

Mgr. Monika Johaníková

Představení a vývoj řízení kontinuity činností

Anotace

Autorka představuje historii řízení kontinuity činností, důvody, proč tato disciplína začala tvořit součást řízení organizace. Samostatná část je věnována standardizaci systému řízení kontinuity činností.

Klíčová slova

Řízení kontinuity činností, standardizace.

Summary

The author introduces history of business continuity management and the reasons, why this discipline became part of management of organization. Separate part of paper consists information of the standardization of the BCM system.

Keywords

Business Continuity Management, standardization.

1. Základní definice pojmu a historický vývoj business continuity managementu

Existuje mnoho definic, vztahujících se k pojmu business continuity (do češtiny možné přeložit jako „řízení kontinuity podnikání“, „management kontinuity činností organizace“, případně „kontinuita podnikání“¹). Všechny definice přitom zdůrazňují nutnost kombinace manažerských disciplín s aktivitami, které pomáhají zajistit kontinuitu základních funkcí organizace za všech okolností.

Řízení kontinuity podnikání organizace, jak je chápáno dnes, vyplynulo z požadavků na zajištění obnovy informačních systémů po haváriích sálových počítačů. Tradičně se havarijní plánování (Disaster Recovery Planning, DRP) soustřeďovalo na obnovu technického vybavení po větším incidentu. Než se původní koncept DRP přerodil v dnešní „certifikovatelný“ systém řízení kontinuity činností uběhlo téměř 40 let. Myšlenka na vytvoření formalizovaných pravidel a postupů řízení eskalace incidentů pochází z druhé poloviny 70. let XX. století. Autorem této myšlenky byl Norman Harris², viceprezident odpovědný za zpracování dat v Bank of Ohio. V dobách hromadného zpracování dat prostřednictvím děrných štítků znamenala jakákoli drobná či větší závada sálového počítače obvykle narušení práce v celé bance. Norman Harris byl kontaktován bez ohledu na denní nebo noční dobu, bez jakéhokoli pokusu o předběžné posouzení závažnosti a rozsahu incidentu svými podřízenými ihned a zpravidla i zbytečně.³ Potřeba vytvořit a formalizovat postupy hlášení a zvládání ICT (Information and Communication Technologies) incidentů se tak zrodila z nutnosti eliminovat plané poplachy – byl vytvořen první plán obnovy po havárii (Disaster Recovery Plan, DRP).⁴

Od počátku se první tvůrci DRP potýkali s tím, jak přesvědčit vedení svých společností, aby schválilo nemalé investice do tvorby havarijních plánů a přípravy záložních lokalit. Zejména, když se jednalo o přípravu na závažné události a havárie, které s velkou pravděpodobností nikdy ani nenastanou. Investice do DRP bylo nutné zdůvodnit a před majiteli obhájit. To vedlo k vytvoření technik pro hodnocení potenciálních dopadů negativních událostí na celkové fungování společnosti. První metodiky analýz obchodních dopadů (Business Impact Analysis, BIA) vznikaly ve Spojených státech v první polovině 80. let XX. století, a jsou tak o několik let starší než samotný koncept řízení kontinuity činností. Je důležité, že hned od začátku byla podchycena klíčová podstata implementace BCM. Dnes je analýza dopadu na obchod neoddelitelnou a klíčovou součástí životního cyklu BCM.⁵

¹ Tento pojem je obvykle používán v obchodních společnostech v České republice.

² Norman L. Harris, prezident Harris Recovery Solutions, Inc. Je považován za lídra v oblasti Information Technology Management, zakladatel Disaster Recovery Planning.

³ Myšlenka se zrodila jednoho nedělního odpoledne během hry golfu. V dobách bez mobilních telefonů obnášelo vyřízení hovoru cestu do klubovny a zpět na odpaliště jamky č. 13, a to ještě v tom lepším případě.

⁴ ŠIROKÝ, Libor. Od Golfu k certifikaci BCMS. Data Security Management. 2010, 3. <<http://www.rac.cz/rac/homepage.nsf/CZ/Clanky>>.

⁵ ŠIROKÝ, Libor. Od Golfu k certifikaci BCMS. Data Security Management. 2010, 3. <<http://www.rac.cz/rac/homepage.nsf/CZ/Clanky>>.

Vytvoření BCM(S)

Počátky dnešního BCM(S) jsou datovány do poloviny 80. let XX. století. O rozšíření původního, čistě technicky zaměřeného konceptu havarijního plánování se zasloužil Ron Ginn⁶. Jako první si totiž uvědomil, že obnova funkčnosti technologií ještě neznamena automatickou obnovou fungování celé obchodní společnosti. Podle vytvořených a otestovaných DRP již nebyl problém obnovit funkčnost sálových počítačů, včetně obnovy dat ze záloh v záložní lokalitě. Nikdo však již neuvažoval nad tím, že bude nutné do záložní lokality přemístit zaměstnance, vytvořit jim vhodné podmínky pro práci, nastavit postupy pro informování zaměstnanců o nastalé události, vytvořit jejich pracovní náplň v následujících hodinách a dnech po havárii, určit způsob a vymezit rozsah informací podávaných zákazníkům a médiím. Dále pak bylo nutné předem promyslet a zahrnout do plánů obnovy další aspekty související se zajištěním kontinuity a obnovy podnikání. To vše původní koncept plánování po havárii zcela opomíjel. A tak přichází na scénu business continuity management, na který je o několik let později aplikován systémový přístup k řízení kontinuity založený na cyklu PDCA (Plánuj – Dělej – Kontroluj – Jednej; Plan – Do – Check – Act).

Rozdíl mezi BCM a BCM(S)

Organizace, které nemají potřebu deklarovat zavedení procesů řízení kontinuity (např. to jejich zákazníci nevyžadují), vystačí s BCM. Ty společnosti, od kterých stávající nebo potenciální partneři vyžadují vyšší garance spolehlivosti, budou usilovat o získání certifikace BCM(S).⁷

Řízení kontinuity činností (Business Continuity Management, BCM)

BCM je řídicí proces podporovaný vedením společnosti, který identifikuje potenciální dopady ztrát a jehož cílem je vytvořit takové postupy a prostředí, které v případě incidentu, narušení nebo ztráty zajistí kontinuitu a obnovu klíčových procesů a činností organizace v požadovaných časech a na předem stanovené minimální úrovni. Jednotlivé činnosti spojené s implementací BCM jsou souhrnně označovány jako „životní cyklus BCM“. [BS 25999 – 1].

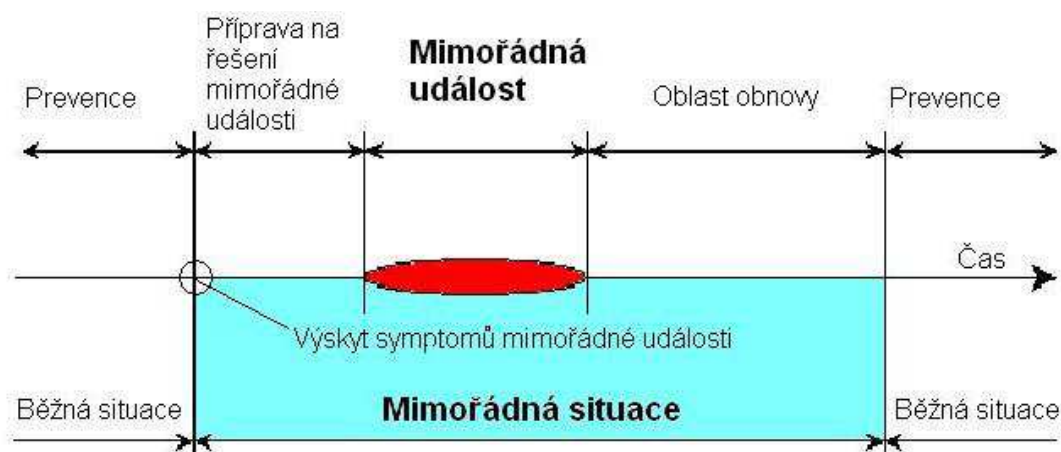
Systém řízení kontinuity činností (Business Continuity Management System, BCMS). Část celkového systému řízení, který prosazuje procesní přístup k implementaci, provozování, monitorování, přezkoumávání a zlepšování všech činností životního cyklu BCM, přičemž systém řízení zahrnuje organizační strukturu, politiky a směrnice, odpovědnosti, postupy, procesy a zejména zdroje. [BS 25999 – 2].

⁶ Jeden z původních zakladatelů britského institutu Business Continuity Institute.

⁷ ŠIROKÝ, Libor. Od Golfu k certifikaci BCMS. Data Security Management. 2010, 3
<<http://www.rac.cz/rac/homepage.nsf/cz/clanky>>.

Od obnovy ke kontinuitě

Byl to rovněž již výše zmiňovaný Ron Ginn, kdo v roce 1985 rozšířený koncept původního DRP (Disaster Recovery Planning) pojmenoval jako řízení kontinuity činností (BCM). V novém světle bylo ICT nutno chápat jako jeden ze zdrojů, které podporují fungování procesů a činností společnosti. Přičemž ale původní postupy a techniky DRP nebyly zatraceny, ale naopak nově aplikovány na mnohem širší okruh procesů a podpůrných činností. Dnes jsou DRP chápány jako podmnožina BCP zaměřená na obnovu ICT zdrojů po incidentu nebo havárii. BCP plány obsahují postupy a kroky pro zajištění kontinuity (přechodné období) a následné obnovy (návrat k normálu) procesů a činností. Dalším logickým krokem ve vývoji BCM byl posun od pouhé obnovy, kdy se pouze vyčkává, až se něco stane, a teprve pak se začíná jednat, ke kontinuitě, kdy jsou dopředu promyšleny kroky obnovy. Jsou zde připraveny i alternativní způsoby fungování v době výpadku. Kde to jde, řeší se prevence a je snaha se hrozbám vyhnout či alespoň pravděpodobnost jejich výskytu minimalizovat (proto je součástí programu BCM také řízení rizik). Namísto pasivního vyčkávání řídí kontinuitu svého podnikání organizace aktivně. Přesto trvalo ještě řadu let, než se tento rozšířený koncept ujal. Ještě dnes je BCM v řadě společností chápáno jako aktivita spadající čistě do působnosti IT oddělení.⁸



Ilustrace: Časová osa řízení kontinuity činností

Počátky BCM(S) certifikace

Prvním standardem, ve kterém se pojem business continuity management objevil, byl britský BS 7799 z roku 1995. Standard, kromě jiných oblastí bezpečnosti, vyzdvihl potřebu zavedení procesu řízení kontinuity činností pro minimalizaci následků a zotavení se ze ztráty informačních aktiv. Události na přelomu tisíciletí rozpoutaly novou vlnu zájmu o havarijní plánování a plánování kontinuity. V roce 2003 zveřejnil Britský

⁸ ŠIROKÝ, Libor. Od Golfu k certifikaci BCMS. Data Security Management. 2010, 3
<<http://www.rac.cz/rac/homepage.nsf/CZ/Clanky>>.

normalizační institut⁹ (British Standard Institution, BSI) veřejně dostupnou specifikaci PAS 56, která sjednotila nejlepší praxi v oblasti řízení kontinuity činností a podle které v následujících letech postupovalo mnoho organizací na celém světě. V roce 2006 byla veřejně dostupná specifikace PAS 56 stažena a nahrazena novou britskou normou pro řízení kontinuity činností BS 25999 – 1. V roce 2007 vydal BSI druhou část tohoto nového standardu, který poskytuje specifikaci pro formální hodnocení schopnosti organizace řídit kontinuitu svých činností. Formální audity BCM(S) probíhají na základě požadavků BS 25999 – 2.

Propojení BCM(S) na ostatní systémy řízení

Systém řízení kontinuity činností patří mezi nejnovější přírůstky systémů řízení. Společně s moderními normami o systémech řízení využívá BS 25999 – 2 pro plánování, zavádění a zlepšování účinnosti systému řízení kontinuity činností cyklus PDCA. Standard je úzce propojen s normami ISO/IEC 9001:2005, ISO/IEC 14001:2004 a ISO/IEC 27001:2005 tak, aby bylo podpořeno jejich konzistentní a jednotné zavedení a provoz. Jeden vhodně navržený systém řízení tak může naplnit společné požadavky všech těchto norem (závazek vedení, řízení zdrojů, požadavky na dokumentaci, interní audity, přezkoumání vedením apod.). Ve svém důsledku tento přístup činí implementaci integrovaného systému řízení (jednotný systém řízení, který splňuje požadavky alespoň dvou systémů řízení) vysoce efektivní.¹⁰

2. Mezinárodní přístupy k řízení kontinuity činností a standardizační procesy

Při hodnocení mezinárodních přístupů k řízení kontinuity činností je možné rozeznat dva důležité zdroje doporučení. První přístup pochází ze Spojeného království, druhý vychází ze zkušeností a praxe ze Spojených států amerických.

Prvním a v současnosti nejvýznamnějším tvůrcem doporučení je Mezinárodní institut pro řízení kontinuity činností (The Business Continuity Institute – The BCI¹¹), který vyvinul a dlouhodobě rozvíjí Směrnice nejlepší praxe.¹² Postavení tohoto konceptu řízení kontinuity se promítlo do britského standardu BS 25999, který se stává uznávaným schématem pro certifikaci organizací s vyzrálým systémem řízení kontinuity.¹³

Druhý pohled, který pochází z USA, lze spojit se zákonem FISMA (Federal Information Security Management Act,¹⁴ přijatý do právního systému USA v roce 2002), který reguluje bezpečnost amerických vládních informačních systémů. V rámci

⁹ British Standards Institution. 2009 [cit. 2011-02-08]. The BSI: Standards, Training, Testing, Assessment and Certification. Dostupné z WWW: <<http://www.bsigroup.com/>>.

¹⁰ ŠIROKÝ, Libor. Od Golfu k certifikaci BCMS. Data Security Management. 2010, 3 <<http://www.rac.cz/rac/homepage.nsf/CZ/Clanky>>.

¹¹ V roce 1994 vznikl ve Spojeném království Business Continuity Institute, který převzal Practices jako svůj základní dokument a dále ho rozvíjel. V roce 2002 BCI vydal dokument Business Continuity Management.

¹² Good Practice Guidelines, který je každoročně aktualizovaný. Následně v roce 2006 vydal BCI britský standard BS 25999 jako standard pro BCM.

¹³ Business Continuity Institute Good Practice Guidelines, BCI 2008 <<http://thebci.org/gpg.htm>>.

¹⁴ Computer Security Division 2002 [cit. 2011-02-08]. NIST National Institute of Standards and Technology. <<http://csrc.nist.gov/groups/sma/fisma/index.html>>.

definovaných pravidel Národního institutu pro standardy a technologie (NIST) publikuje mnoho doporučení, která jsou určena pro zvýšení bezpečnosti vládních informačních systémů Spojených států amerických. Nicméně tato pravidla a doporučení jsou intenzivně využívána i pro řadu komerčních či nevládních informačních systémů. Mezi organizací publikované NIST dokumenty patří i směrnice pro řešení mimořádných a krizových situací včetně dokumentů pro řízení podpory kontinuity managementu.¹⁵

Standardizační procesy

V oblasti řízení kontinuity činností existovalo v minulosti velké množství různých doporučení a metodik, ale chyběl všeobecně uznávaný standard, který by tyto činnosti zastřešil. S cílem definovat výchozí principy a jednotnou terminologii a zavést základní rámec na řízení kontinuity činností byla v roce 2003 vydaná veřejně dostupná specifikace (Publicly Available Specification) PAS 56. Základem pro PAS 56 byla publikace GPG02 – Good Practice Guidelines z roku 2002, která obsahovala soubor vybraných praktik a doporučení pro oblast řízení kontinuity činností. Specifikace PAS 56 byla připravena a vydána britským normalizačním institutem – British Standard Institution (BSI) ve spolupráci s Business Continuity Institute (BCI). V roce 2005 prošla GPG aktualizací (GPG 05). Specifikace PAS 56 a publikace GPG05 se stali východiskem pro standard BS 25999, který se skládá ze dvou částí.¹⁶

První část se nazývá A Code of Practice for Business Continuity, druhá část pak Specification for Business Continuity Management.

BS 25999 – 1: 2006 A Code of Practice for Business Continuity, definuje zásady, terminologii a doporučení pro tvorbu procesu řízení kontinuity činností, dále její implementaci BCM uvnitř organizace a také obsahuje pravidelné řešení BCM ve vztahu organizace – zákazník. Norma dále definuje etapy životního cyklu BCM a opatření, která jsou v ní uvedena, vychází z nejlepších praktik používaných v rámci řízení kontinuity činností.

BS 25999 – 2: 2007 Specification for Business Continuity Management slouží k zavedení a certifikaci systému řízení kontinuity činností v organizaci. Je kompatibilní s normou řízení kvality ISO 9001. Umožňuje tedy integraci a sdílení společných zdrojů (například v oblasti dokumentace).¹⁷

V roce 2012 byla na základě nových praktických poznatků a inovovaných postupů vydána norma ISO 22301:2012 – Ochrana společnosti - Systémy BCM – Požadavky. Tato norma upravuje opatření pro nastavení systému řízení kontinuity činností v organizaci. Struktura standardu je tvořena tak, aby byly obecně popsány veškeré kroky a náležitosti, které jsou nezbytné pro formální ověření komplexnosti nastaveného systému. Detailnější popisy jednotlivých kroků a částí systému jsou součástí standardu ISO/IEC 22313:2012 – Ochrana společnosti – Systémy BCM – Poučení.

¹⁵ DOUCEK, Petr; NOVÁK, Luděk. Když ICT nefungují – řízení kontinuity činností. Systémová integrace. 2010, 2, s. 43 – 52.

¹⁶ ČSN BS 25999 – 1. Management kontinuity činností organizace – Část 1: Soubor zásad. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. s. 49.

¹⁷ SZABADOS, Ľubomír, et al. Business Continuity Management: Příručka manažera. Bratislava: TATE International Slovakia, 2008. s. 49.

Důležitou součástí souboru norem je také ISO 27301:2011 – Informační bezpečnost – Bezpečnostní techniky – Poučení pro připravenost informačních a komunikačních technologií na kontinuitu činností.

Výhody aplikace BCM do organizace

Program BCM se stal ve většině velkých firem a organizacích důležitou součástí dobrého a kvalitního managementu. Manažeři a vlastníci mají odpovědnost za udržení schopnosti organizace fungovat bez přerušení. Organizace neustále vytvářejí závazky, např. uzavírají kontrakty nebo mají povinnost dodávat produkty. Mají také morální a sociální odpovědnost, především když poskytují odezvu na stav nouze nebo veřejnou či dobrovolnou službu.

Ale každá činnost v organizaci může být předmětem přerušení. Například může dojít k selhání počítačových technologií, záplavám, narušení funkce organizace, úmyslnému poškození organizace nebo dokonce k teroristickému útoku na organizaci. BCM poskytuje schopnost adekvátně reagovat na přerušení provozu při současné ochraně prosperity a zajištění bezpečnosti.

Pokud je program v organizaci efektivně zaveden přináší mnoho **výhod**. Mezi ně patří například to, že organizace je schopna proaktivně identifikovat dopady přerušení provozu. Po identifikaci bude mít k dispozici efektivní odezvu na přerušení, která minimalizuje dopady na celou organizaci.

Některá rizika pro organizaci jsou nepojistitelná, tudíž bude mít schopnost neustále udržovat na přijatelné úrovni i tato nepojistitelná rizika. Tím získá konkurenční výhodu pomocí prokázané schopnosti udržovat dodávky, čímž také zvyšuje svou reputaci.¹⁸ Program BCM se implementuje do celé organizace, tím se podpoří a posílí spolupráce mezi týmy, odděleními nebo pobočkami v organizaci. V neposlední řadě je také schopna prokázat věrohodnost odezvy pomocí procesů procvičování.

Výsledky efektivního programu BCM uvedené v normě ČSN BS 25 999-1 jsou neoddiskutovatelné. V organizaci dochází k tomu, že:

- klíčové produkty jsou identifikovány a chráněny a tím je zajištěna jejich kontinuita;
- je umožněna způsobilost managementu incidentů k zajištění efektivní odezvy;
- porozumění organizace sobě samé a svým vztahům s ostatními organizacemi, relevantními regulačními orgány nebo vládními resorty, místní samosprávou a bezpečnostními a záchrannými složkami je správně vytvořeno, dokumentováno a chápáno;
- u personálu je pomocí příslušného testování prováděn výcvik pro efektivní reagování na incident, nebo přerušení;
- jsou pochopeny a plněny požadavky zainteresovaných stran;
- personál má v případě přerušení k dispozici adekvátní podporu a komunikační prostředky;

¹⁸ ČSN BS 25999 – 1. Management kontinuity činností organizace – Část 1: Soubor zásad. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. s. 12 – 13.

- je zajištěn dodavatelský řetězec organizace;
- je chráněna reputace organizace a funguje v souladu s požadavky zákonů a předpisů.¹⁹

Jak je uvedeno v předchozím odstavci, podpora managementu je pro implementaci BCM klíčová. Jen management je oprávněný přijímat strategické rozhodnutí, disponuje zdroji a stanovuje priority. Získat důvěru managementu není vůbec jednoduchou záležitostí, proto je nutné managementu vysvětlit proč BCM vyžaduje jejich stálou podporu, jaké jsou důvody pro zavedení BCM a srovnat náklady a výnosy se zavedením BCM.²⁰

Zavedení programu kontinuity podnikání do organizace přináší mnoho výhod nejen pro organizaci samotnou, ale má také velký přínos pro bezpečnost státu. Stát totiž vnímá podnik nejen jako potencionální zdroj rizika, nebo jako objekt působení bezpečnostním rizik, ale vidí ho i jako dodavatele nezbytných (mobilizačních) dodávek²¹. Při zajišťování bezpečnosti nedokáže pokrýt z vlastních zdrojů všechny krizové situace, proto se spoléhá na statky a služby vyprodukované podnikatelskými subjekty²². Tyto podnikatelské subjekty se tedy zavazují k nepřetržité činnosti. Při aplikaci BCM nebo jiných bezpečnostních programů (plánů) organizace zvyšují svoji odolnost vůči incidentům a budou schopny dostát závazkům nejen vůči zákazníkům nebo dodavatelům, ale i vůči státu.

¹⁹ ČSN BS 25999 – 1. Management kontinuity činností organizace – Část 1: Soubor zásad. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. s. 12.

²⁰ SZABADOS, Ľubomír, et al. Business Continuity Management: Příručka manažera. Bratislava: TATE International Slovakia, 2008. s. 96.

²¹ Více v zákoně č. 241/2000 Sb.; o hospodářských opatření pro krizové stavy.

²² HRAZIN, Lukáš; LUŽA, Oldřich. Ekonomika při řešení krizových situací: Vybrané kapitoly. Praha: Policejní akademie České republiky v Praze, 2010. Úloha podnikové sféry v civilním nouzovém plánování, s. 30-33.