

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Business Continuity Management jako jeden z nástrojů zvládání rizik

Ing. Martin Tobolka

AEC, spol. s r.o.





Co je BCM ?

- Mezi časté příčiny přerušení kontinuity činností patří
 - technická selhání (energie, HW, SW),
 - přírodní živly (požár, působení vody),
 - lidský faktor (hrozby úmyslné i neúmyslné) apod.
- Řízení kontinuity činností (Business Continuity Management) je proces, který připraví organizaci na řešení těchto situací a zmírní jejich následky.
- Nejdůležitější je správně se připravit na krizové události, včas odhalit tuto událost, určit její příčinu a následně obnovit základní (nouzové) funkce organizace.

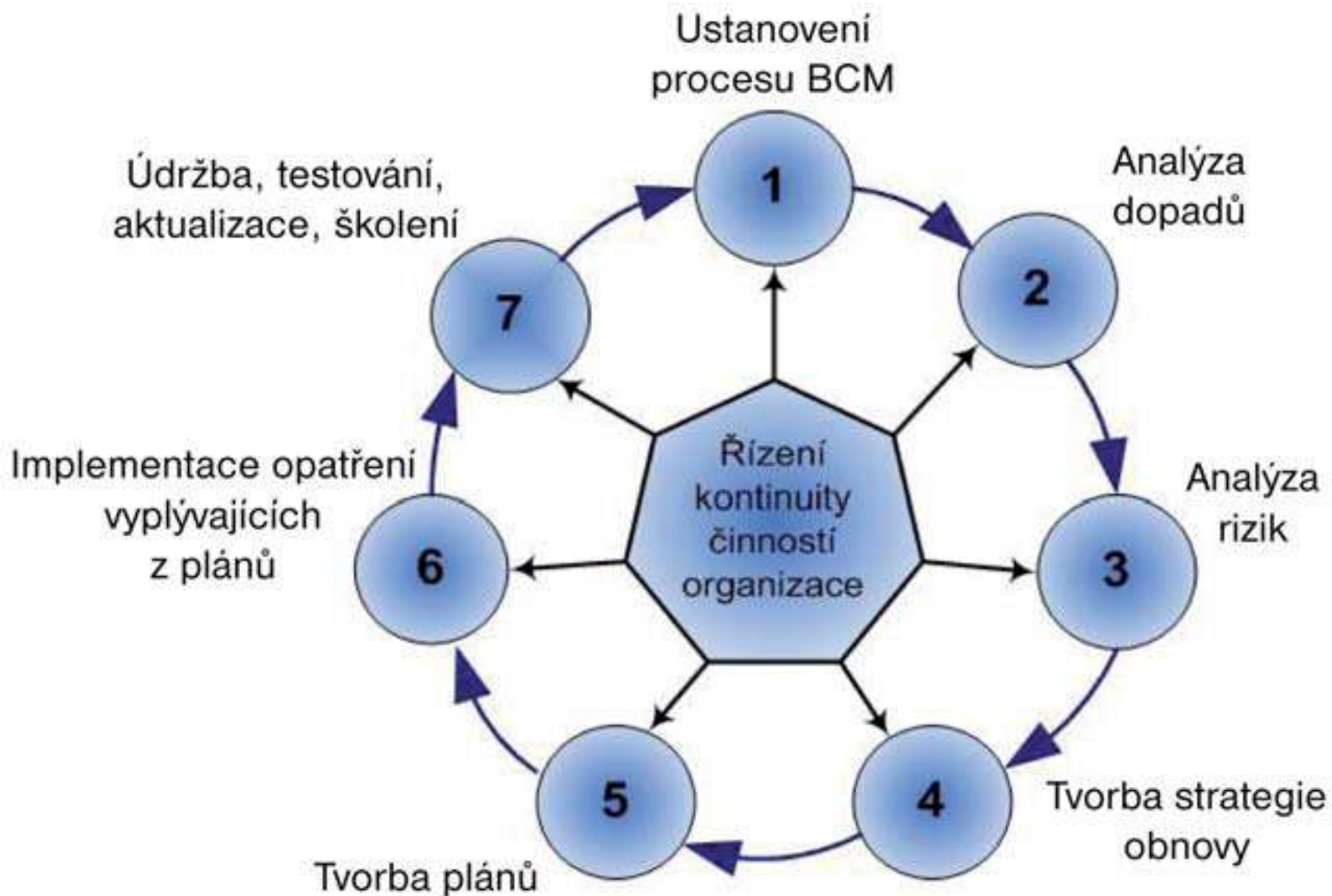


Proč řešit BCM ?

- Snížení finančních ztrát v případě přerušení kontinuity organizace.
- Poskytnutí záruk vůči zákazníkům, akcionářům a managementu organizace díky zajištění kontinuity hlavní podnikatelské činnosti v době havárie.
- Pomocí analýzy dopadů jsou identifikovány finanční náklady při výpadcích konkrétních procesů společnosti.
- Je na míru vypracována strategie obnovy klíčových procesů včetně priorit obnovy a zajištění nouzového provozu.
- V této oblasti, více než jinde, platí, že prevence je vždy vhodnější a zejména levnější než následné odstraňování škod.



Zavádíme BCM





Podklady strategie obnovy

- **Analýza dopadů:** určení kritických procesů organizace, kvantitativní ohodnocení možných dopadů a případných ztrát při realizaci hrozby. Jsou identifikovány maximální doby nedostupnosti kritických procesů, identifikovány zdroje pro obnovu činností a stanoveny minimální úrovně zdrojů nutné pro dosažení stanovených lhůt obnovy činnosti.
- **Analýza rizik IS:** Zahrnuje identifikaci aktiv, relevantních hrozeb a zranitelností, které působí na aktiva. Je řešena pravděpodobnost jejich uskutečnění s určením nejvíce ohrožených kritických činností. Dále jsou posouzena zavedená opatření a je stanovena přijatelná úroveň rizika a stanoven plán opatření.
- Na základě analýzy dopadů je **stanovena strategie** řízení kontinuity činností a určeny **priority obnovy kritických procesů** a jejich požadavky na prostředky IS/ICT.



Výstupy BIA

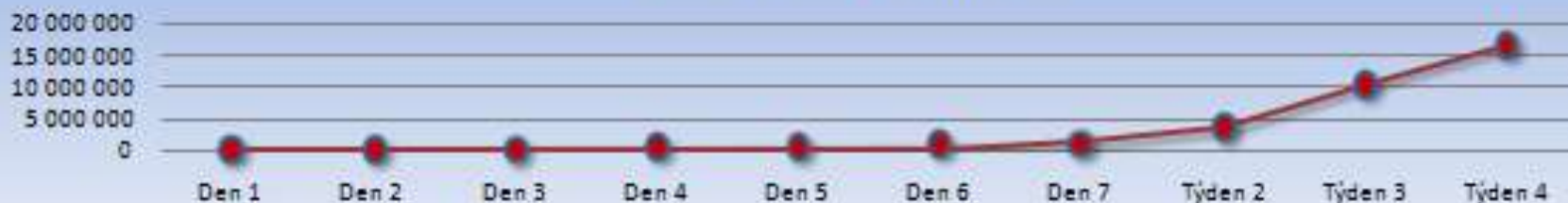
Ztracený obrat



Fixní náklady



Dodatečné náklady



Zdroj: data poskytnutá BCM zákazníkem AEC



Dopad 1 z N nefunkčních procesů



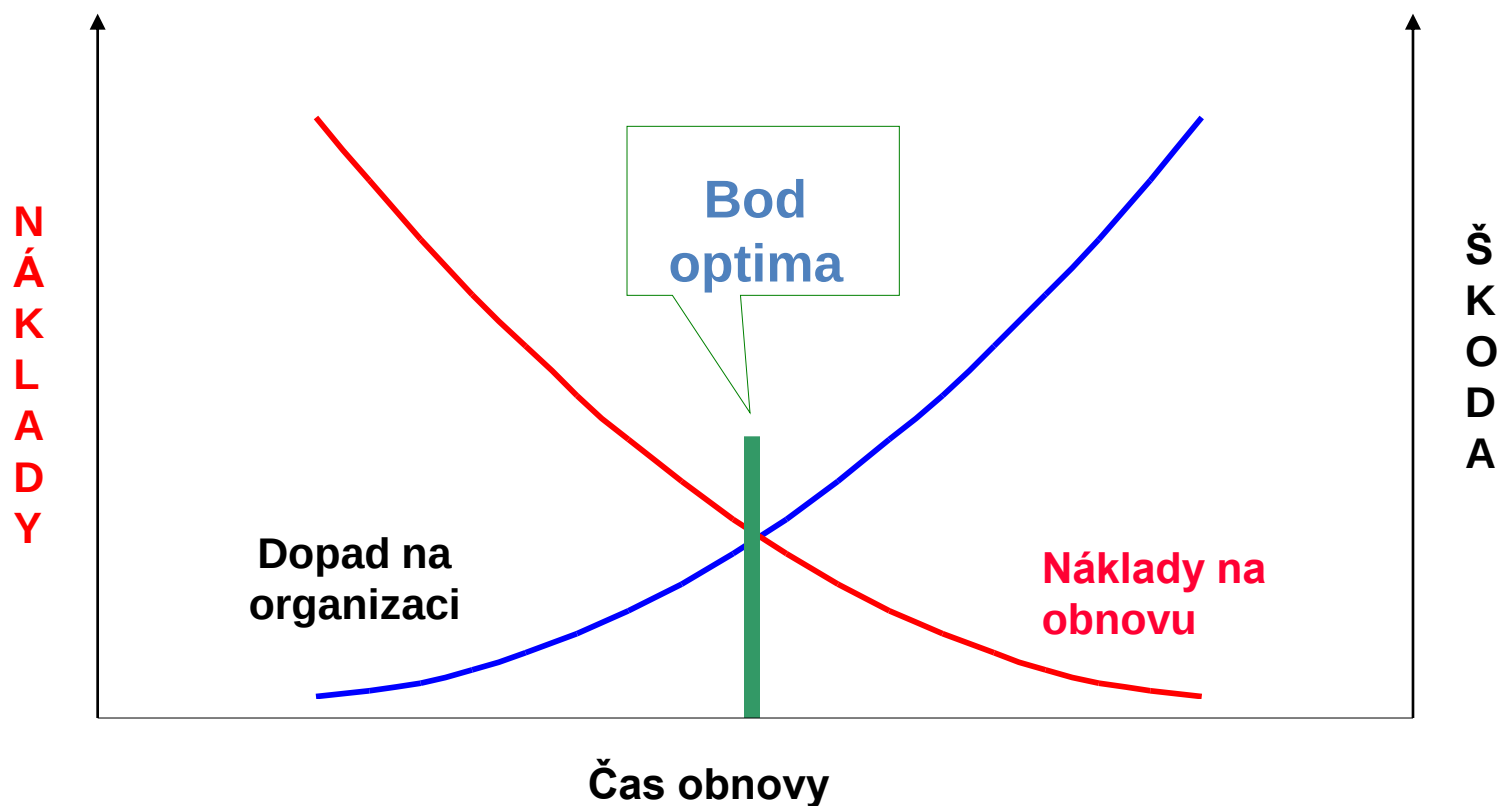
Zdroj: data poskytnutá BCM zákazníkem AEC

16. února 2011

SECURITY 2011



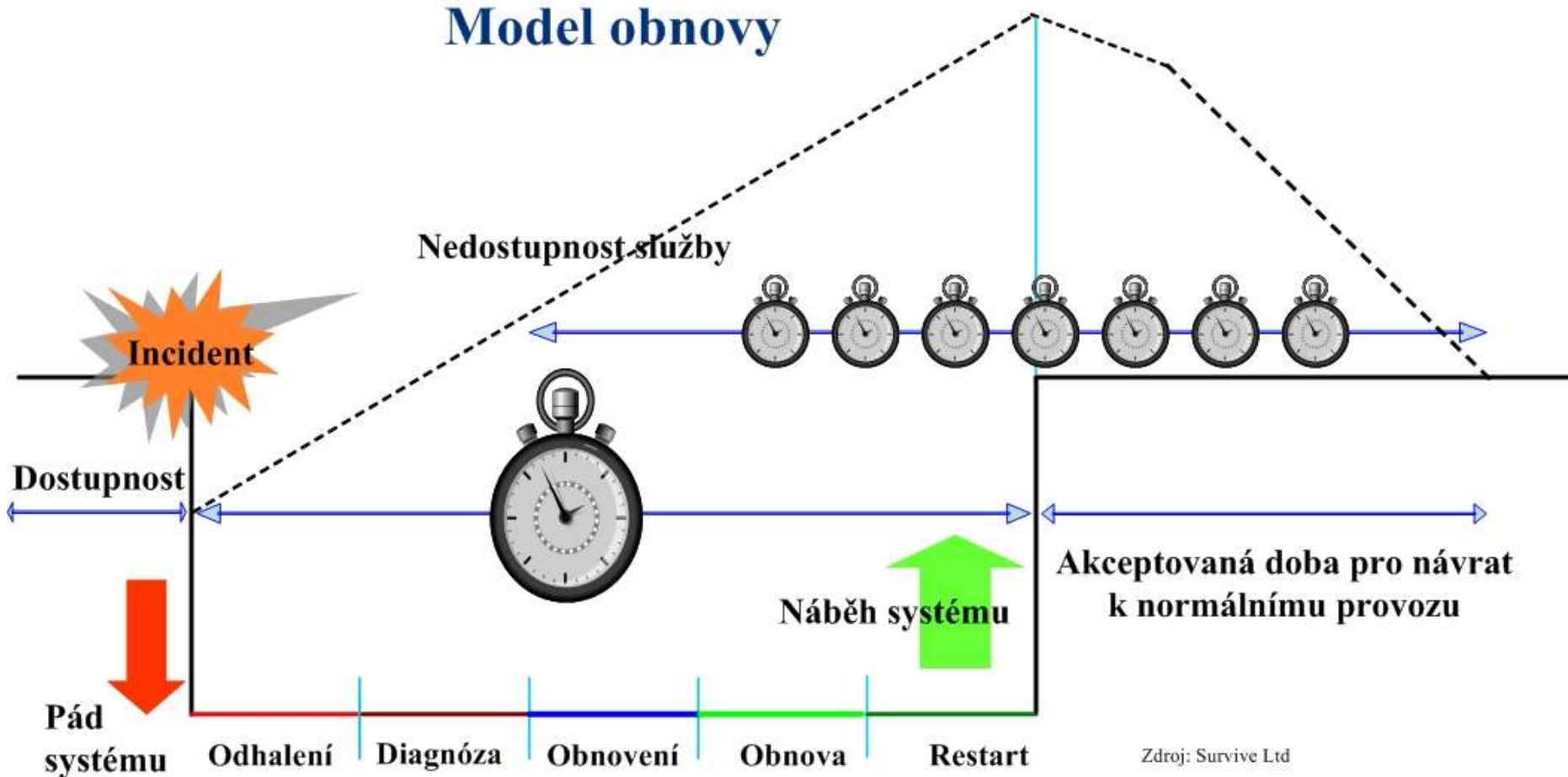
Optimální náklady k pokrytí BCM



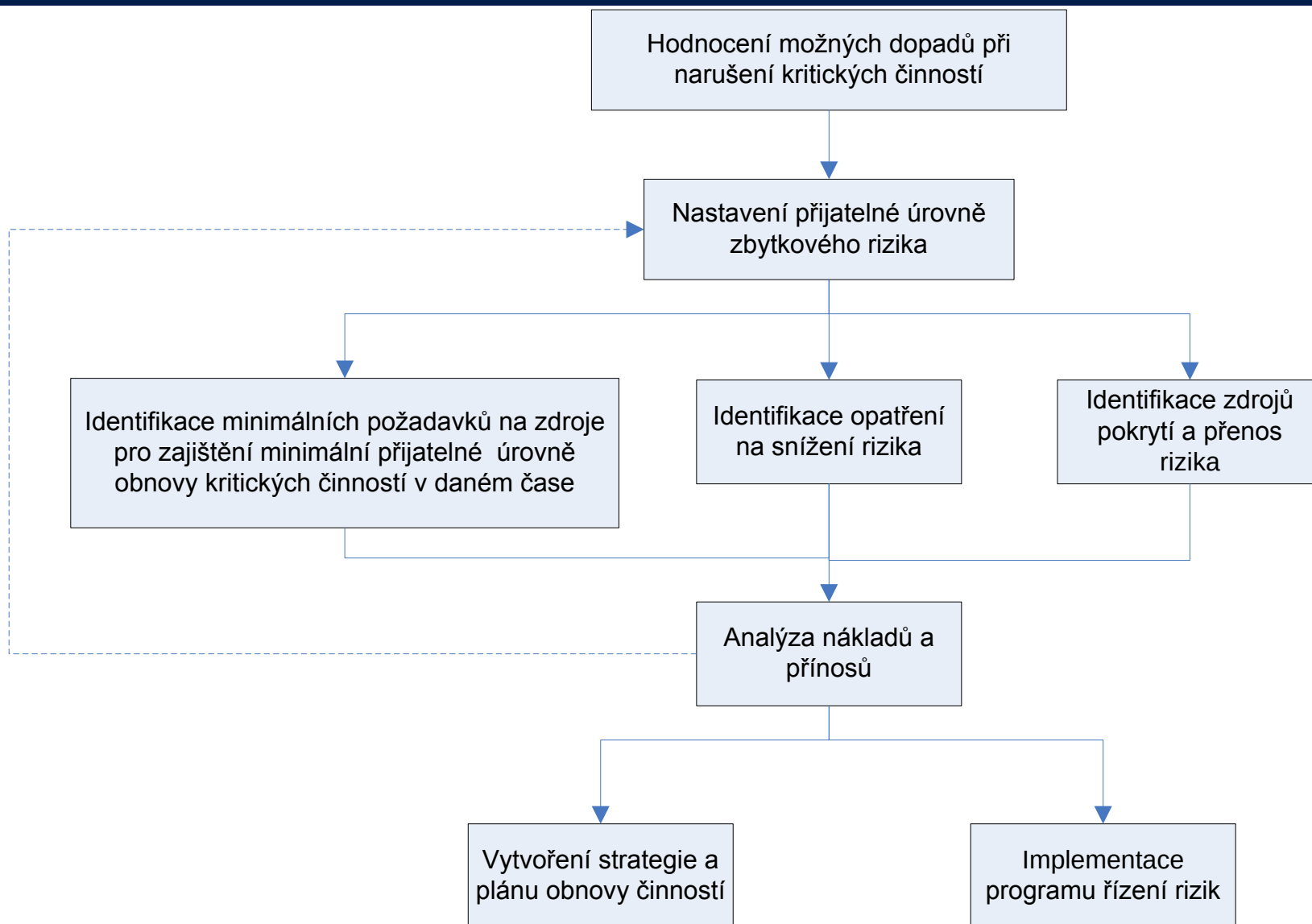


Časový průběh nedostupnosti

Model obnovy



Tvorba strategie obnovy





Tvorba BCM

- Plán kontinuity organizace (BCM)
 - tvoří základní dokument, ve kterém jsou definovány jednotlivé role, týmy, vazby apod.
 - určeny strategie a procesy pro řízení zachování provozu organizace
 - mohou být zdokumentovány v navazujících dokumentech
- Havarijní plán
 - popisuje činnosti, které je potřeba začít provádět bezprostředně po zjištění mimořádné události.
 - jsou určeni kompetentní lidé a jejich kontakty



Tvorba BCM

- Plán nouzového provozu
 - definuje pracovní postupy a činnosti, kterými lze udržet kritické procesy alespoň v omezené míře
 - časová osa a návaznosti dílčích plánů obnovy
 - cílem je minimální dopad na chod organizace
- Plán obnovy
 - většinou technicky nebo speciálně zaměřené plány určené pracovníkům konkrétních týmů obnovy
 - startují je ukončením havarijního plánu
 - vedou k obnovení běžného provozu před incidentem



Praktické užití BCM – reálný přínos

Účinnost plánů obnovy při použití v případě incidentu za období 2007-2009.

V průzkumu jsou společnosti s nejméně 100 zaměstnanci. Mezi nimi jsou nejvíce zastoupeny (61 %) společnosti do 500 zaměstnanců.



Zdroj: Průzkum stavu informační bezpečnosti V ČR 2009, NBÚ, Ernst & Young



Testování BCM

- Teoretické testy
 - kontrola obsahu
 - průchod plánem a/nebo infrastrukturou
 - simulační
- Praktické testy
 - funkční
 - úplné přerušení
- Nesoustředit se pouze na testování ICT, ale věnovat se účastníkům plánu, jejichž znalosti, dovednosti a schopnosti správně se rozhodnout jsou klíčové.
- Nutná pravidelná revize postupů - řízení změn.



Četnost testování v organizacích



Zdroj: Průzkum stavu informační bezpečnosti V ČR 2009, NBÚ, Ernst & Young

16. února 2011

SECURITY 2011



Normativní podklady

- ISO/IEC 27001 – část Řízení kontinuity činností organizace
 - díky certifikaci ISMS dnes nejčastější důvod zavedení BCM
- ČSN BS 25999-1:2006 a BS 25999-2:2007,
 - dříve PAS 56
 - BCM jako součást celkového řízení organizace
 - možnost certifikace
- BS 25777:2008
 - vychází z PAS 77
 - doporučení pro řízení kontinuity ICT s souladu s celkovým Business continuity managementem dle BS 25999:2006



Mám BCM a klidně spím – proč?

- Fungující řízení kontinuity činností společnosti je vytvoření a implementace efektivního a zaměstnanci pochopeného procesu obnovy kritických procesů a technologií v případě havarijní situace.
- V případě havárie ve Vaší společnosti Vám plán kontinuity zajistí obnovu klíčových procesů aniž by to mělo negativní dopad na plnění stanovených podnikatelských záměrů, smluvních povinností a závazků vůči zákazníkům.
- Po implementaci řízení kontinuity víte, jak zvládnete provoz ICT při nejčastějších technických selháních (výpadek dodávek energie, selhání technického nebo programového vybavení), při působení přírodních živlů (požár, povodeň), selhání lidského faktoru (chyby uživatelů, podvody, krádeže, napadení IS) apod.



Podíl organizací se zavedeným BCM

Po skokovém zlepšení se v této oblasti dostáváme asi opět pomalu do dlouhodobého normálu, kdy je rozdělení společností, které mají a nemají vypracovány plány obnovy funkčnosti zhruba „fifty-fifty“.

After a sudden improvement in this sphere we are gradually returning to the long-term norm, i.e. the division of companies which have and do not have disaster recovery plans in place is about fifty-fifty.



Zdroj: Průzkum stavu informační bezpečnosti V ČR 2009, NBÚ, Ernst & Young

16. února 2011

SECURITY 2011

Děkujeme za pozornost.

Ing. Martin Tobolka
AEC, spol. s r.o.
martin.tobolka@aec.cz

