TVORBA BEZPEČNOSTNÍ POLITIKY ORGANIZACE A HAVARIJNÍHO PLÁNU

Dagmar Brechlerová
KIT PEF ČZU, Praha 6, Kamýcká, dagmar.brechlerova@seznam.cz

ABSTRAKT:
Budování bezpečnosti v organizaci není amatérská činnost, ale řídí se normami nebo dokumenty, které sice nejsou normou, ale „de facto“ normou. V příspěvku jsou popsány některé používané postupy a to zejména ISMS tj. Information Security Management System dle normy ISO/IEC 27001:2005 a BCM Business Continuity Management dle PAS56.

ABSTRACT:
Building of IT security nowadays cannot be taken unprofessionally. It is necessary to use specialized instruments. This document describes instruments for security building in some organization. There are utilities such as ITIL, COBIT, but the most important for security building is the Information Security Management System according of ISO/IEC 27001:2005. There are also other security standards from 27000 line ISO standards. For BCM Business Continuity Management there are other norms and standards, for example PAS56.

KLÍČOVÁ SLOVA:
ISMS, havarijní plán, PAS56, ISO/IEC 27001:2005

Úvod:
Pro řízení bezpečnosti informací existuje mnoho postupů, návodů, standardů a norem, které v různé výši naplňují představu o efektivním a komplexním řízení bezpečnosti informací v organizaci. Mezi základní požadavky na řízení bezpečnosti informací patří:

- jednoduchost tj. snadná implementace a provoz řízení bezpečnosti
- efektivnost tj. maximalizace přínosů z vložených investic
- účinnost tj. skutečné řízení rizik
- hospodárnost tj. minimalizace nákladů
- prokazatelnost tj. možné reportování výsledků a možnost získání některé uznávané certifikace.

Mezi nejpoužívanější systémy řízení bezpečnosti informací patří ITIL Security Management, Cobit a ISO 27001. Tyto možnosti jsou podrobněji popsány dále. Dále je popsána metodika pro budování havarijních plánů PAS 56.

ITIL (Information Technology Infrastructure Library)

Standard ITIL vznikl jako knihovna doporučení pro řízení IT služeb a infrastruktury informačních systémů. V rámci ITIL jsou vydávány publikace obsahující Best Practices a Know how pro oblasti IT služeb, vzdělávání IT odborníků, certifikace společností, poskytování IT konzultačních služeb, vývoje a implementace softwarových nástrojů pro podporu procesů řízení služeb informačních technologií. ITIL také tvoří platformu pro profesionály z oboru a odbornou veřejnost. [1]

Cobit (Control Objectives for Information and related Technology)

Cobit je metodikou, definující postupy a procesy podporující systémové řízení, kontrolu a audit informačních technologií. Je založena na souboru mezinárodně uznávaných nejlepších

praktik a vědomostí. Smyslem postupů Cobit [2] je zajistit, aby užívání a nasazování informační infrastruktury bylo v souladu se strategickými cíli organizace a přispívalo k jejímu dlouhodobému rozvoji.

ISO/IEC 27001:2005

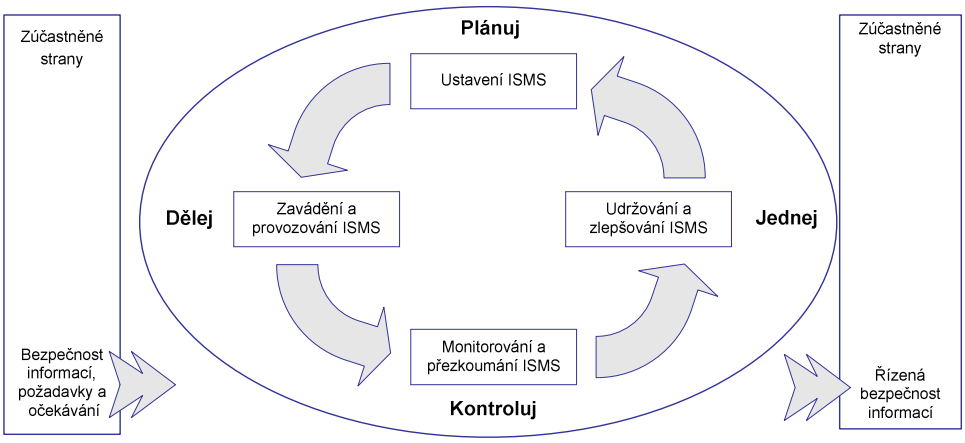
V současnosti nejpoužívanějším standardem pro zavádění systému řízení bezpečnosti informací ISMS tj. Information Security Management System do organizace je norma ISO/IEC 27001:2005 (dále jen ISO 27001). [3] Tato norma byla uveřejněna Mezinárodní organizací pro normalizaci ISO v roce 2005. Norma je aktualizovanou verzí Britského standardu BS 7799-2:2004 – *Information technology - Security techniques - Information security management systems - Requirements* (dále jen BS 7799-2).

ISO 27001 zavádí systémový a komplexní přístup k řešení bezpečnosti informací a představuje prakticky využitelný návod k implementaci systému řízení bezpečnosti informací do organizace. Norma nejen řeší problematiku nakládání s informacemi zpracovávanými výpočetní technikou a informačními systémy, ale definuje i pravidla a postupy při práci s informacemi obecně (např. s tištěnými dokumenty). Pokrývá všechny oblasti bezpečnosti informací:

- Administrativní: soulad s legislativními předpisy, organizačním řádem, interními normami organizace atd.
- Logická: definice postupů a procesů.
- Fyzická: bezpečnost prostředí.
- Technická: bezpečnostní prostředky a technologie.

Norma zavádí tzv. „procesní přístup“ k ISMS - Information Security Management Systems. Pojímá všechny činnosti v organizaci jako procesy, které je nutno identifikovat, popsat, řídit a zlepšovat. Každá činnost, která využívá zdroje a je řízena za účelem přeměny vstupů na výstupy, může být považována za proces. Výstup z jednoho procesu tak tvoří vstup pro další proces. K tomuto účelu využívá tzv. PDCA model (Plan/Plánuj-Do/Dělej-Check/Kontroluj-Act/Dělej). Tento model je možné použít ve všech procesech řízení bezpečnosti informací, kde zajišťuje kontinuální zlepšování ISMS (viz Obrázek 1).

PDCA nemusí být pouze jedním lineárním procesem, lze jej chápat spíše jako nekonečný proud PDCA smyček, které probíhají současně, navazují na sebe a mohou se i částečně překrývat. Díky trvalému procesu PDCA je možné řídit bezpečnost, i v tak heterogenním prostředí plném neustálých změn, jako je IT. ISMS je tedy založen na neustálém opakování PDCA cyklu.



Obrázek 1 - PDCA model aplikovaný na procesy ISMS,Zdroj: ISO/IEC 27001:2005 : Překlad a interpretace pro české prostředí.: Risk Analysis Consultants, s.r.o., 2005. 31 s.

ISO 27000 tvoří více norem, jde o celou sérii. Jádrem je ISO 27001, která poskytuje model pro zavedení efektivního systému řízení bezpečnosti informací v organizaci a doplňuje tak normu ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management (dále jen ISO 27002). Obě normy jsou úzce propojeny, každá z nich však plní jinou roli. Norma ISO 27002 je podrobným přehledem (katalogem) bezpečnostních opatření, která mohou být vybrána při budování ISMS, norma ISO 27001 specifikuje požadavky na to, jak ISMS v organizaci správně implementovat a provozovat..

ISO 27001 tedy poskytuje podporu pro ustavení, zavedení, provozování, monitorování, udržování a zlepšování systému řízení bezpečnosti informací. Norma prosazuje přijetí procesního přístupu při realizaci ISMS. Důraz klade na:

- pochopení požadavků na bezpečnost informací a potřebu stanovení politiky a cílů bezpečnosti informací
- zavedení a provádění kontrol v kontextu s řízením celkových rizik činností organizace
- monitorování a přezkoumávání funkčnosti a efektivnosti ISMS
- neustálé zlepšování ISMS založené na objektivním měření

Etapy řešení bezpečnosti podle ISMS - přípravné části

- Zhodnocení kladů a záporů
- Příprava managementu a rozhodnutí o zavedení ISMS
- Výběr standardu
- Souhlas managementu
- Určení základních východisek a cílů projektu

Realizace projektu

- GAP analýza
- Analýza rizik
- Implementace opatření
- Prověrka souladu

Navrhovaná struktura bezpečnostní dokumentace pro organizaci vyplývající z tvorby bezpečnosti v souladu s normou ISO

Podle normy ISO 27001 a ISO 27002 **musí být dokumentace jasně formalizována,** ale přitom musí samozřejmě odrážet skutečné potřeby organizace. Jak uvedeno dříve, provádí se postupně PDCA cyklem, takže nejdříve vznikne základní dokumentace, která se poté rozpracovává.

Podle ISMS **musí !!!! dokumentace obsahovat následující:**

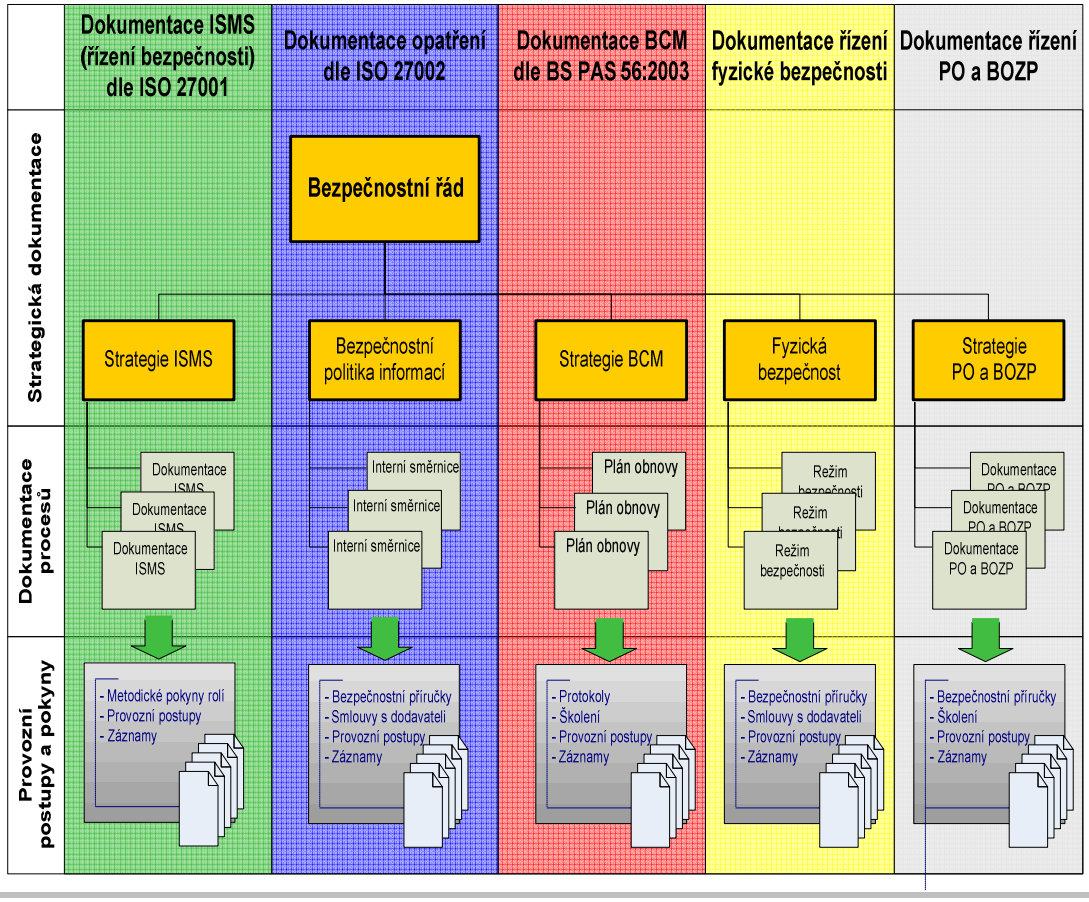
a) Dokumentovaná prohlášení politiky a cílů ISMS
b) Rozsah ISMS
c) Postupy a opatření podporující ISMS
d) Popis použitých metodik hodnocení rizik
e) Zprávu o hodnocení rizik
f) Plán zvládání rizik
g) Dokumentované postupy nezbytné pro zajištění efektivního plánování, provozu a řízení procesů bezpečnosti informací organizace a popis toho, jakým způsobem je měřena účinnost zavedených opatření
h) Záznamy vyžadované touto normou
i) Prohlášení o aplikovatelnosti

Rozsah dokumentace se může lišit podle velikosti organizace, typu činnosti organizace a požadavcích na bezpečnost. Dokumenty mohou být v jakékoliv formě a na jakémkoliv nosiči. Norma obsahuje pro jednotlivé vyžadované dokumenty vždy odkaz, kdy a jak vznikají.

Dokumenty požadované ISMS musí být chráněny a řízeny. Musí být vytvořen dokumentovaný postup tak, aby vymezil řídící činnosti potřebné k

a) schvalování obsahu dokumentů před jejich vydáním
b) přezkoumání dokumentů, případně jejich aktualizaci a opakovanému schvalování
c) zajištění identifikace změn dokumentů a aktuálního stavu revize dokumentů
d) zajištění dostupnosti příslušných verzí aplikovatelných dokumentů v místech jejich používání
e) zajištění čitelnosti a snadné identifikovatelnosti dokumentů
f) zajištění dostupnosti dokumentů pro všechny, kteří je potřebují, zajištění přenášení, ukládání a likvidace dokumentů v souladu s potupy odpovídající jejich klasifikaci
g) zajištění identifikace dokumentů externího původu
h) zajištění řízené distribuce dokumentů
i) zabránění neúmyslného použití zastaralých dokumentů
j) aplikování jejich vhodné identifikace pro případ dalšího použití

Následující obrázek ukazuje možnou základní strukturu dokumentace.



Obrázek 2 - Možná struktura vzniklé dokumentace podle ISMS

U dokumentace je nutné dodržet, aby odpovídala platné legislativě ČR a nebyla s ní v rozporu, aby byla v souladu s jinými normami organizace a aby byla vynutitelná. U té dokumentace, která je určena zaměstnancům, je nutné, aby s ní byli seznamováni, školeni atd. Formalizace této dokumentace je určena normou ISO 27001 a ISO 27002. Opět připomínáme, že celé budování může probíhat v několika smyčkách, takže v další smyčce může vzniknout další dokumentace na doladění již uvedené.

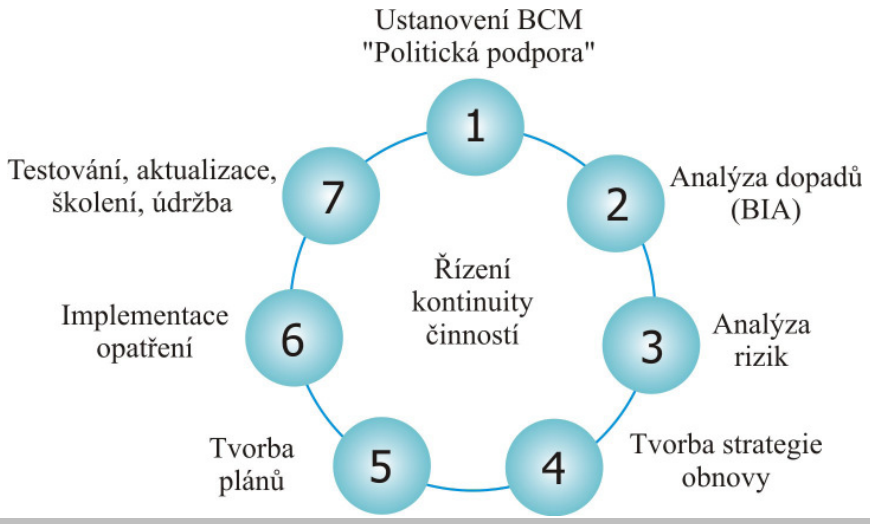
Business Continuity Management

BCM Business Continuity Management (řízení kontinuity činnosti organizace) dle PAS 56 (Publicly Available Specification, nejedná se o normu, ale o veřejně dostupnou specifikaci).

U jednotlivých etap atd. se neuvádí možné či doporučované výstupy, jde o stovky možností, které je možné po rozhodnutí pro realizaci BCM dohledat v PAS 56 a podle nich se inspirovat. Řízení kontinuity je pro každou organizaci speciální, šité na míru, neexistuje obecně, nejde jen po obnovení IT po havárii, ale o krizové řízení, řízení rizik a obnovování technologií. Činnost BCM je přímo propojena s podnikovým řízením. Nejde jen o reaktivní opatření, ale aktivní zvyšování odolnosti proti narušení, přerušení poskytovaných funkcí nebo ztrátě funkcí. Řízení kontinuity se musí plánovat napříč celou organizací, jde o vazbu mnoha součástí.

Musí existovat role **manažer BCM**, který může být spojen s bezpečnostním manažerem. Materiál PAS 56 pomáhá manažerovi BCM vytvořit BCM a implementovat BCM. Doporučená opatření je nutno vždy přizpůsobit organizaci konkrétně dle jejích potřeb.

Následující obrázek ukazuje životní cyklus. Jde ale o kontinuální cyklický proces (jako ostatně při tvorbě bezpečnosti je obvyklé), takže po 7 opět může následovat 1



Obrázek 3 - Životní cyklus BCM

Nutná pravidla pro řízení programu BCM:

Musí jít o standardní řídící proces řízený z nejvyšších pozic organizace.
Musí být plně podporován vedením
Musí být určen člen vedení, jemuž je přidělena celková odpovědnost za způsobilost BCM
Řízení kontinuity musí být na úrovni provozní a strategické.

Dále jsou popsány následující kroky životního cyklu BCM

Porozumění činnosti organizace (bod 1 Politická podpora)

Na začátku je třeba položit a zodpovědět následující otázky:

- Jaké jsou klíčové záměry a cíle organizace?
- Jakých výstupů a dosažitelných výsledků je zapotřebí, aby bylo dosaženo těchto cílů?
- V jakém časovém horizontu je třeba těchto cílů dosáhnout?
- Koho je třeba interně i externě zapojit k dosažení výsledků?
- Jak budou tyto cíle dosaženy? ¨

Analýza dopadů BIA (Business Impact Analysis)

BIA je základem celého procesu řízení kontinuity činnosti. Identifikují a kvantifikují se dopady, přerušení nebo narušení kritických činností, naleznou se závislosti mezi nimi. Poskytované procesy, služby a produkty se musí analyzovat jako celek. Tato analýza se musí provést před tím, než se určí přijatelné riziko.

Hodnocení rizik (RA risk assessment)

Hodnocení rizik umožní minimalizovat ovlivnění incidentem. Je poté možno definovat, implementovat a řídit adekvátní soubor opatření.

Strategie řízení kontinuity činnosti
Strategie se zabývá určením výběru alternativních metod, použitím kterých budou po incidentu zachovány kritické činnosti organizace na minimální přijatelné úrovni.

Vývoj a implementace plánů
Vychází z analýzy rizik, přijatelné úrovně zbytkového rizika a z provozního prostředí. Buď jsou jednotlivé plány jednotlivé dokumenty, nebo je vše jeden dokument.

Vytvoření a upevňování kultury
Vytvoření, zavedení a upevnění kultury řízení kontinuity činnosti v organizaci. Mělo by dojít k tomu, že organizace, ale i její partneři získaly důvěru v to, že je schopna zvládnout incidenty.

Testování, aktualizace, změny, audit
Dříve se testoval pouze IT systém, dnes se za kritický prvek považuje testování toho, že jsou lidé vycvičení pro případ incidentu. Testování by mělo zahrnout strategii řízení kontinuity činností, plán obnovy funkčnosti, nácvik rolí členů týmu a personálu a nakonec i testování IT systému organizace. PAS 56 obsahuje **Hodnotící kritéria BCM**, což je soubor klíčových otázek, které odrážejí jednotlivé etapy životního cyklu programu řízení kontinuity činnosti organizace. Organizace je může použít jako sama sebe hodnotící kritéria. Jedná se o stovky otázek, které postupně procházejí budování BCM.

Závěr: Bezpečnost informačního systému je pro každou organizaci zásadní. Proto její budování musí provedeno profesionálně za použití vhodných nástrojů. V příspěvku jsou popsány některé z nich.

LITERATURA
[1] Moravec M., Brechlerová D.:ITIL and security management, Agrárni perspektivy 2007 sborník , ISBN978-80-213-1675-1, ČZU
[2] http://www.itil.cz/index.php?id=929 citace dne 5.4.2010
[3] http://www.iso.org/iso/catalogue_detail?csnumber=42103 citace dne 5.4.2010