa environmentálneho IS v čase, keď je jeho informačný systém, prípadne jeho časť, nefunkčná. Najvhodnejšou metódou na ochranu je pripravenosť. Plánovací proces dokáže minimalizovať narušenie funkčnosti systému, posilniť jeho stabilitu a optimalizovať obnovu systému po narušení.

Medzi ďalšie ciele havarijného plánu patria:

- Zavedenie pocitu bezpečnosti do environmentálneho informačného systému.
- Minimalizovanie času potrebného na zotavenie.
- Garantovanie pripravenosti záložného riešenia.
- Poskytnutie pravidiel pre testovanie plánov.

Minimalizovanie prijímania rozhodnutí v čase narušenia.

Cieľom tohto príspevku je vypracovanie havarijných plánov pre podporu funkčnosti environmentálneho informačného systému. Havarijné plány EIS môžeme chápať ako podmnožinou havarijných plánov.

Kritické procesy prevádzkovateľa environmentálneho IS

Strategická os	Popis
Zabezpečovanie výkonu monitoringu ŽP	Základná funkcia
Súlad s legislatívou	Prvou rovinou je porušenie platných legislatívnych predpisov a následné postihy Zvýšené požiadavky na podporu.
Ekonomická stabilita	Strategická os má tri roviny: Prvou je zabezpečenie vstupného toku financií Druhou rovinou je zabezpečenie toku financií vo vnútri organizácie tak, aby bola zabezpečená jej činnosť. Tretou rovinou je zabezpečenie distribúcie finančných tokov k partnerom Zvýšené požiadavky na podporu.

Strategická os	Popis
Ochrana dobrého mena	Poškodenie dobrého mena, resp. jeho strata, strata dôvery, vládnych orgánov, posudzované s ohľadom na možné negatívne ohlasy verejnosti a médií na potenciálne krízy (havarijné stavy) v systéme.
Riadenie a rozvoj ľudských zdrojov	Zabezpečenie kvalitného, odborne vzdelaného a stabilného personálu schopného podporovať základné funkcie spoločnosti.

Tab. 1 Havarijné plány EIS

Kritické aktíva prevádzkovateľa EIS predstavujú aktíva (dôležité údaje o životnom prostredí, o ohrozujúcich vplyvoch na životné prostredie a podobne), ktoré podporujú činnosť rozhodovania environmentálneho manažmentu. Veľké narušenie týchto aktív a oneskorená obnova ich činnosti môže viesť k priamym, alebo aj k nepriamym škodám. Zoznam kritických aktív je potrebné pravidelne kontrolovať, prehodnocovať a aktualizovať.

Objekty – budovy, meracie stanice, externé vyhodnocovacie zariadenia

Zamestnanci – vedúci zamestnanci a zamestnanci zodpovedný za funkčnosť EIS

Architektúra IS – servery, LAN, WAN

Podsystemy IS – personálna agenda, účtovníctvo a podobne

Environmentálne údaje – v elektronickej alebo papierovej podobe

Návrh, implementácia a údržba havarijných plánov je komplexná činnosť, ktorá si vyžaduje metodiku. Metodika potom delí proces havarijného plánovania do viacerých fáz.

Prevenia. Bezpečnosť organizácie stojí a padá na úrovni prevencie. Prevencia voči požiarom, živelným pohromám, voči narušeniu priestorov organizácie nepovolanými osobami, prevencia voči úniku dát alebo informácií, prevencia voči strate dát či už úmyselnej alebo náhodnej – všetky tieto faktory sú kamienkami v mozaike. Účinná prevencia môže zabrániť vzniku mnohých škôd, prípadne eliminovať následky, či už hmotné alebo nehmotné (strata dát, poškodenie dobrého mena spoločnosti). Prevenciou v oblasti IT je hlavne tvorba záloh údajov, bezpečné uloženie záloh ale aj školenia pracovníkov na vznik havarijných situácií. Súčasťou prevencie je aj tvorba havarijných plánov.

Reakcia na narušenie. Bezpečnostné pravidlá každej organizácie by mali zabezpečovať, aby okamžite po vzniku narušenia boli chránené životy ľudí a následne až technológie poskytujúce a spravujúce environmentálne informácie. Po detekovaní narušenia nastupuje havarijný tím. Riaditeľ havarijného tímu bude informovaný o veľkosti a následkoch narušenia a jeho zodpovednosťou je určiť nasledujúci postup.

Obnova. Po prijatí rozhodnutia riaditeľom havarijného tímu nasleduje obnova kritických aplikácií. Toto je najkritickejšia fáza, pretože ak sa v nej ukáže, že organizácia nemôže v akceptovateľnom rozsahu obnoviť svoju činnosť, môže to mať ďalekosiahle následky. V tejto fáze sa havarijné tímy riadia havarijnými plánmi. Ich úlohou je predovšetkým zabezpečiť náhradné prostriedky (servery, stanice používateľov, sieťová infraštruktúra, komunikačná infraštruktúra). Po zabezpečení hardvéru nasleduje obnova softvérového vybavenia (štart systémov, databáz) a údajov. Súčasťou plánov musí byť aj otestovanie tohto havarijného riešenia. Následne je obnovená prevádzka v havarijnom stave (ktorý nemusí byť identický s normálnym).

Konsolidácia. Nasleduje fáza konsolidácie, ktorá pokrýva obnovenie nekritických podporných činností. Sú to činnosti, ktoré sa síce od organizácie očakávajú, ale nemajú priamy vplyv na jej úlohy

(informácie, Internet,...) Návrat do pôvodného stavu. Keď je environmentálna organizácia zotavená z narušenia a dokáže poskytovať všetky bežné služby na akceptovateľnej úrovni, nastáva fáza návratu. Dĺžka tejto fázy nie je dopredu známa, záleží od rozsahu narušenia. Predovšetkým je potrebné zistiť a analyzovať všetky škody (ich rozsah, pôvod a ako im predísť do budúcnosti), zabezpečiť materiál, financie a ľudské zdroje na obnovu. V prípade poškodenia budovy, miestností alebo rozvodov nastáva rekonštrukcia týchto zariadení. Potom nasleduje obnovenie systémov, aplikácií a údajov. Po otestovaní funkčnosti obnoveného stavu nasleduje presun pracovníkov a prevádzky a činnosť organizácie pokračuje v pôvodnom stave.

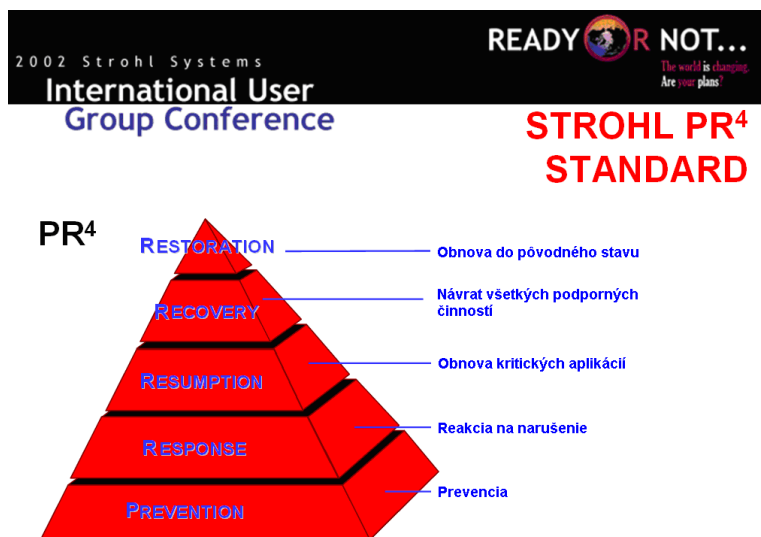
Predpoklady funkčnosti HP. Podmienkou pre vytvorenie fungujúceho systému havarijných plánov je pripraviť vhodné technické a organizačné podmienky.

Pre východiskový stav, analýza IT prostredia poskytuje nasledovné vstupy ovplyvňujúce tvorbu havarijných plánov:

Účinná prevencia môže zabrániť vzniku mnohých škôd, prípadne eliminovať následky, či už hmotné (poškodenie zariadenia, budovy) alebo nehmotné (strata dát, poškodenie dobrého mena spoločnosti). Prevenciou v oblasti IT je hlavne tvorba záloh údajov, bezpečné uloženie záloh ale aj školenia pracovníkov na vznik havarijných situácií.

Najkritickejšia fáza je fáza obnovy, pretože ak sa v nej ukáže, že organizácia nemôže v akceptovateľnom rozsahu obnoviť svoju činnosť, môže to mať ďalekosiahle následky. V tejto fáze sa havarijné tímy riadia havarijnými plánmi. Pre úspešné zvládnutie havarijnej situácie je potrebné zostaviť havarijný tím. Každý člen havarijného tímu musí mať presne stanovené právomoci a zodpovednosť v procese obnovy.

V predkladanom príspevku sme vychádzali z metodológie PR4 (Prevention, Response, Resumption, Recovery, Restoration) firmy Strohl Systems, ktorá je jednou z vedúcich spoločností zaoberajúcou sa havarijným plánovaním s dlhoročnou tradíciou.



Obr. 1 Schéma metodológie PR4 firmy Strohl Systems

ZÁVER

V predkladanom príspevku sme vychádzali z metodológie PR4 (Prevention, Response, Resumption, Recovery, Restoration) firmy Strohl Systems, ktorá je jednou z vedúcich spoločností zaoberajúcou sa havarijným plánovaním s dlhoročnou tradíciou.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

- [1] CHOVANCOVÁ, J. - HERCZNER, P., 2006: *Špecifikácia indikátorov pre účely environmentálneho reportingu*. - In: Novus scientia 2006 : 9. celoštátna konferencia doktorandov technických univerzít a vysokých škôl, 6.12.2006, Košice : Zborník referátov. Košice : TU-SjF, 2006. s. 189-194. ISBN 80-8073-354-6.
- [2] CHOVANCOVÁ, J. - MAJERNÍK, M., 2006: *Environmentálny reporting ako nástroj vonkajšej komunikácie podniku*. - In: Trendy v systémoch riadenia podnikov : 9. medzinárodná vedecká konferencia, Herľany, 26.-27. október 2006 : Zborník príspevkov. Košice : TU, 2006. 6 s. ISBN 80-8073-660-X.
- [3] PROCHÁZKOVÁ, D., 2003: *Krizové řízení – nástroj pro přežití a rozvoj v obtížných podmínkách*. - In: Současnost a budoucnost krizového řízení. T-soft, Praha 2003,30, 03K-KR-09.
- [4] PROCHÁZKOVÁ, D. – DYTRYCH, P., 2004: *Zdroje rizik pro podnik a řízení bezpečnosti podniku*. - In: Metodické problémy oceňování podniku, Ed. M. Mařík. Nakladatelství VŠE, Praha 2004, 303p, ISBN 80-245-0738-2, 250-256.
- [5] RUSKO, M., 2004. *Environmentálne orientovaný manažment v praxi manažéra*. - Žilina: Strix [VeV]. Edícia EV-2, Prvé slovenské vydanie, ISBN 80-969257-1-7, 190 s.
- [6] RUSKO, M., 2006: *Bezpečnostné a environmentálne manažérstvo*. - Bratislava : VeV et Strix, Edícia EV-7 , Prvé slovenské vydanie, ISBN 80-969257-9-2, 389 s.
- [7] STROHL PR4 Standard.[on-line] Available on-URL: ><http://www.strohlsystems.com>< [cit. 2002-12-19]
- [8] ŠESTÁK, B. – PROCHÁZKOVÁ, D., 2005: *Bezpečnost jako jeden ze základních aspektů rozvoje společnosti*. - In: Bezpečnostní teorie a praxe. Sborník PA ČR 2004, díl II, ISBN 80-7251-169-6. PA ČR, Praha 2005, 355-71.

ADRESA AUTORA

Ing. Pavol Vojtek, Sociálna poisťovňa, pobočka Prešov, Slovenská republika, e-mail:
 >Pavol.Vojtek@hotmail.com<

RECENZENT

Doc. Ing. Jozef Halász, PhD., Technická Univerzita, Strojnícka fakulta, Katedra environmentalistiky a riadenia procesov, Park Komenského 5, 042 00 Košice, Slovenská republika